Pace Law Review

Volume 33
Issue 3 *Summer 2013*

Article 7

July 2013

The Expanded Use of Wiretap Evidence in White-Collar Prosecutions: Rebalancing Privacy Through More Vigorous Enforcement of the Predicate Offense Requirement and the Suppression Provisions of Title III

Kyle G. Grimm
Cadwalader, Wickersham & Taft, LLP

The Expanded Use of Wiretap Evidence in White-Collar Prosecutions: Rebalancing Privacy Through More Vigorous Enforcement of the Predicate Offense Requirement and the Suppression Provisions of Title III

Kyle G. Grimm, Esq.*

I. Introduction

Eavesdropping on private conversations has occurred since time immemorial. At common law this practice was considered a nuisance punishable as a crime.[1] Along with the development of electricity and the telegraph, the secret interception of private electronic messages began.[2] States recognized early on the danger to individual privacy accompanying the ability to surreptitiously listen to private telegraph and telephone messages. As early as the turn of the Twentieth Century, states such as Illinois and California prohibited the use of wiretaps.[3] In addition to these privacy concerns, however, law-enforcement agencies were also quick to recognize the advantages of being able to covertly listen to a private conversation. During the era of Prohibition, for example,

* Cadwalader, Wickersham & Taft, LLP; J.D., *summa cum laude*, Seton Hall University School of Law; B.S., Union College.

1. *See* 4 WILLIAM BLACKSTONE, COMMENTARIES *169. Although at common law a nuisance was generally punishable as a criminal offense, today it is generally considered a tort. *See, e.g.*, *In re* Lead Paint Litig., 924 A.2d 484, 495 (N.J. 2007) (citing RESTATEMENT (SECOND) OF TORTS § 821B cmt. b (1979)).

2. *See, e.g.*, Berger v. New York, 388 U.S. 41, 45-47 (1967) (recounting the early history of eavesdropping laws).

3. *See id.* at 46.

"wiretaps were the principal source of information relied upon by the police as the basis for prosecutions."[4] The use of wiretaps remains prevalent today. It continues to be one of the most important law enforcement tools available and one of the most persuasive pieces of evidence that can be presented to a jury. Indeed, as the world has become more "connected" with emerging technology, the prevalence of wiretap use in criminal investigations has increased. The reported number of authorized wiretap applications has grown by a total of sixty-one percent from 2001 through 2011.[5]

The expanded use of wiretaps presents troubling questions for courts and litigants. Although wiretaps are generally subject to challenges under the Fourth Amendment, the modern use of wiretaps has been defined largely by statute. Following several developments in the area of Fourth Amendment jurisprudence, Congress enacted the Wiretap Act of 1968, which was passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III" or "Title III of the Crime Control Act").[6] The purpose of Title III was to balance properly the competing law enforcement and privacy interests inherent in the government's covert interception of personal conversations.[7] In order to preserve individual privacy, Congress enacted several statutory protections meant

4. *Id.*

5. *See* ADMIN. OFFICE OF THE U.S. COURTS, APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 10 (June 2012), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/2011WireTap.pdf [hereinafter 2011 WIRETAP REPORT]. This, however, may also be due in part to federal and state officials' increased awareness of reporting requirements. *See* ADMIN. OFFICE OF THE U.S. COURTS, APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 7 (June 2011), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/2010WireTapReport.pdf [hereinafter 2010 WIRETAP REPORT] (noting that the thirty-four percent increase in reported wiretaps between 2009 and 2010 was "due, at least in part, to enhanced [Administrative Office of the United States Courts'] efforts to ensure that federal and state authorities were aware of their reporting responsibilities under 18 U.S.C. § 2519").

6. Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801-802, 82 Stat. 197, 211-23 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2012)).

7. *See id.*§ 801(b), 82 Stat. at 211.

to avoid government investigators resorting to wiretap use as a matter of course. Two of the most important requirements mandate that a wiretap may be used only where the government is investigating a specific enumerated offense found in Title III and that the government may use a wiretap only where it is "necessary" to advance a criminal investigation.[8] As several recent white-collar prosecutions indicate, both of these requirements have been weakened by the courts.[9] In turn, this development threatens the balance of interests that Congress sought to achieve in enacting Title III.[10]

Starting in the late 1960s, Congress directed that wiretaps could be authorized for use only where government officials are investigating certain enumerated offenses specifically listed in Title III.[11] Most pervasively, wiretaps have been permitted for use by government officials in investigating organized drug-trafficking schemes. For example, in 2011, narcotics investigations accounted for over eighty-five percent of all court-authorized electronic intercepts.[12] Recently, however, federal authorities have been able to obtain convictions for white-collar crimes beyond those enumerated in Title III based, in part, on the use of wiretap evidence.[13] Over the past several years in the Southern District of New York, more than 65 people have been convicted of insider trading either through plea agreement or jury verdict.[14] Of the eight cases to go to

8. *See* discussion *infra* Parts III.B.1., III.B.3.

9. *See id.*

10. *See supra* note 7 and accompanying text.

11. *See* Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 216-17 (1968) (codified as amended at 18 U.S.C. § 2516 (2012)).

12. 2011 WIRETAP REPORT, *supra* note 5, at 16 tbl.3 (a total of 2,334 out of 2,732 wiretaps warrants were granted to investigate narcotics offenses).

13. *See, e.g.*, Peter J. Henning, *The Winning Record of Prosecutors of Insider Trading*, N.Y TIMES DEALBOOK (Aug. 21, 2012, 11:49 AM), http://dealbook.nytimes.com/2012/08/21/the-winning-record-of-prosecutors-of-insider-trading/ (discussing recent cases).

14. Walter Pavlo, *Doug Whitman Guilty of Insider Trading*, FORBES, (Aug. 20, 2012, 1:49 PM), http://www.forbes.com/sites/walterpavlo/2012/08/20/doug-whitman-guilty-of-insider-trading/.

trial, the government has a perfect conviction rate.[15] In the most high-profile of these cases, the prosecution of Raj Rajaratnam, founder of the Galleon Group hedge fund, federal prosecutors relied heavily on the use of wiretaps.[16] The Galleon-related cases mark "the first time that court-authorized wiretaps have been used to target significant insider trading on Wall Street."[17] This development sent shock-waves through the world of finance; the change in investigative technique signaled by these cases has alternatively been described as "seismic,"[18] "dramatic,"[19] and a "landmark."[20] Preet Bharara, the United States Attorney for the Southern District of New York, summed up the anxiety felt on Wall Street when announcing the arrest of several insider-trading defendants: "Today, tomorrow, next week, the week after, privileged Wall Street insiders who are considering breaking the law will have to ask themselves one important question: Is law enforcement listening?"[21]

In addition to the expanded use of wiretaps during the investigation of crimes not specifically enumerated under Title III, courts have also been weakening other statutory

15. Henning, *supra* note 13.

16. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *1-2 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

17. Preet Bharara, U.S. Attorney for the S. Dist. of N.Y., Prepared Remarks for U.S. Attorney Preet Bharara: U.S. v. Raj Rajaratnam, et al.; U.S. v. Dainielle [sic] Chiesi, et al., Hedge Fund Insider Trading Takedown 2 (Oct. 16, 2009), *available at* http://www.justice.gov/usao/nys/hedgefund/hedgefundinsidertradingremarks101609.pdf.

18. *See* Stephen A. Miller, *Will There be a 'CSI Effect' for Wiretapping?*, L. TECH. NEWS (ONLINE) (May 23, 2011), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202494773565&Will_There_Be_a_CSI_Effect_for_Wiretapping&slreturn=20120722144320.

19. *See White Collar Crime, Blue Collar Tactics: A Defense Lawyer's Perspective*, BAKER BOTTS, http://www.bakerbotts.com/infocenter/publications/detail.aspx?id=037e2b4e-0948-44d4-8159-129d0e61c018 (last visited July 13, 2013).

20. *See* Patricia Hurtado, *FBI Pulls Off 'Perfect Hedge' to Nab New Insider Trading Class*, BLOOMBERG (Dec. 20, 2011, 12:00 AM), http://www.bloomberg.com/news/2011-12-20/fbi-pulls-off-perfect-hedge-to-nab-new-insider-trading-class.html.

21. *See* Bharara, *supra* note 17, at 2.

requirements. Congress sought to limit the increasing use of wiretaps by, *inter alia*, limiting their application to cases where resorting to this invasive technique is considered "necessary."[22] In order to establish the required "necessity" during the warrant application process, a government official applying for a wiretap warrant must provide "a full and complete statement" of those facts surrounding the investigation and why the government has been unsuccessful in its investigation, or why it would likely be unsuccessful if alternative techniques were tried.[23] A recent trend has emerged, however, wherein courts analyzing a suppression motion have applied the constitutional standard of *Franks v. Delaware*[24] to the statutorily-based necessity requirement.[25] This has permitted the government to, in effect, obtain a wiretap warrant without the appropriate judicial pre-screening as mandated by Title III. In turn, this is likely to increase the use of wiretaps as an investigative technique because a wiretap applicant may now obtain a warrant based upon faulty information and justify its "necessity" after the fact.

With the expanded use of wiretaps, courts will be faced in the coming years with questions concerning the contours of statutory authorization and the consequences of this expanded use into areas not traditionally associated with wiretap evidence. This is especially true in light of the fact that the United States Department of Justice ("DOJ") has already promised that its use of wiretaps will "'continue to go up dramatically.'"[26] This Article attempts to highlight some of the consequences of failing to strictly adhere to the statutory requirements of Title III, most importantly the predicate

22. *See* 18 U.S.C. § 2518(1)(c) (2012).

23. *Id.*

24. 438 U.S. 154 (1978).

25. *See, e.g.*, United States v. Shryock, 342 F.3d 948, 977 (9th Cir. 2003); United States v. Green, 175 F.3d 822, 828 (10th Cir. 1999); United States v. Guerra-Marez, 928 F.2d 665, 670-71 (5th Cir. 1991); United States v. Cole, 807 F.2d 262, 267-68 (1st Cir. 1986); United States v. Ippolito, 774 F.2d 1482, 1484-85 (9th Cir. 1985).

26. *See* Hilary Russ, *DOJ Promises More Wiretaps in White Collar Cases,* LAW360.COM (Nov. 4, 2010, 3:24 PM), http://www.law360.com/topnews/articles/206673/doj-promises-more-wiretapsin-white-collar-cases.

offense and necessity requirements. It then suggests several ways to rebalance privacy interests in the larger context of wiretap use. Part II of this article will provide a brief history of wiretap jurisprudence leading up to the passage of Title III of the Crime Control Act in 1968.[27] Part III will provide an overview of the current statutory scheme applicable to the use of wiretaps.[28] Part IV will examine several recent trends in which wiretap evidence was used to obtain convictions for crimes not specifically listed in Title III and in which courts have adopted a constitutional analysis in determining whether evidence should be suppressed for a violation of the statutory-based necessity requirement.[29] Finally, Part V will discuss several alternative approaches courts could adopt in enforcing the strictures of Title III in order to more appropriately balance privacy interests as Congress originally intended.[30]

II. The History of Wiretap Jurisprudence Leading up to Title III of the Crime Control Act

The use of wiretaps extends as far back as the beginning of the Twentieth Century, and possibly even as far back as the late Nineteenth Century.[31] It was not until 1928, in *Olmstead v. United States*,[32] that the Supreme Court first visited the use of wiretaps in criminal prosecutions.[33] At the time *Olmstead* was decided, the Fourth Amendment was interpreted to protect against unwarranted trespass of a man's house, his person, his papers and his effects—i.e., it protected material things.[34] In *Olmstead*, the Court concluded that admitting into evidence information obtained by wiretap did not violate the Fourth

27. *See* discussion *infra* Part II.

28. *See* discussion *infra* Part III.

29. *See* discussion *infra* Part IV.

30. *See* discussion *infra* Part V.

31. *See* Berger v. New York, 388 U.S. 41, 45-50 (1967) (recounting the early history of eavesdropping laws).

32. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

33. *See Berger*, 388 U.S. at 50.

34. *See Olmstead*, 277 U.S. at 464.

Amendment.[35] In reaching this conclusion, the Court reasoned that telegraph and telephone messages were different in kind than those instrumentalities that were traditionally protected by the Fourth Amendment.[36]

For the next thirty years, constitutional considerations played no role in determining whether the use of wiretap evidence was permitted in the prosecution of criminal defendants. In 1967, however, *Olmstead* was overruled by *Berger v. New York*[37] and *Katz v. United States*.[38] These cases shifted the paradigm of Fourth Amendment protection from one based on notions of physical invasion to one based on expectations of privacy.[39] In *Berger*, the Court held for the first time that the Fourth Amendment was applicable when challenging the use of wiretaps in criminal prosecutions.[40] More specifically, the *Berger* court concluded that a New York statute authorizing the issuance of a wiretap warrant was facially unconstitutional because it authorized eavesdropping "without requiring belief that any particular offense has been or is being committed," and because it did not contain a particularity requirement.[41] The Court recognized that "[b]y its very nature eavesdropping involves an intrusion on privacy that is broad in scope,"[42] and that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping

35. *Id.* at 466.

36. *See id.* at 464-65.

37. 388 U.S. 41 (1967).

38. 389 U.S. 347 (1967).

39. In *Katz*, the Court concluded that "the Fourth Amendment protects people, not places." *Id.* at 351. As such, "what he [or she] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351-52 (citing Rios v. United States, 364 U.S. 253 (1960); *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

40. *See Berger*, 388 U.S. at 53-58.

41. *Id.* at 58-59. The particularity requirement stems from the Fourth Amendment's command that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*." U.S. CONST. amend. IV (emphasis added). "In the wiretap context, [the Fourth Amendment's particularity] requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized." United States v. Donovan, 429 U.S. 413, 427 n.15 (1977).

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

devices."[43]

During the thirty-year period between *Olmstead* and *Berger*, the statutory landscape regulating the use of wiretap evidence began to take shape. Despite rejecting any constitutional challenge to their use, *Olmstead* marked a larger shift in the use of wiretaps in criminal prosecutions by issuing a call to arms for Congress to act.[44] The *Olmstead* Court stated: "Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence."[45]

Congress responded in 1934 by passing what became section 605 of the Federal Communications Act (FCA).[46] Section 605, as originally enacted, provided in relevant part:

> No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, . . . in response to a subpoena [sic] issued by a court of competent jurisdiction, or on demand of other lawful authority.[47]

43. *Id.* at 63.

44. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("In an ironic sense, although *Katz* overruled *Olmstead*, Chief Justice Taft's suggestion in the latter case that the regulation of wiretapping was a matter better left for Congress has been borne out." (internal citation omitted)).

45. Olmstead v. United States, 277 U.S. 438, 465-66 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

46. Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103-04 (1934) (codified as amended at 47 U.S.C. § 605 (2012)); *see also Berger*, 388 U.S at 51 ("Congress soon thereafter, and some say in answer to *Olmstead*, specifically prohibited the interception without authorization and the divulging or publishing of the contents of telephonic communications.").

47. § 605, 48 Stat. at 1103.

In its first landmark case addressing this statute, *Nardone v. United States* ("Nardone I"),[48] the Supreme Court interpreted the term "any person" to include federal authorities; the Court refused to read into the statute an implied exception for federal officers who obtained wiretap evidence in violation of the statute.[49] The Court read section 605 in accordance with its plain meaning such that it prohibited "anyone, unless authorized by the sender, to intercept a telephone message, and directs in equally clear language that 'no person' shall divulge or publish the message or its substance to 'any person.'"[50] Moreover, the Court concluded that "[t]o recite the contents of the message in testimony before a court is to divulge the message."[51] Thus, federal prosecutors could not use wiretap evidence obtained in violation of section 605 in a criminal prosecution because Congress had specifically prohibited it.[52] When the defendant in *Nardone I* again worked his way back to the Supreme Court two years later, the Court held that section 605 barred not only the use of evidence obtained in violation of the FCA, but that it also barred the "fruits" derived from that evidence from being admitted.[53]

Over the next three decades, section 605 played a central role in determining the admissibility of wiretap evidence in the federal courts. Numerous cases over this period addressed the reach and meaning of the statute. First, in *Weiss v. United States*,[54] the Court concluded that section 605 applied to both interstate and wholly-intrastate communications.[55] Three years later, the Court held that only a party to the recorded conversation had standing to object to its use in evidence.[56] In *Schwartz v. Texas*,[57] the Court held "that § 605 applies only to the exclusion in federal court proceedings of evidence obtained

48. Nardone v. United States (*Nardone I)*, 302 U.S. 379 (1937).
49. *See id.* at 382-84.
50. *Id.* at 382.
51. *Id.*
52. *See id.* at 383-85.
53. *See* Nardone v. United States (*Nardone II)*, 308 U.S. 338, 340-41 (1939).
54. 308 U.S. 321 (1939).
55. *See id.* at 329.
56. *See* Goldstein v. United States, 316 U.S. 114, 121-22 (1942).
57. 344 U.S. 199 (1952).

and sought to be divulged in violation thereof; it does not exclude such evidence in state court proceedings."[58] *Schwartz* treated section 605 as simply a "rule of evidence," and reasoned that Congress did not unequivocally declare its intent to preempt state law in this area.[59] The Court continued to treat section 605 as a rule of evidence in *Benanti v. United States*.[60] There, the Court determined that evidence unlawfully obtained in violation of section 605 was inadmissible in federal court despite the fact that it was obtained by state officials.[61] In the same year *Benanti* was decided, the Court also held that no violation of the statute occurred where police had listened to a conversation with the permission of one of the parties.[62] Finally, in 1968, the year after the Court refocused its Fourth Amendment jurisprudence on the notion of privacy, the Court decided *Lee v. Florida*.[63] In *Lee*, the Court overruled its previous decision in *Schwartz* and held that section 605 rendered inadmissible any evidence obtained in violation of the FCA in state court prosecutions.[64]

In response to the Court's decisions in *Berger* and *Katz*[65]—

58. *Id.* at 203.

59. *Id.*

60. 355 U.S. 96, 100 (1957).

61. *See id.* at 100 ("[E]vidence obtained by means forbidden by Section 605, whether by state or federal agents, is inadmissible in federal court.").

62. *See* Rathbun v. United States, 355 U.S. 107, 108, 111 (1957).

63. 392 U.S. 378 (1968).

64. *See id.* at 385-87. The Court reasoned that *Schwartz* was decided "in the shadow of *Wolf v. People of State of Colorado*." *Lee*, 392 U.S. at 383 (citation omitted). The Court in *Wolf* held that "in a prosecution in a State court for a State crime the Fourteenth Amendment does not forbid the admission of evidence obtained by an unreasonable search and seizure." Wolf v. Colorado, 338 U.S. 25, 33 (1949), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961). The *Mapp* Court held that evidence obtained in violation of the Fourth Amendment, as applied to the states through the Fourteenth Amendment, was inadmissible in a state court prosecution. *See Mapp*, 367 U.S. at 655. The Court in *Lee* thus subsequently concluded that "[i]n view of the *Nardone* and *Benanti* decisions, the doctrine of *Schwartz v. State of Texas* cannot survive the demise of *Wolf v. People of the State of Colorado*." *Lee*, 392 U.S. at 385.

65. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (characterizing Title III of the Omnibus Crime Control and Safe Streets Act of 1968 as a response the Supreme Court's decision in *Katz*); *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 849

and just two days after the Court handed down its decision in *Lee*—Congress ushered in a new era for the use of wiretaps in criminal prosecutions by passing Title III of the Crime Control Act.[66] Title III, among other things, rewrote section 605 to apply principally to communication personnel,[67] and it set forth a separate regime for authorizing wiretaps by law enforcement authorities.[68]

III. Title III: The Current Statutory Scheme

In passing Title III Congress intended "to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce."[69]

(2004) (arguing that the decisions in *Berger* and *Katz*, a wiretap and a bugging case respectively, "were carefully timed to influence the shape of statutory law").

66. Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801-802, 82 Stat. 197, 211-23 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2012)).

67. *See id.* § 803, 82 Stat. at 223-25 (codified as amended at 47 U.S.C. § 605 (2012)).

68. *See id*. § 802, 82 Stat. at 212-23 (codified as amended at 18 U.S.C. §§ 2510-22 (2012)).

69. *See id.* § 801(b), 82 Stat. at 211; *see also* Gelbard v. United States, 408 U.S. 41, 48-49 (1972). The court noted that:

> The Senate committee report that accompanied Title III underscores the congressional policy: 'Title III has as it [*sic*] 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.' Hence, although Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern.

Congress achieved these goals by (i) "defin[ing] on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized"; (ii) by "prohibit[ing] any unauthorized interception of such communications"; and (iii) by regulating "the use of the contents thereof in evidence in courts and administrative proceedings."[70] In the years since 1968, Title III has been amended numerous times.[71]

In its current iteration, Title III broadly prohibits the interception and disclosure of wire, oral, or electronic communications,[72] and it makes doing so a crime punishable by a fine, a term of imprisonment, or both.[73] In addition, Title III prohibits the use of wiretap evidence in any judicial, administrative, regulatory, and other similar proceeding if the communication was obtained in violation of federal law.[74] Title III, however, does not entirely prohibit the use of wiretaps by law enforcement. Instead, Title III sets forth a comprehensive scheme that government officials must follow in order to secure an electronic surveillance order.[75]

A. *What Constitutes a Wiretap Under Title III*

The term "wiretap" is not used in Title III to describe the use of electronic eavesdropping devices.[76] Rather, the scope of Title III is defined in terms of the type communication at issue, whether information from this protected communication is obtained or used by a third party, and the manner in which information from a protected communication is obtained.[77] In common usage, the term "wiretapping" is thought to be "confined to the interception of communication by telephone

Id. (internal citation omitted).

70. *See* § 801(b), 82 Stat. at 211.

71. *See, e.g.*, 18 U.S.C. § 2511 (2012) (amended in 1970, 1978, 1984, 1986, 1994, 1994, 1996, 2001, 2002, 2008, 2008).

72. *See id.* § 2511(1); *see also Gelbard*, 408 U.S. at 46.

73. See 18 U.S.C. § 2511(4)(a).

74. *See id.* § 2515.

75. *See id.* § 2518(1).

76. *See generally id.* §§ 2510-2522.

77. *See id.*

and telegraph and generally may be performed from outside the premises to be monitored."[78] This is in contrast to "bugging," which generally refers to "the interception of all oral communications in a given location" and is typically "accomplished by installation of a small microphone in the room to be bugged and transmission to some nearby receiver."[79] Title III regulates both wiretapping and bugging by prohibiting the "interception" and "disclosure" of "wire, oral, or electronic communications."[80]

1. Protected Communications

In order to fall under the purview of Title III, the communication at issue must be a protected communication. There are three different categories of communications protected against unlawful interference: wire communications, oral communications, and electronic communications.[81] The statutory definitions provided for the types of communications regulated under Title III are broad in scope.

A "wire communication" is expansively defined under Title III as:

> [A]ny 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.[82]

78. Dalia v. United States, 441 U.S. 238, 240 n.1 (1979) (citation omitted).

79. *Id.* (citations omitted).

80. *See* 18 U.S.C. § 2511.

81. *See generally id.* § 2510.

82. *See id.*

This definition includes spoken communication made over both land-based phone lines and cell phones.[83] Importantly, however, a "wire communication" is limited to only the "aural acquisition" of information, which "literally translated mean[s] to come into possession through the sense of hearing."[84] Therefore, information, such as the numbers dialed, that is transmitted via cell phone, other than the voices of the phone call participants, does not fall within the purview of Title III.[85] Rather, the numbers dialed, signaling information, and many other similar types of non-aural information transmitted via cell phone are governed by the Pen Register and Trap and Trace Statute ("Pen Register Act").[86]

In contrast to a wire communication, "an oral communication is one carried by sound waves, not by an electronic medium."[87] Under Title III, "oral communication" is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not

83. *See* Bartnicki v. Vopper, 532 U.S. 514, 524 & n.7 (2001) (citing Nix v. O'Malley, 160 F.3d 343, 346 (6th Cir. 1998); McKamey v. Roach, 55 F.3d 1236, 1240 (6th Cir. 1995)); *see also In re* U.S. for an Order Authorizing Roving Interception of Oral Communications, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003) ("Despite the apparent wireless nature of cellular phones, communications using cellular phones are considered wire communications under the statute, because cellular telephones use wire and cable connections when connecting calls." (citing 18 U.S.C. § 2510(1); S. Rep. No. 99-541, at 11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3565; H. Rep. No. 99-647, at 31 (1986); *Bartnicki*, 532 U.S. at 524)). Telephone intercepts accounted for ninety-six percent of all intercepts installed by government investigators in 2011, and the majority of these intercepts involved cellular phones. *See* 2011 WIRETAP REPORT, *supra* note 5, at 9.

84. Smith v. Wunker, 356 F. Supp. 44, 46 (S.D. Ohio 1972) (citation omitted); *cf.* United States v. Larios, 593 F.3d 82, 90 (1st Cir. 2010) ("Every circuit court to address the issue has concluded that Title III does not regulate *silent* video surveillance.") (emphasis added) (collecting cases).

85. *See, e.g.*, United States v. New York Tel. Co., 434 U.S. 159, 166 (1977) ("Both the language of the statute and its legislative history establish beyond any doubt that pen registers are not governed by Title III.").

86. *See* 18 U.S.C. §§ 3121-3127. A "pen register" is defined under the Pen Register Act as "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(3).

87. S. Rep. No. 99-541, at 13, *reprinted in* 1986 U.S.C.C.A.N. at 3567.

subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication."[88] The most important aspect of this definition is the expectation of privacy of those carrying on the conversation. As several circuit courts have noted: "The legislative history of Title III shows that Congress intended th[e] definition [of 'oral communication'] to parallel the 'reasonable expectation of privacy test' articulated by the Supreme Court in *Katz*."[89]

Although wire communications and oral communications are conceptually distinct, it is possible for a communication to appropriately be characterized as both in certain situations.[90] As explained in one House Report:

> The definitions of wire communication and oral communication are not mutually exclusive. Accordingly, different aspects of the same communication might be differently characterized. For example, a person who overhears one end of a telephone conversation by listening in on the oral utterances of one of the parties is intercepting an oral communication. If the eavesdropper instead taps into the telephone wire, he is intercepting a wire communication.[91]

Beyond regulating wire and oral communications, Congress responded to evolving technology by amending Title

88. 18 U.S.C. § 2510(2).

89. United States v. Turner, 209 F.3d 1198, 1200 (10th Cir. 2000) (citing S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2178; United States v. Longoria, 177 F.3d 1179, 1181 (10th Cir. 1999)); *see also Larios*, 593 F.3d at 92 (citing United States v. Dunbar, 553 F.3d 48, 57 (1st Cir. 2009)). Moreover, at least one circuit court has held that the definition of "oral communication" should "evolve" along with Fourth Amendment jurisprudence. *See Larios*, 593 F.3d at 92-93.

90. *See* United States v. Borch, 695 F. Supp. 898, 899, 901-02 (E.D. Mich. 1988) (oral communications intercepted via inadvertently open phone line are not wire communications), *rev'd on other grounds sub nom*. United States v. Baranek, 903 F.2d 1068 (6th Cir. 1990).

91. H. Rep. No. 99-647, at 34 (1986).

III to provide protection for all "electronic communications."[92] With this addition, "authority to intercept electronic communications became subject to the same requirements as those applicable to the interception of oral and wire communications."[93] The term "electronic communication" includes "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" with four limited exceptions.[94] Some examples of electronic communications include "digital-display paging devices, fax machines, [and] text messaging."[95] Perhaps most importantly, the definition of "electronic communications" encompasses nearly all communications sent from a computer, including email. Courts have held, for example, that websites[96] and the submission of online forms[97] fall within the definition of "electronic communication." Not all communications originating on a computer, however, fall within this definition. At least one district court, in a fact-intensive analysis, determined that capturing keystrokes on a computer during the transfer of this information from the keyboard to the local

92. *See* Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, tit. I, §§ 101-102, 100 Stat. 1848, 1848-53 (1986).

93. Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995) (citing 18 U.S.C. § 2516).

94. *Brown*, 50 F.3d at 289 (citing 18 U.S.C. § 2510(12)). These exceptions 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 [18 U.S.C. § 3117]); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. §2510(12).

95. *See* 2011 WIRETAP REPORT, *supra* note 5, at 9.

96. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

97. *See, e.g.,* United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); *see also In re* Pharmatrak Inc., 329 F.3d 9, 18 (1st Cir. 2003) (citing *Steiger*, 318 F.3d at 1047; *Konop*, 302 F.3d at 876).

computer's hard drive was not an "electronic communication."[98] The court's reasoning in this case relied heavily on the fact that the keystrokes were recorded as they went from the keyboard to another internal part of the computer—i.e., the communication at issue was wholly internal to the computer system itself.[99] This analysis seemingly suggests that the transmission of keystrokes over the internet—e.g., from a computer modem to a program such as Google—likely would fall within the definition of an "electronic communication." Thus, it appears that while not all internal computer communications are covered by Title III, all internet communications of any stripe likely fall within its reach.

2. Prohibited Conduct

Once it is established that a communication is covered by Title III, the "interception" of this communication is generally prohibited.[100] Under the statute, to "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."[101] This definition has two main elements: first, the contents of covered communication must be "acqui[red]" and second, this "acquisition" must occur by way of an "electronic, mechanical, or other device."[102]

Initially, courts throughout the country, largely relying on an influential case from the Fifth Circuit, interpreted the acquisition requirement narrowly to include only the "contemporaneous acquisition of the communication."[103]

98. *See* United States v. Ropp, 347 F. Supp. 2d 831, 832 (C.D. Cal. 2004).

99. *See id.* at 837-38.

100. *See* 18 U.S.C. § 2511(1) (2012).

101. *Id.* § 2510(4).

102. *See id.*

103. United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976), *superseded by statute* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), *as recognized in* United States v. Smith, 155 F.3d 1051, 1057 n.11 (9th Cir. 1998) (citing cases). The *Turk* court reasoned:

> The words acquisition . . . through the use of any . . . device

Congress, however, later amended the definition of "intercept" to include "aural or other acquisition," as opposed to merely "aural acquisitions."[104] Similarly, Congress amended the definition of wire communications to include "any electronic storage of such communication."[105] Thus, the contemporaneity requirement is no longer required to "intercept" a wire communication as defined under Title III.[106] Despite this, courts have continued to apply a contemporaneity requirement where electronic communications are at issue.[107] The definition of electronic communication makes no reference to stored information.[108] Courts have relied on this textual difference to conclude that it was "Congress' understanding that, although one could intercept a *wire* communication in storage, one could not intercept an *electronic* communication in storage."[109] Stored electronic communications—e.g., emails stored on a computer server—are governed by a different statutory scheme called the Stored Communications Act, which was passed as Title II of the Electronic Communications Privacy Act of 1986.[110]

> suggest that the central concern is with the activity engaged in at the time of the oral communication which causes such communication to be overheard by the uninvited listeners. If a person secrets a recorder in a room and thereby records a conversation between two others, an acquisition occurs at the time the recording is made. . . . [If] a new and different aural acquisition occurs each time a recording of an oral communication is replayed[, it] [] would mean that innumerable interceptions, and thus violations of [Title III], could follow from a single recording.

Turk, 526 F.2d at 658. (internal quotation marks and footnotes omitted).

104. *See* § 101(a)(1)(3)(A), 100 Stat. at 1848 (codified as amended at 18 U.S.C. § 2510(4)).

105. *See* § 101(a)(1)(D), 100 Stat. at 1848 (codified as amended at 18 U.S.C. § 2510(1)).

106. *See, e.g.*, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-62 (5th Cir. 1994); *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002) (collecting cases).

107. *See, e.g.*, *Steve Jackson Games, Inc.*, 36 F.3d at 460 (citing *Turk*, 526 F.2d at 658).

108. *See* 18 U.S.C. § 2510(12).

109. *Konop*, 302 F.3d at 877 (internal quotation marks omitted) (collecting cases).

110. *See* Stored Communications Act of 1986, Pub. L. No. 99-508, tit. II, § 201, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§

In addition to the "acquisition" requirement, a communication is only "intercepted" within the meaning of Title III if the acquisition is done through an "electronic, mechanical, or other device."[111] This phrase is defined in a circular fashion as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication."[112] There are two exceptions to this definition, neither of which is particularly relevant to the use of wiretaps by law enforcement.[113]

B. *Procedure for Obtaining a Wiretap Warrant by Law Enforcement*

In addition to broadly prohibiting the use of wiretaps by those unassociated with law enforcement, Title III also sets out a detailed scheme that allows government officials to obtain a warrant permitting the use of covert electronic surveillance.[114] In promulgating this statutory scheme, Congress sought to balance two competing concerns. First, Congress recognized that "[t]he interception of [wire, oral, and electronic] communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice."[115] At the same time, however, Congress sought to protect the privacy of innocent individuals. Congress therefore determined that

2701-2711).

111. 18 U.S.C. § 2510(5).

112. *Id.*

113. First, the "business extension use" exception permits the interception of wire communications where: (1) the equipment used "constitute[s] a 'telephone or telegraph instrument, equipment or facility, or a[] component thereof,' either provided by, and installed by, [the service provider] in the ordinary course of *its* business or, equivalently, supplied by [the subscriber] for connection to [the service provider's] facilities," and (2) the use of that equipment "fall[s] within the ordinary course of [] business." Sanders v. Robert Bosch Corp., 38 F.3d 736, 740 (4th Cir. 1994); *see also* 18 U.S.C. § 2510(5)(a). Second, "a hearing aid or similar device being used to correct subnormal hearing to not better than normal" may be used without violating Title III. *See* 18 U.S.C. § 2510(5)(b).

114. *See id.* § 2518.

115. *See* Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968, Pub. L. No. 90-351, tit. III, § 801(c), 82 Stat. 197, 211 (1968).

clandestine wiretap surveillance should occur "only when authorized by a court of competent jurisdiction" and that interception "should further be limited to certain major types of offenses and specific categories of crime."[116]

Before addressing the statutory scheme applicable to securing a wiretap warrant, it is important to note that a warrant is necessary only where all parties to the intercepted communication are unaware of the surveillance.[117] Section 2511(2)(c) of Title III provides that "[i]t shall not be unlawful . . . 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."[118] Thus, in many cases, the government must resort to the warrant-application procedures of Title III only where they have no cooperating witness to rely upon. Accordingly, prosecutors principally rely on the use of wiretaps only in complex criminal schemes, where discretion is paramount to the investigation. This can perhaps account for the relatively small (but increasing) number of authorized federal wiretaps throughout the country.[119]

Generally speaking, once the Attorney General or another designated DOJ official has pre-approved the use of a wiretap,[120] there are four main requirements that a government applicant must comply with in order to obtain a valid warrant under Title III. First, a specific predicate offense must be identified as the basis for the investigation.[121] Second, the government must provide a full and complete statement of the facts and circumstances sufficient to establish probable cause and to satisfy a heightened particularity requirement.[122] Third, the use of a wiretap must be "necessary" to further the

116. *See id.* § 801(d), 82 Stat. at 211-12.

117. *See* 18 U.S.C. § 2511(2)(c).

118. *Id.*

119. In 2011, for example, the Administrative Office of the United States Courts reported that only 792 court-authorized intercepts were granted at the federal level. *See* 2011 WIRETAP REPORT, *supra* note 5, at 7.

120. *See generally* United States v. Giordano, 416 U.S. 505, 508 (1974) (discussing requirement); *see also* 18 U.S.C. § 2516(1).

121. *See* discussion *infra* Parts III.B.1.

122. *See* discussion *infra* Parts III.B.2.

government's investigation.[123] Finally, the government must reasonably minimize its interceptions to relevant communications.[124]

1. Predicate Acts

Title III permits the use of wiretaps in the investigation of dozens of specifically enumerated federal criminal offenses.[125] The list of predicate offenses, however, is limited. For example, a number of fraud-based crimes are listed as predicate offenses, including mail fraud, wire fraud, money laundering, bank fraud, and computer fraud.[126] But other frauds, such as a securities fraud prosecution for insider trading, are not listed as predicate offenses.[127] In addition to listing certain federal offenses, Title III also permits limited state offenses to be investigated using a wiretap so long as a separate state statute authorizes its use.[128] These state offenses include "murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year."[129]

Although the investigation of a predicate crime is a necessary requirement for securing an electronic surveillance order, courts have permitted the use of wiretaps in the prosecution of crimes not specifically listed in Title III. As the United State Court of Appeals for the Second Circuit has stated, "even if wiretaps could not be authorized for the purpose of investigating [certain] crimes, nothing in Title III

123. *See* discussion *infra* Parts III.B.3.

124. *See* discussion *infra* Parts III.B.4.

125. For a list of predicate crimes, *see* 18 U.S.C. § 2516(1). An investigation into a conspiracy to commit any predicate offense may also serve as a valid basis for an electronic surveillance order under Title III. *See id.* § 2516(1)(t).

126. *See id.* § 2516(1)(c).

127. *See generally* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *9-23 (S.D.N.Y. Nov. 24, 2010) (discussing relationship between wire fraud and securities fraud under Title III), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

128. 18 U.S.C. § 2516(2).

129. *Id.*

bars the use of the fruits of authorized wiretaps obtained in the pursuit of investigations of suspected crimes that *are* listed in Title III" during the prosecution of non-Title III crimes.[130] This is specifically provided for in the statutory text:

> When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or 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 [otherwise] provided.[131]

This provision has been described as, "in essence[,] a plain-view exception [to the predicate offense requirement] allowing the government to present evidence of other crimes discovered while investigating an authorized offense."[132]

In order for the government to use this "otherwise intercepted" evidence at trial, however, the prosecutor must apply to a judge "as soon as practicable."[133] Title III does not itself define the applicable procedure for seeking subsequent approval. The congressional history of this provision, however, indicates that Congress thought that a subsequent application should show (i) "that the original order was lawfully obtained;" (ii) that the original application "was sought in good faith and not as [a] subterfuge search;" and, (iii) that the "otherwise intercepted . . . communication was in fact incidentally

130. SEC v. Rajaratnam, 622 F.3d 159, 173 (2d Cir. 2010) (citing 18 U.S.C. § 2517(5)).

131. 18 U.S.C. § 2517(5).

132. Howard J. Kaplan et al., *The History and Law of Wiretapping*, ABA SECTION OF LITIG. 2012 SECTION ANNUAL CONFERENCE: THE LESSONS OF THE RAJ RAJARATNAM TRIAL: BE CAREFUL WHO'S LISTENING 6 (April 20, 2012), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf; *see also Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *9-10 (calling this statutory provision a "plain-view exception" (citing United States v. Masciarelli, 558 F.2d 1064, 1067 (2d Cir. 1977); 18 U.S.C. § 2517(5))).

133. 18 U.S.C. § 2517(5).

intercepted during the course of a lawfully executed order."[134]

2. Probable Cause and Particularity

In addition to investigating a predicate offense, an investigating officer must support his or her application for an electronic surveillance order with enough information so that a neutral and detached judge might conclude that there is probable cause to issue the warrant. The statute specifically provides that an applicant for a wiretap warrant must include:

> [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 [in the case of a "roving" wiretap], 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.[135]

The standard for establishing probable cause under Title III is co-equal with the standard generally applied for any regular search warrant;[136] the "totality-of-the-circumstances" must reflect a "fair probability that . . . evidence of a crime will

134. S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2189 (citations omitted).

135. 18 U.S.C. § 2518(1)(b).

136. *Id.* § 2518(3); *see also* United States v. Diaz, 176 F.3d 52, 110 (2d Cir. 1999) (quoting United States v. Fury, 554 F.2d 522, 530 (2d Cir. 1977)); United States v. Leisure, 844 F.2d 1347, 1354 (8th Cir. 1988) ("[S]tatutory probable cause standards set out in Title III are co-extensive with the constitutional requirements embodied in the fourth amendment [sic].") (citations omitted).

be found."[137] A judge may issue a wiretap warrant only if he or she finds, in addition to "necessity," probable cause to believe: (i) "that an individual is committing, has committed, or is about to commit a [predicate] offense;" (ii) "that particular communications concerning that [predicate] offense" are likely to be acquired through the permitted interception; and, (iii) that the location in which the interception is to occur is being used, or is about to be used, in connection with the predicate offense.[138]

Unlike probable cause, the particularity requirements under Title III are more stringent than the requirements under the Fourth Amendment.[139] "In the wiretap context, [the Fourth Amendment particularity] requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized."[140] Additional information, such as the name of the persons likely to be overheard, is not constitutionally required.[141] Title III, however, requires that the following information be identified with particularity:

> (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

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

138. 18 U.S.C. § 2518(3); *see also* United States v. Yannotti, 541 F.3d 112, 124 (2d Cir. 2008) (quoting *Diaz*, 176 F.3d at 110).

139. *See, e.g.*, United States v. Gaines, 639 F.3d 423, 430-31 (8th Cir. 2011).

140. United States v. Donovan, 429 U.S. 413, 427 n.15 (1977).

141. *See id.*

> interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.[142]

This list of particulars is significantly more detailed than that which is required under the Fourth Amendment. In certain situations, Title III provides for relaxed particularity requirements in the case of wire and electronic intercepts upon a showing of probable cause to believe that a party is avoiding intercepts at a particular site,[143] or, in the case of oral intercepts, that providing the required specificity "is not practical."[144] In these situations, a "roving" wiretap warrant is issued, which allows investigators to target specific persons at various locations.[145] "Roving" wiretaps are relatively rare, however, with only three federal and eight state-authorized "roving" wiretap warrants issued in 2011.[146] These heightened particularity requirements have led as least one commentator to note that "direct constitutional challenges to wiretaps have rarely been litigated since the passage of Title III . . . because Title III itself provides broader grounds for the suppression of improperly obtained wiretap evidence than the exclusionary rule."[147]

142. 18 U.S.C. § 2518(4).

143. *See id.* § 2518(11)(b).

144. *See id.* § 2518(11)(a).

145. *See* 2011 WIRETAP REPORT, *supra* note 5, at 8.

146. *See id.*

147. Kaplan et al., *supra* note 132 at 4; *see also* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("After *Katz,* Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.") (internal citation omitted). Although "necessity" is not a constitutionally required prerequisite to a valid wiretap, its basis is found in the Court's opinion in *Berger*. There, the Court stated:

> Finally, the statute's procedure, necessarily because its success depends on secrecy, has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts. On the contrary,

3. "Necessity" Requirement

Congress also included within Title III a requirement that law enforcement may resort to the use of wiretaps only when doing so is "necessary" to further the investigation.[148] The necessity requirement was added to Title III by Congress "to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime."[149] In other words, mandating that a "full and complete statement" regarding necessity be provided in the warrant application is designed "both to underscore the desirability of using less intrusive procedures and to provide courts with some indication of whether any efforts were made to avoid needless invasion of privacy."[150] Necessity in the absolute sense, however, is not required. Rather, Congress assumed that courts would apply this requirement "in a practical and commonsense fashion."[151] Therefore, although wiretaps should not be routinely used at the outset of an investigation, they also need not be used as only a last resort.[152]

Before obtaining a warrant, a prosecutor must provide "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

> it permits uncontested entry without any showing of exigent circumstances. *Such a showing of exigency, in order to avoid notice would appear more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized*.

Berger v. New York, 388 U.S. 41, 59 (1967) (emphasis added).

148. *See* 18 U.S.C. § 2518(1)(c).

149. United States v. Kahn, 415 U.S. 143, 153 n.12 (1974) (citing S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112).

150. United States v. Lilla, 699 F.2d 99, 104 (2d Cir. 1983).

151. S. Rep. No. 90-1097, *reprinted in* 1968 U.S.C.C.A.N. at 2190.

152. *See, e.g.*, United States v. Martinez, 588 F.2d 1227, 1231 (9th Cir. 1978) (citations omitted); *see also* United States v. Poulsen, 655 F.3d 492, 504 (6th Cir. 2011) ("The requirement is intended to ensure that 'the investigators give serious consideration to the non-wiretap techniques prior to applying for wiretap authority.'" (quoting United States v. Alfano, 838 F.2d 158, 163 (6th Cir. 1988) (citation omitted))).

be too dangerous."[153] A barebones or boilerplate affidavit is not sufficient.[154] Similarly, "allegations that the crime being investigated is inherently difficult to solve will not, by themselves, suffice."[155] After proffering "a reasoned explanation, grounded in the facts of the case, and which squares with common sense,"[156] an electronic surveillance order may be issued where the "judge determines on the basis of the facts submitted by the applicant that"[157] clandestine electronic surveillance is needed for the investigation to progress.[158] A judge's decision as to the necessity of issuing a wiretap warrant is afforded considerable discretion; a wiretap warrant will not be later invalidated, for example, simply because a defense lawyer can point to some investigative technique that could have been but was not used.[159]

4. "Minimization" Requirement

As another additional layer of protection for personal privacy, Title III contains several provisions meant to minimize the intrusion of government agents in private conversations. First, there are temporal limits on a wiretap warrant; no communication may be intercepted "in any event longer than thirty days."[160] If necessary, an extension may be sought, but the applicant must provide "a statement setting forth the results thus far obtained from the interception, or a reasonable

153. 18 U.S.C. § 2518(1)(c).

154. *See Martinez*, 588 F.2d at 1231-32.

155. *Id.* at 1231 (citations omitted); *see also Lilla*, 699 F.2d at 104 (collecting cases).

156. United States v. Scala, 388 F. Supp. 2d 396, 404 (S.D.N.Y. 2005) (internal quotation marks omitted).

157. 18 U.S.C. § 2518(3).

158. *See id.* § 2518(3)(c).

159. *See, e.g.*, United States v. Webster, 734 F.2d 1048, 1055 (5th Cir. 1984) (quoting United States v. Hyde, 574 F.2d 856, 867 (5th Cir. 1978)); *see also* United States v. Concepcion, 579 F.3d 214, 217 (2d Cir. 2009) ("[W]e grant considerable deference to the district court's decision whether to allow a wiretap.").

160. 18 U.S.C. § 2518(5). Courts have generally authorized intercepts for the longest time permitted by Title III. In both 2010 and 2011, the average length of an original authorization was twenty-nine days. *See* 2011 WIRETAP REPORT, *supra* note 5, at 7.

explanation of the failure to obtain such results."[161] This way, an issuing judge is able to maintain supervision over the surveillance.[162] Additional temporal protections provide that any interception must be done "as soon as practicable" and "must terminate upon attainment of the authorized objective."[163]

In a broad sense, Title III provides that electronic surveillance must be carried out in a fashion that "minimize[s] the interception of communications not otherwise subject to interception."[164] This requirement "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."[165] Courts have long recognized that avoiding the interception of all innocent conversations is nearly impossible.[166] For example, in 2011, an average wiretap surveillance scheme intercepted 3,716 communications, but only 868 of those communications were incriminating.[167] Partially because of this, investigators must do only what is reasonable, and there is no bright-line rule as to what is reasonable in this context.[168] Instead, reasonableness is to be determined on a case-by-case basis.[169] For example, the more wide-spread a conspiracy is the more covert surveillance is justified.[170] Reasonableness must be looked at in the context of the entire wiretap surveillance scheme; it cannot be determined on a "chat-by-chat" basis.[171] Moreover, the focus of

161. 18 U.S.C. § 2518(1)(f); *see also id.* § 2518(5). The longest intercept permitted in 2011 lasted for 246 days and was used in a narcotics investigation. *See* 2011 WIRETAP REPORT, *supra* note 5, at 7.

162. A judge may also require that progress reports be submitted. *See id.* § 2518(6).

163. *Id.* § 2518(5).

164. *Id.*

165. Scott v. United States, 436 U.S. 128, 140 (1978).

166. *See, e.g.*, United States v. Bynum, 485 F.2d 490, 500 (2d Cir. 1973), *cert. granted, judgment vacated*, 417 U.S. 903 (1974).

167. *See* 2011 WIRETAP REPORT, *supra* note 5, at 21 tbl.4.

168. *See Scott*, 436 U.S. at 139-40.

169. *Id.* at 140.

170. *Id.*

171. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *99 (S.D.N.Y. Nov. 24, 2010) (quoting United States

this inquiry should be on the actions of the government agent conducting the surveillance, not on his or her motives.[172] The government has the initial burden to establish prima facie that its interceptions were reasonably minimized.[173] After the government meets its burden, a defendant must prove that, "despite a good faith compliance with the minimization requirements, a substantial number of non-pertinent conversations have been intercepted unreasonably."[174]

C. *Prohibition on Use of Wiretap Evidence Obtained in Violation of Title III*

The penalties for improperly intercepting communications in violation of Title III are relatively severe. An individual subjects him or herself to up to five years in prison, as well as a fine, for unlawfully intercepting a protected communication.[175] In addition, no recordings obtained in violation of the statute may be admitted as evidence in a court proceeding. 18 U.S.C. § 2515 provides:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before

v. McGuinness, 764 F. Supp. 888, 901 (S.D.N.Y. 1991)), *aff'd*, 719 F.3d 139 (2d Cir. 2013). *But cf.* United States v. Goffer, 756 F. Supp. 2d 588, 595-96 (S.D.N.Y. 2011) (noting that the Second Circuit has not definitively ruled on this issue, but stating that "district courts in [the Second] Circuit have favored the approach of suppressing only the improperly minimized calls" (citing United States v. Principie, 531 F.2d 1132, 1140-41 (2d Cir. 1976); United States v. Pierce, 493 F. Supp. 2d 611, 636 (W.D.N.Y. 2006); United States v. King, 991 F. Supp. 77, 92 n.16 (E.D.N.Y. 1998); United States v. Orena, 883 F. Supp. 849, 855 (E.D.N.Y. 1995))).

172. *Scott*, 436 U.S. at 139.

173. *Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *100 (citing United States v. Rizzo, 491 F.2d 215, 217 n.7 (2d Cir. 1974)).

174. *Id.* (quoting United States v. Menendez, No. S(3) 04 Cr. 219 (DAB), 2005 U.S. Dist. LEXIS 11367, at *8 (S.D.N.Y. June 8, 2005); United States v. Ianniello, 621 F. Supp. 1455, 1470 (S.D.N.Y. 1985)) (internal quotation marks omitted).

175. *See* 18 U.S.C. § 2511(4)(a) (2012).

> 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.[176]

A wiretap performed in accordance with a judicially-sanctioned wiretap warrant is not in violation of the statute so long as the application requirements of Title III are complied with.[177] Suppression is appropriate, however, in three situations: "(i) [if] 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."[178] The Supreme Court has interpreted the contours on Title III's suppression provision in only three cases, all of which were decided in the 1970s.[179] These cases are discussed more fully below.[180] In the context of governmental investigations, courts have been increasingly forgiving of defects in the application process for electronic surveillance warrants. As some of the recently decided insider-trading cases illustrate, this is a troubling trend likely to spur the increased use of wiretaps as a matter of course.[181]

IV. Recent Developments and the Weakening of Title III's Restrictive Provisions

When Title III was originally promulgated, Congress appeared to go to great lengths to balance properly privacy and law-enforcement interests. As discussed above, several layers of protection were added to prevent government-secured electronic surveillance orders from becoming commonplace and

176. 18 U.S.C. § 2515.

177. *See generally id.* §§ 2511-2522.

178. *See id.* § 2518(10)(a).

179. *See* United States v. Donovan, 429 U.S. 413 (1977); United States v. Giordano, 416 U.S. 505 (1974); United States v. Chavez, 416 U.S. 562 (1974).

180. *See* discussion *infra* Part IV.B.

181. *See* discussion *infra* Part IV.A.

from being overly intrusive.[182] Recent developments, however, appear to indicate that the balance is decisively tilting away from privacy protection in favor of a more broad-based use of wiretap surveillance by law enforcement. A review of recent insider-trading cases indicates some troubling trends: first, the apparent scope of the types of cases that could be investigated using covert electronic surveillance has become unbounded;[183] second, courts have steadily weakened the standard for suppression under Title III—in part by conflating Title III and Fourth Amendment analyses—in apparent contradiction to several Supreme Court cases dating to the 1970s.[184]

A. *Plain View, Predicate Offenses, and the Expanding Landscape of Wiretap Surveillance*

In several recent securities fraud prosecutions, the defendants have sought to suppress wiretap evidence by arguing that securities fraud is not a predicate offense under Title III.[185] To date, none of these challenges have been successful.[186] This recent case law presents a troubling trend resulting in what effectively amounts to a presumption of good faith on behalf of prosecuting authorities in the investigation of almost any crime. This presumption is nearly impossible to overcome so long as (1) probable cause exists to investigate wire fraud, mail fraud, money laundering, or racketeering activity, and (2) the desire to investigate a related non-Title III offense is openly acknowledged in the wiretap warrant

182. *See supra* Part III.

183. *See* discussion *infra* Part IV.A.

184. *See* discussion *infra* Part IV.B.

185. *See, e.g.*, United States v. Gupta, No. 11 Cr. 907 (JSR), 2012 U.S. Dist. LEXIS 45610, at *2 (S.D.N.Y. Mar. 26, 2012) (discussing that Gupta argued that insider trading is not governed by Title III); United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *8 (S.D.N.Y. Nov. 24, 2010) (noting that motions by Raj Rajaratnam and Danielle Chiesi make roughly the same arguments, including that securities fraud is not a predicate offense under Title III), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

186. *See Gupta*, 2012 U.S. Dist. LEXIS 45610, at *2 (stating that Judge Holwell's opinion in *Rajaratnam* explained how insider trading is "an offense as to which wiretapping is authorized under Title III" (citing *Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *19)).

affidavit.[187]

Perhaps the case most indicative of this recent trend is a decision made by Judge Richard Holwell in the prosecution of defendants Raj Rajaratnam and Danielle Chiesi.[188] In this case, both defendants sought to suppress the wiretap evidence obtained by federal prosecutors by arguing, *inter alia*, that securities fraud—the crime for which both defendants were indicted—was not a predicate offense.[189] In rejecting this argument, Judge Holwell found that probable cause existed to believe that the defendants were committing wire fraud and that the government acted in good faith in investigating this predicate offense.[190] As a result, the incidental interceptions of evidence indicative of a securities-fraud scheme were subject to the plain-view exception contained in § 2517(5), and therefore this evidence was not suppressed.[191] Although this conclusion is in some sense unsurprising given the statutory mandate of § 2517(5), the collateral consequences of the reasoning underpinning this conclusion may have long-ranging effect.

The defendants in the *Rajaratnam* case made three primary arguments seeking to suppress the wiretap intercepts on the basis that it was not a predicate offense: first, defendants argued that it was the securities fraud investigation, not the wire fraud investigation, that was the

187. *See, e.g.*, *Gupta*, 2012 U.S. Dist. LEXIS 45610, at *2-3. The court stated:

> So long as the Government acts in good faith with respect to informing the Court of the crimes it is investigating and learning of in connection with the wiretap, as Judge Howell [sic] and this Court conclude was done here, the Government is free to use evidence obtained from an authorized wiretap in the prosecution of a crime not listed in § 2516.

Id.

188. *See Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *1-8. Rajaratnam and Chiesi's convictions were later upheld on appeal, although the Second Circuit did not address this argument in its opinion. *See* United States v. Rajaratnam, 719 F.3d 139 (2d Cir. 2013).

189. *See Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *1-2.

190. *Id.* at *9-23.

191. *Id.*

government's primary purpose; second, even if securities fraud investigation was not the primary purpose, it was at least an anticipated consequence of electronic surveillance; and third, authorizing the interception of communications evidencing securities fraud would undermine congressional intent.[192]

The court rejected the defendants' first argument, stating that it "unrealistically assume[d] a gulf between" wire fraud and securities fraud.[193] Although the court recognized that securities fraud and wire fraud have different elements that the government must prove to secure a conviction, the court nevertheless noted that "unlikely is the insider trading scheme that uses no interstate wires."[194] In fact, the court recognized that "[s]ometimes the government even charges both kinds of fraud for the same core conduct."[195] This presents a troubling reality, however, in an ever more "connected" world. What the court noted about the relationship between securities fraud and wire fraud can also be said about the relationship between wire fraud and a laundry list of other offenses not specifically subject to electronic surveillance under Title III.

Although courts describe the federal mail and wire fraud statutes in different ways, a federal prosecutor must prove beyond a reasonable doubt five general elements in order to secure a conviction. The government must prove "that the defendant (1) used either mail or wire communications in the foreseeable furtherance, (2) of a scheme to defraud, (3) involving a material deception, (4) with the intent to deprive another of, (5) either property or honest services."[196] Nearly

192. *Id.* at *14.

193. *Id.*

194. *Id.* at *15.

195. *Id.* (citing H. Rep. 100-910 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6074; United States v. Carpenter, 484 U.S. 19, 28 (1987)).

196. Charles Doyle, *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law,* CONG. RESEARCH SERV. (July 21, 2011), http://www.fas.org/sgp/crs/misc/R41930.pdf [hereinafter Doyle, *Mail and Wire Fraud*]; *see also* United States v. Briscoe, 65 F.3d 576, 583 (7th Cir. 1995) (citing United States v. Ames Sintering Co., 927 F.2d 232, 234 (6th Cir. 1990) (per curiam)); United States v. Frey, 42 F.3d 795, 797 (3d Cir. 1994) (noting that "the wire fraud statute is identical to mail fraud statute except that it speaks of communications transmitted by wire."). The crime of wire fraud consists of several elements, notably (1) a scheme to defraud and, (2) the use of interstate wire communication to further the scheme. S*ee, e.g.*, United

every white-collar criminal offense has the capacity to meet this definition so long as the jurisdictional element—i.e., the use of a wire or mail communication—is satisfied.

Federal offenses that are distinct crimes but under certain circumstances could nevertheless also be prosecuted as wire fraud include: (1) the knowing submission of a false claim against the United States;[197] (2) conspiracies to defraud the United States;[198] (3) knowing and willfully making a material false statement on a matter within the jurisdiction of the federal government;[199] (4) securities and commodities fraud;[200] (5) fraud in foreign labor contracting;[201] (6) theft or bribery related to programs receiving federal funds;[202] (7) violations of the Foreign Corrupt Practices Act;[203] and (8) Medicare[204] and Medicaid[205] kickback schemes.[206] None of these offenses, however, are predicate offenses under Title III.[207]

The fact that the same primary conduct can serve as evidence in a prosecution under multiple federal criminal statutes is not unique to the wire fraud context. Judge Holwell, for example, noted in the *Rajaratnam* case that prosecutors had also named money laundering as a Title III predicate offense.[208] The main federal money laundering statute, 18

States v. Proffit, 49 F.3d 404, 406 n.1 (8th Cir. 1995) (citations omitted) (noting four elements); United States v. Hanson, 41 F.3d 580, 583 (10th Cir. 1994) (citations omitted) (noting two elements); United States v. Faulkner, 17 F.3d 745, 771 (5th Cir. 1994) (citations omitted) (noting two elements); United States v. Cassiere, 4 F.3d 1006, 1011 (1st Cir. 1993) (citation omitted) (noting three elements); United States v. Maxwell, 920 F.2d 1028, 1035 (D.C. Cir. 1990) (citations omitted) (noting two elements).

197. *See* 18 U.S.C. § 287 (2012).

198. *See id.* § 371.

199. *See id.* § 1001.

200. *See id.* § 1348.

201. *See id.* § 1351.

202. *See id.* § 666.

203. *See id.* 15 U.S.C. § 78dd-1-dd-3 (2012).

204. *See id.* 42 U.S.C. § 1320a-7b (2012).

205. *See id.*

206. For a discussion of the crimes listed in notes 197-205, s*ee generally* Doyle, *Mail and Wire Fraud*, *supra* note 196, at 14-23.

207. *See* 18 U.S.C. § 2516.

208. See United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *12-13 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013); *see also* 18 U.S.C. § 2516(1)(c).

U.S.C. § 1956,

> outlaws financial transactions involving the proceeds of other certain crimes—predicate offenses referred to as 'specified unlawful activities' (sometimes known as SUA)—committed or attempted (1) with the intent to promote further [SUA] offenses; (2) with the intent to evade taxation; (3) knowing the transaction is designed to conceal laundering of the proceeds; or (4) knowing the transaction is designed to avoid anti-laundering reporting requirements.[209]

There are three general categories of SUA offenses: state, foreign, and federal crimes.[210] Similar to wire fraud, many of these SUA offenses are not listed as offenses subject to electronic surveillance under Title III. For example, the list of SUA offenses include the following crimes not generally subject to investigation using wiretap surveillance: fraud by or against a foreign bank;[211] theft or bribery related to programs receiving federal funds;[212] crimes related to fraudulent bank entries;[213] fraud in federal credit union entries;[214] crimes related to Federal Deposit Insurance transactions;[215] and numerous environmental crimes.[216] There has also been recent consideration of naming tax evasion itself as a predicate

209. Charles Doyle, *Money Laundering: An Overview of 18 U.S.C. 1956 and Related Federal Criminal Law,* CONG. RESEARCH SERV. 2 (July 21, 2011), http://www.fas.org/sgp/crs/misc/RL33315.pdf [hereinafter Doyle, *Money Laundering*].

210. *See id.* at 4-5.

211. *See* 12 U.S.C. § 3101(7) (2012); *see also* 18 U.S.C. § 1956(c)(7)(B)(iii).

212. *See* 18 U.S.C. § 666; *see also id.* § 1956(c)(7)(D).

213. *See id.* § 1005; *see also id.* § 1956(c)(7)(D).

214. *See id.* § 1006; *see also id.* § 1956(c)(7)(D).

215. *See id.* § 1007; *see also id.* § 1956(c)(7)(D).

216. These include crimes under the Federal Water Pollution Control Act, 33 U.S.C. §§ 1251-1376 (2012), the Ocean Dumping Act, 33 U.S.C. §§ 1401-1445, 16 U.S.C. § 1447-1447f (2012), 33 U.S.C. §§ 2801-2805, the Act to Prevent Pollution from Ships, 33 U.S.C. §§ 1905-1915, the Safe Drinking Water Act, 42 U.S.C. §§ 300f-300j-26 (2012), and the Resources Conservation and Recovery Act, 42 U.S.C. §§ 6901-6992(k); *see also* 18 U.S.C. 1956(c)(7)(E).

offense for money laundering; the Financial Action Task Force, a global body set up to fight money laundering, recently added "serious tax crimes" to its list of predicate money laundering offenses.[217]

Most expansively, however, money laundering under § 1856 also includes in its list of SUA offenses, any crime that can constitute a predicate offense under the Racketeer Influenced and Corrupt Organizations ("RICO") Act.[218] Violations of RICO may also independently serve as a basis for electronic surveillance under Title III.[219] Regardless of whether RICO or money laundering is used as the gateway to a wiretap warrant, the list of RICO predicate offenses is staggering. Justice Scalia has derisively noted that the prosecutable offenses under RICO include "a laundry list of nearly every federal crime under the sun."[220] Thus, these four crimes—i.e., wire fraud, mail fraud, money laundering, and racketeering—all provide a backdoor into Title III for offenses that cannot otherwise be investigated using covert electronic surveillance.[221] Moreover, under most circumstances these

217. *See* David Jolly, *International Crackdown on Tax Crimes Intensifies*, N.Y. TIMES, Feb. 16, 2012, at B4, *available at* http://www.nytimes.com/2012/02/17/business/global/global-financial-task-force-to-take-on-tax-cheats.html?_r=0.

218. *See* 18 U.S.C. § 1956(c)(7)(A). For the RICO statute, *see* 18 U.S.C. §§ 1961-1968 (2012).

219. *See id.* § 2516(1)(c).

220. James v. United States, 550 U.S. 192, 223 (2007) (Scalia, J., dissenting).

221. The DOJ has specifically adopted this reading of the predicate offense requirement. *See* Brief for the United States of America at 55-56, United States v. Rajaratnam, 719 F.3d 139 (2d Cir. 2013) (No. 11-4416-cr), 2012 WL 1573547, at *55-56. They wrote:

> Insider trading violates various criminal statutes explicitly listed in Title III, including the wire fraud statute. In addition to wire fraud, Title III authorizes the interception of wire communications to seek evidence of money laundering. Both wire fraud and securities fraud are specified unlawful activities under the money laundering statute. Accordingly, certain financial transactions involving the proceeds of insider trading constitute money laundering. Title III also allows courts to authorize the use of wiretap recordings in the prosecution of crimes not listed

crimes can be the basis for nearly any white-collar criminal investigation and subsequent prosecution.

As noted above, although Congress provided for what amounts to a plain-view exception to the predicate offense requirement, it also provided protection against abuse of this exception.[222] Namely, a prosecutor must obtain court permission "as soon as practicable" in order to use wiretap evidence obtained incidentally when investigating a predicate offense.[223] In line with the legislative history of Title III, courts have largely adopted a "good faith" standard for determining whether to admit otherwise intercepted evidence.[224]

In the *Rajaratnam* case, Judge Holwell concluded that the government had acted in good faith, and not as a subterfuge for gathering evidence of securities fraud, because the government "candidly detailed the nature of the scheme for which wiretaps were sought."[225] "In other words," Judge Holwell clarified, "the government made quite clear that it wanted to use wiretaps to investigate an insider trading conspiracy, and that the evidence would likely uncover evidence of wire fraud[,] money laundering . . . and securities fraud . . . ."[226] This reasoning results in the perverse notion that the more blatant the government is in disclosing that its primary intent is to seek evidence of a non-predicate offense, the more likely the government will be in successfully using this evidence.[227] The court implicitly concluded that, so long as probable cause exists to investigate a predicate offense, it did not matter whether investigating a non-predicate offense was the government's primary goal.[228] The Second Circuit recently embraced this

in the statute.

Id. (internal citations omitted).

222. *See supra* Part III.B.1.

223. 18 U.S.C. § 2517(5).

224. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *11-15 (S.D.N.Y. Nov. 24, 2010) (compiling cases), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

225. *Id.* at *12.

226. *Id.* (citation omitted).

227. *See id.* at 12-13.

228. *Id.*

reality with open arms. The court in *United States v. Goffer*,[229] concluded that a representation that the government expected to uncover evidence of securities fraud in a wiretap application "ensured that the wiretaps were not obtained as a 'subterfuge' or to surreptitiously investigate crimes other than those about which they informed the court."[230] This statement seems to reveal that the Second Circuit understood the government to be investigating securities fraud when applying for the wiretap warrant at issue.

Although the Second Circuit in *Goffer* did not explain the logic behind this conclusion, Judge Holwell in *Rajaratnam* did. In rejecting one argument made by the Defendants, Judge Holwell explained in a footnote that:

> The issuing judges did not know and could not have predicted that the government would ultimately charge the defendants with only securities fraud, not wire fraud or money laundering. But the government should not be required to charge the crime for which it obtains wiretap authorization. Although charging a defendant with the crime for which wiretapping was authorized is some evidence of the government's good faith, the converse is not necessarily true. The government's charging decisions depend on a variety of factors. That it decides not to charge a defendant with a crime for which it previously sought wiretap authorization does not imply it had no legitimate reason for a wiretap to begin with.[231]

Judge Holwell then went on to reject the defendants' second argument—i.e., that the securities fraud evidence was not obtained "incidentally"—because the government

229. No. 11-3591-cr(L), 2013 WL 3285115, at *1 (2d Cir. July 1, 2013).

230. *Id.* at *5.

231. *Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *13 n.5 (internal citations omitted).

anticipated its discovery.[232] Despite recognizing that earlier cases had used the word "inadvertent" in dicta, the court dismissed this reading of the statute noting that the legislative history instead used the word "incidental" and concluded that "recent authority has implicitly rejected [the 'inadvertent'] gloss on the standard."[233] This interpretation adopts the same standard applicable to the plain-view exception under the Fourth Amendment. In *Horton v. California*,[234] the Supreme Court held that evidence found in plain view, the incriminating nature of which is immediately apparent, need not be suppressed where the investigating officers have a valid search warrant for the premises, despite the fact that the discovery of this evidence was not "inadvertent."[235] In other words, the plain-view exception does not require that the discovery of the evidence in plain view be an unexpected consequence of the otherwise valid search.[236]

In practical effect, the standard of good faith adopted by the *Rajaratnam* court results in a presumption of good faith on behalf of the government that a defendant will rarely, if ever, be able to overcome.[237] A criminal defendant is not likely to ever have access to subjective evidence of the intent of investigating authorities. Therefore, in nearly all instances, only objective evidence may be relied upon to attack the government's good faith.[238] The defendants in *Rajaratnam*

232. *See* i*d.* at *14-19.

233. *Id.* at *17 (citing United States v. Marion, 535 F.2d 697, 701 (2d Cir. 1976); United States v. Masciarelli, 558 F.2d 1064, 1067 (2d Cir. 1977); *In re* Grand Jury Subpoena Served on John Doe, 889 F.2d 384, 388 (2d Cir. 1989); United States v. Wager, No. 00 Cr. 629 (TPG), 2002 U.S. Dist. LEXIS 17739, at *2 (S.D.N.Y. Sept. 19, 2002); United States v. McKinnon, 721 F.2d 19, 22-23 (1st Cir. 1983)).

234. 496 U.S. 128 (1990).

235. *See id.* at 133-37.

236. *See id.*

237. *But cf.* United States v. Gigante, 538 F.2d 502, 505 (2d Cir. 1976) (rejecting argument that suppression for failing to abide by the sealing provisions of Title III was draconian and unwarranted absent proof of actual tampering, in part because of the fear that editing and modification of wiretap evidence "can rarely, if ever, be detected").

238. *See, e.g.,* United States v. Rajaratnam, 719 F.3d 139, 154 (2d Cir. 2013) ("Subjective intent, after all, is often demonstrated with objective evidence.").

presented the court with two pieces of objective evidence: first, the government did not charge either defendant with a Title III predicate offense; and second, the government knew that it was likely to uncover incriminating evidence of securities fraud.[239] Taken together, these two pieces of evidence present, at the very least, a prima facie case that the government was engaging in a subterfuge search and never intended its investigation of wire fraud to be its primary objective. Even this evidence, however, was insufficient in the court's eyes to suppress the fruits of the wiretap warrant.[240] This is troubling because these two pieces of evidence will often be the only objective indication of the government's intent a defendant is likely to have. Taking this conclusion—along with the backdoor route into Title III provided by investigations into mail fraud, wire fraud, money laundering, and racketeering—the flood gates to investigating non-Title III offenses are wide open. As long as the wiretap applicant readily acknowledges that an otherwise impermissible wiretap investigation is related to a permissible wiretap investigation, it will be nearly impossible for a defendant to prove bad faith.

Other courts have adopted similar reasoning. During the prosecution of Rajat Gupta, the former head of the consulting company McKinsey & Co., and a co-conspirator of Raj Rajaratnam and Danielle Chiesi, Gupta's lawyers made arguments nearly identical to that of Rajaratnam and Chiesi.[241] The court, however, fully accepted the reasoning of Judge Holwell.[242] In the recent case of *United States v. Levy*,[243] another judge in the Southern District of New York adopted similar reasoning.[244] Most recently, the Second Circuit has

239. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *12-13 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

240. *Id.* at *19.

241. United States v. Gupta, No. 11 Cr. 907 (JSR), 2012 U.S. Dist. LEXIS 45610, at *2 (S.D.N.Y. Mar. 26, 2012) ("Gupta offers no arguments different from the arguments Judge Holwell considered in the *Rajaratnam* case. He argues instead that Judge Holwell's conclusions are in error.").

242. *Id.*

243. No. 1:(S5) 11 Cr. 62 (PAC), 2012 WL 5830631, at *1 (S.D.N.Y. Nov. 16, 2012).

244. *See id.* at *3-10.

expressly put its stamp of approval on this reasoning.[245] This emerging trend is likely to encourage government authorities to continue to expand the use of wiretaps in white-collar investigations not specifically listed under Title III.

B. United States v. Giordano *and the Movement away from Strict Compliance with the Necessity Requirement*

Another troubling trend has emerged in the context of Title III: courts are relaxing the statutory requirements of substantive wiretap application provisions—most importantly, the necessity requirement. As a result, courts rarely suppress evidence on the basis of the government's failure to strictly abide by § 2518, which requires a "full and complete statement" by the applicant as to why a wiretap is necessary.[246] For example, within the Second Circuit, there have only been two cases in which wiretap evidence was suppressed based on the government's failure to prove necessity, and one of those cases was later reversed on appeal.[247] This development seemingly contradicts a line of cases decided by the Supreme Court in the 1970s. Rather than applying the suppression standard expressed in *United States v. Giordano*[248] and its progeny, courts have superimposed the Fourth Amendment standard expressed in *Franks v. Delaware*[249] onto the statute-based necessity requirement. By ignoring the mandate of *Giordano*, these same courts have permitted wiretap applicants a 'second bite at the apple' that was not imagined within the framework of the statutory scheme.

245. "When the government investigates insider trading for the bona fide purpose of prosecuting wire fraud, it can thereby collect evidence of securities fraud, despite the fact that securities fraud is not itself a Title III predicate offense." United States v. Goffer, No. 11-3591-cr(L), 2013 WL 3285115, at *5 (2d Cir. July 1, 2013) (quoting *Rajaratnam*, 2010 WL 4867402, at *6).

246. 18 U.S.C. § 2518(1)(c) (2012).

247. *See Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *89 n.26 (citing United States v. Lilla, 699 F.2d 99 (2d Cir. 1983); United States v. Concepcion, No. 07 CR 1095 (SAS), 2008 U.S. Dist. LEXIS 51386, at *1 (S.D.N.Y. June 30, 2008), *rev'd* 579 F.3d 214 (2d Cir. 2009)).

248. 416 U.S. 505 (1974).

249. 438 U.S. 154 (1978).

In *Giordano*, the Supreme Court held that "[t]he mature judgment of a particular, responsible Department of Justice official is interposed as a critical precondition to any judicial order" permitting the use of a wiretap.[250] Therefore, "primary or derivative evidence secured by wire interceptions pursuant to a court order issued in response to an application which was, in fact, not authorized by one of the statutorily designated officials must be suppressed."[251] In reaching this conclusion, the Court stated that the issue of suppression under Title III "does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of Title III."[252] The Court then noted that § 2515 mandates the exclusion of wiretap evidence form judicial proceedings "if the disclosure of that information would be in violation of this chapter," and that § 2518(10)(a) in turn supplies three statutory grounds for suppression.[253] These three grounds for suppression include: "(i) if 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."[254]

250. *Giordano*, 416 U.S. at 515-16. The Court reasoned that this requirement was intended to hold certain public officials politically accountable. *See id.* at 516-23. The specific statute in place at the time of the *Giordano* decision was later amended to include, in addition to certain DOJ officials requiring Senate confirmation, "[t]he 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 or National Security Division specially designated by the Attorney General." *See* 18 U.S.C. § 2516(1). As the D.C. Circuit Court of Appeals stated in *United States v. Anderson*, 39 F.3d 331 (D.C. Cir. 1994), *abrogated by Richardson v. United States*, 526 U.S. 813 (1999), under the current statute "[i]t would perhaps be more accurate, then, to attribute to Congress the purpose of limiting such authority to identifiable officials in positions of trust." *Anderson*, 39 F.3d at 339 n.6.

251. *Giordano,* 416 U.S. at 508.

252. *Id.* at 524; *see also* Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001) ("Congress made [Title III] the primary vehicle by which to address violations of privacy interests in the communications field. . . . All such constitutional questions are pretermitted.").

253. *Giordano*, 416 U.S. at 524 (quoting 18 U.S.C. § 2515 (2012)) (internal quotation marks omitted).

254. 18 U.S.C. § 2518(10)(a).

In interpreting these three grounds for suppression, the Court determined "that paragraphs (ii) and (iii) must be deemed to provide suppression for failure to observe some statutory requirements that would not render interceptions unlawful under paragraph (i)."[255] This, however, does not mean "that no statutory infringements whatsoever are also unlawful interceptions within the meaning of paragraph (i)."[256] Therefore, although subsection (i) undoubtedly permits suppression for violations of the Fourth Amendment, it also permits suppression for certain statutory violations as well.[257] The Court then set forth the governing standard for what constitutes an "unlawful" interception under the first prong of § 2518(10)(a):

> [W]e think Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device . . . [Where a requirement] was intended to play a central role in the statutory scheme[,] . . . suppression must follow when it is shown that this statutory requirement has been ignored.[258]

In reconciling legislative history by indicating that § 2518(10)(a) was meant to "largely reflect[] existing law" but at the same time "serve to guarantee that the standards of [Title III] will sharply curtail the unlawful interception of wire and oral communications," the Court held that "it would not extend existing search-and-seizure law for Congress to provide for the suppression of evidence obtained in violation of explicit statutory prohibitions."[259]

255. *Giordano*, 416 U.S. at 527.
256. *Id.*
257. *Id.*
258. *Id.* at 527-28.
259. *Id.* at 528-29 (internal quotation marks and citations omitted).

The Supreme Court revisited the issue of suppression under Title III in the same year that *Giordano* was decided. In *United States v. Chavez*,[260] the Court concluded that evidence derived from a wiretap need not be suppressed where the Attorney General authorizes the wiretap application but where the application and order both incorrectly identify an Assistant Attorney General as the authorizing official.[261] "Under § 2515, suppression is not mandated for every violation of Title III . . . ."[262] In *Chavez*, "the misidentification of the officer authorizing the wiretap application did not affect the fulfillment of any of the reviewing or approval functions required by Congress."[263] Rather, the requirement that the authorizing official be named was meant to serve a reporting requirement and to hold this official publicly responsible for the wiretap; it did not provide an essential or functional role in protecting against unwarranted wiretap use.[264] In dicta, the Court concluded that despite the outcome of this particular case, "*strict adherence* by the Government to the provisions of Title III would nonetheless be more in keeping with the responsibilities Congress has imposed upon it when authority to engage in wiretapping or electronic surveillance is sought."[265] The Court has since "reemphasize[d]" this.[266]

Both *Giordano* and *Chavez* set forth the applicable framework for suppression under Title III, and only one other case has been considered by the Supreme Court under this framework.[267] In *United States v. Donovan*, the Court held that

260. 416 U.S. 562 (1974).

261. *Id.* at 565.

262. *Id.* at 575.

263. *Id.*

264. *See id.* at 577-79.

265. *Id.* at 580 (emphasis added).

266. *See* United States v. Donovan, 429 U.S. 413, 439-40 (1977).

267. In 1974, the Court also decided *United States v. Kahn*, 415 U.S. 143 (1974), which held that the government's failure to name a party in the application whose conversation was likely subject to interception did not require suppression where the government did not have probable cause to believe that the un-named person was committing the offense under investigation. *See id.* at 155. In other words, "Title III requires the naming of a person in the application or interception order only when the law enforcement authorities have probable cause to believe that that individual is 'committing the offense' for which the wiretap is sought." *Id.* This decision,

the government's failure to strictly adhere to the following non-substantive provisions of Title III does not make subsequent intercepts "unlawful" and therefore does not require suppression: (1) the identification of all those likely to be heard during the intercept, as required under § 2518(1)(b)(iv)[268]; and (2) the "duty to inform the judge of all identifiable persons whose conversations were intercepted," as required pursuant to § 2518(8)(d).[269] In reaching this conclusion the Court continued to place an emphasis on the statutory preconditions that help both the Justice Department and the issuing judge in determining whether a wiretap is appropriate in a given case. In other words, emphasis is placed on those provisions that were "intended to serve as an independent restraint on resort to the wiretap procedure."[270] For example, the Court stated that the intercept at issue in *Chavez* "was lawful because the Justice Department had performed its task of prior approval, and the instant intercept is lawful because the application provided sufficient information to enable the issuing judge to determine that the statutory preconditions were satisfied," regardless of whether or not certain people were identified in the application.[271] To a lesser degree, the Court has also placed emphasis on the government's intent in failing to abide by the statutory provisions,[272] although the Court has never expanded

however, focused more on the statutory text of §§ 2518(1)(b)(iv) and 2518(4)(a), not on Title III's suppression provision. *See generally id*. at 152-58. Similarly, the Court briefly discussed suppression in *Scott v. United States*, 436 U.S. 128 (1978), but ultimately did not need to interpret § 2518(10)(a) because it concluded that there was no statutory violation of the minimization requirement. *See id*. at 142-43.

268. *See Donovan*, 429 U.S. at 435-37.

269. *Id*. at 438.

270. *Id*. at 439; *see also* United States v. Gigante, 538 F.2d 502, 505 (2d Cir. 1976) (finding that the requirement of judicial sealing immediately upon the expiration of the authorizing order was designed to limit the use of intercept procedures and was therefore central to the statutory scheme and rejecting argument that suppression for failing to abide by this requirement was unwarranted and draconian in light of the "carefully planned strictures on the conduct of electronic surveillance").

271. *Donovan*, 429 U.S. at 436.

272. *See, e.g.*, *id*. at 436 n.23. Here, the court stated:

> There is no suggestion in this case that the Government agents knowingly failed to identify [defendants] for the

upon this.[273]

The Supreme Court has not revisited the issue of suppression under Title III since the 1970s. Despite the fact that the Court's suppression analysis focuses on whether each statutory requirement is directly related to limiting the use of wiretaps, lower federal courts have recently weakened this standard. In the context of the "necessity" requirement, several circuit courts have adopted a *Franks*[274] analysis in determining whether wiretap evidence should be suppressed.[275] Similarly, the district court in the *Rajaratnam* prosecution used this analysis, and the Second Circuit later affirmed.[276] In the context of the necessity requirement, a *Franks* analysis requires suppression where the defendant, after an evidentiary hearing, can prove (1) that a misstatement or omission regarding the issue of necessity in the government's application was the result of a "deliberate falsehood" or "reckless disregard for the truth"; and (2) that the omitted or erroneous information was material to the district court's finding of necessity.[277]

> purpose of keeping relevant information from the District Court that might have prompted the court to conclude that probable cause was lacking. If such a showing had been made, we would have a different case.

Id.

273. *But cf.* Scott v. United States, 436 U.S. 128, 139 n.13 (1978) (discussing the role of motive under a Fourth Amendment suppression analysis).

274. A *Franks* analysis refers to the case Franks v. Delaware, 438 U.S. 154 (1978). *Franks* was decided on constitutional grounds. *See id.* at 155-56.

275. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 549-51 (D.C. Cir. 2010); United States v. Rice, 478 F.3d 704, 716-18 (6th Cir. 2007) (Bell, C.J., dissenting); United States v. Shryock, 342 F.3d 948, 976-77 (9th Cir. 2003); United States v. Green, 175 F.3d 822, 828 (10th Cir. 1999); United States v. Miller, 116 F.3d 641, 663-65 (2d Cir. 1997); United States v. Guerra-Marez, 928 F.2d 665, 669-71 (5th Cir. 1991); United States v. Cole, 807 F.2d 262, 267-68 (1st Cir. 1986); United States v. Ippolito, 774 F.2d 1482, 1485 (9th Cir. 1985). Another circuit has expressly refrained from deciding this issue. See United States v. Heilman, 377 F. App'x 157, 177 (3d Cir. 2010).

276. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *69-94 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

277. *See, e.g.*, United States v. Rajaratnam, 719 F.3d 139, 146 (2d Cir. 2013) (quoting United States v. Canfield, 212 F.3d 713, 717–18 (2d Cir. 2000);

Surprisingly, almost none of the cases that have used this standard have discussed it within the context of the suppression analysis from *Giordano* and its progeny. The leading case on this issue in the First Circuit, for example, cites *Giordano* once, but does so for a proposition unrelated to the issue of suppression.[278] Likewise, the first case from the Ninth Circuit applying this standard only mentions *Giordano* once in passing,[279] while at least three other cases from that circuit applying this standard fail to directly cite to *Giordano* at all.[280] Similar statements can be made with respect to decisions from the Fifth Circuit,[281] the Second Circuit,[282] the Third Circuit,[283]

see also United States v. Small, 423 F.3d 1164, 1172 (10th Cir. 2005) ("Under [the *Franks*] standard, the defendant must show that any misstatements were made knowingly, intentionally, or recklessly, and that the erroneous information was material to the district court's finding of necessity.").

278. *See Cole*, 807 F.2d at 267-68 (discussing *Giordano* in relation to finding that a judge needs to make prior to authorizing a wiretap).

279. *See Ippolito*, 774 F.2d at 1486. The court in *Ippolito* did state, however, that

> [b]ecause the challenged statements in the wiretap application at issue deal with the necessity or alternative methods requirement for obtaining a wiretap, it is first necessary to determine whether necessity is an essential, congressionally warranted *requirement*, and not merely a factor meant to inform the issuing judge of the difficulties involved in the use of conventional techniques.

Id. at 1485 (quoting United States v. Pacheco, 489 F.2d 554, 565 (5th Cir. 1974)) (internal quotation marks omitted). This sounds in some respects similar to a *Giordano* analysis.

280. *See Shryock*, 342 F.2d at 976-77; United States v. Blackmon, 273 F.3d 1204, 1207 (9th Cir. 2001); United States v. Bennett, 219 F.3d 1117, 1121-26 (9th Cir. 2000); *see also* United States v. Simpson, 813 F.2d 1462, 1472-73 (9th Cir. 1987) (not citing *Giordano* and concluding that "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.").

281. *See* United States v. Guerra-Marez, 928 F.2d 665, 669-71 (5th Cir. 1991) (not citing *Giordano*).

282. *See* United States v. Miller, 116 F.3d 641, 663-65 (2d Cir. 1997) (discussing the necessity requirement without a *Giordano* analysis); United States v. Torres, 901 F.2d 205, 231 (2d Cir. 1990) (discussing suppression for failure to abide by the necessity requirement but without discussing *Giordano*), *abrogation recognized by* United States v. Al Jaber, 436 F. App'x 9, 12 (2d Cir. 2011); *see also* United States v. Bianco, 998 F.2d 1112, 1126-27

the Sixth Circuit,[284] the D.C. Circuit,[285] and the Tenth Circuit.[286] The application of *Giordano* to the necessity requirements of Title III was directly addressed by the Second Circuit in *Rajaratnam*, with the court ultimately concluding that *Giordano* did not preclude the application of a *Franks* analysis to the necessity requirement.[287] The Court reached this conclusion, however, largely by relying on previous case law that did not fully analyze the application of *Giordano*.[288]

At least one circuit has recognized the heavier burden that Title III places on the government vis-à-vis the Fourth Amendment. In *United States v. Rice*,[289] the court adhered more closely to the *Giordano* line of reasoning. The Sixth Circuit, after citing to *Giordano*, stated that "[b]ecause the necessity requirement is a component of Title III, and because suppression is the appropriate remedy for a violation under Title III, where a warrant application does not meet the necessity requirement, the fruits of any evidence obtained through that warrant must be suppressed."[290] The court then

(2d Cir. 1993) (discussing the application of the *Franks* analysis to Title III's "roving" wiretap requirements, and citing to § 2518(10)(a) but failing to mention *Giordano*), *abrogation recognized by* United States v. Galpin, No. 11-4808-cr., 2013 WL 3185299, at *7 (2d Cir. 2013).

283. *See* United States v. Heilman, 377 F. App'x 157, 177 (3d Cir. 2010) (noting that most circuits have adopted *Franks* analysis in the context of the necessity requirement, refusing to address the issue because the defendant had failed to even make a preliminary showing under *Franks*, and not mentioning *Giordano*).

284. *See* United States v. Stewart, 306 F.3d 295, 304-05 (6th Cir. 2002) (stating that *Franks* applied to challenges based on the necessity requirement without discussion and without citing *Giordano*); *see also* United States v. Poulsen, 655 F.3d 492, 503-05 (6th Cir. 2011) (same); United States v. Rice, 478 F.3d 704, 716-18 (6th Cir. 2007) (Bell, C.J., dissenting) (same).

285. *See* United States v. Maynard, 615 F.3d 544, 549-51 (D.C. Cir. 2010) (applying *Franks* to a necessity challenge without citing to *Giordano* or its progeny).

286. *See* United States v. Small, 423 F.3d 1164, 1172-73 (10th Cir. 2005) (failing to cite *Giordano*); *see also* United States v. Green, 175 F.3d 822, 828-29 (10th Cir. 1999) (same).

287. United States v. Rajaratnam, 719 F.3d 139, 152 (2d Cir. 2013).

288. *Id.* at 151-52 (citing United States v. Bianco, 998 F.2d 1112, 1126 (2d Cir. 1993); United States v. Miller, 116 F.3d 641 (2d Cir. 1997)); *see also id.* at 152 n.16 (collecting cases).

289. 478 F.3d 704 (6th Cir. 2007).

290. *Id.* at 710.

performed a *Franks* analysis and "reformed [the warrant application] for its factual deficiencies," by simply ignoring the false information.[291] Importantly, however, the *Rice* court then went on to reject the Government's argument that the wiretap evidence, even if obtained in violation of Title III, should nevertheless be admitted based on the good faith exception of *United States v. Leon.*[292] Rather, the court concluded that "the good-faith exception to the warrant requirement is not applicable to warrants obtained pursuant to Title III" based upon both the statute's text and legislative history.[293] On this point, the court reasoned: (i) "[t]he statute is clear on its face and does not provide for any exception"; (ii) *Leon* was decided sixteen years after the passage of Title III and therefore "Congress obviously could not know that Fourth Amendment search and seizure law would embrace a good-faith exception"; and (iii) in contrast to the exclusionary rule "Congress has already balanced the social costs and benefits and has provided that suppression is the sole remedy for violations of the statute."[294] Although the court still utilized a *Franks* analysis

291. *Id.* at 711.

292. 468 U.S. 897 (1984); *Rice*, 478 F.3d at 711-14.

293. *Rice*, 478 F.3d at 711. At least three other circuits have reached a different conclusion. *See* United States v. Brewer, 204 F. App'x 205, 208 (4th Cir. 2006); United States v. Moore, 41 F.3d 370, 376-77 (8th Cir.1994); United States v. Malekzadeh, 855 F.2d 1492, 1497 (11th Cir. 1988); *see also* United States v. Solomonyan, 451 F. Supp. 2d 626, 628 (S.D.N.Y. 2006); United States v. Mullen, 451 F. Supp. 2d 509, 530-31 (W.D.N.Y. 2006). In *United States v. Heilman*, 377 F. App'x 157 (3d Cir. 2010), the Third Circuit made note of this split authority and specifically declined to decide whether there was a good-faith exception to the necessity requirement. *Id.* at 185 n.21.

294. *Rice,* 478 F.3d at 713. In another case, the Ninth Circuit declared that there is a two-step approach to reviewing necessity determinations, the first step of which entails "review[ing] de novo whether the application for wiretapping was submitted in compliance with 18 U.S.C. § 2518(1)(c)." United States v. Garcia-Villalba, 585 F.3d 1223, 1228 (9th Cir. 2009) (quoting United States v. McGuire, 307 F.3d 1192, 1197 (9th Cir. 2002)). This standard, however, appears only to apply where only the facial sufficiency of the warrant application is challenged and not its factual validity. *See* United States v. Rivera, 527 F.3d 891, 898 (9th Cir. 2008) ("In reviewing whether an affidavit contains a full and complete statement of facts in compliance with § 2518(1)(c), we assess whether the affidavit attests that adequate investigative tactics were exhausted before the wiretap order was sought or that such methods reasonably appeared unlikely to success or too dangerous.") (reaffirming United States v. Ippolito, 774 F.2d 1482 (9th Cir. 1985)); *see also Garcia-Villalba*, 585 F.3d at 1227-35 (not presenting a

for the necessity requirement, its reasoning on the issue of a good-faith exception is more closely aligned with the reasoning underpinning *Giordano*.[295]

Although at least one court has shown hints of adopting a more *Giordano*-like analysis, the Sixth Circuit's decision in *Rice* failed to fully repudiated the applicability of *Franks* to the necessity requirement. Applying a *Franks* analysis to the necessity requirement shifts the burden of proving necessity away from the government and onto the defendant challenging the warrant: defendants must now prove falsity or omission, and that the information is material. For example, courts have consistently concluded that where the government applies for an electronic surveillance order, it "must overcome the statutory presumption against granting a wiretap application by showing necessity."[296] In other words, the government has the burden of establishing the necessity of a wiretap to its investigation. But, applying a *Franks* analysis to the necessity requirement has the effect of taking the burden of proof on the issue of necessity away from the government. Under *Franks*, a defendant has the burden of first proving the knowing, intentional, or reckless falsity of the affidavit, and then they have the additional burden of proving that this false or omitted information was material to the court's determination of

challenge to the factual statements in the warrant application); *McGuire*, 307 F.3d at 1197 (same).

295. For example, the argument that *Leon* is not applicable to Title III because it was decided years after Title III's adoption can also be applied to *Franks*. *See* Reply Brief for Defendant-Appellant at 8-9, United States v. Rajaratnam, No. 11-4416-cr, 2013 WL 3155848, at *1 (2d Cir. June 24, 2013) (No. 11-4416-cr), 2012 WL 1903399, at *8-9 ("*Giordano* predates *Franks* because Title III predates *Franks*. And that means that the Congress that adopted Title III could not possibly have intended for its straightforward statutory text to be so sweepingly countermanded by a *Franks* doctrine of which it had never heard."). This argument, however, has been rejected by the Second Circuit. *See Rajaratnam*, 719 F.3d at 152; *see also United States v. Bianco*, 998 F.2d 1112, 1126 (2d Cir. 1993).

296. *Ippolito*, 774 F.2d at 1486 (citations omitted). This is a different question from the question of who has the burden of proof in overturning a district court order granting a wiretap warrant after the court has made a finding of necessity. *See, e.g.*, United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *87 (S.D.N.Y. Nov. 24, 2010) (citing Franks v. Delaware, 438 U.S. 154, 155-56 (1978)), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

necessity.[297] Thus, the government can secure a wiretap warrant by recklessly or intentionally failing to provide a "full and complete statement" establishing necessity and then shift the burden to the defendant to essentially disprove necessity based upon what a "full and complete statement" would otherwise reveal. This weakens the statutory purpose of the necessity requirement, which is to discourage use of wiretaps as a matter of course. This burden shift is thus likely to aggravate the trend towards increased use of wiretaps by law enforcement.

V. Re-Establishing Privacy as a Cardinal Principle Through Vigorous Judicial Enforcement of Title III's Substantive Requirements

With the expanded use of wiretaps in white-collar prosecutions, it becomes more important than ever for the judiciary to act as a bulwark against prosecutors seeking to engage in covert electronic surveillance beyond what Congress sought to permit. By more vigorously enforcing the requirements of Title III that are meant to limit the use of wiretaps, courts can rebalance privacy and law-enforcement concerns more in line with congressional intent. Several recent developments in white-collar criminal prosecutions indicate two important changes are needed. First, courts must more strictly enforce the predicate offense requirement by refocusing on the limitations imposed on use of the plain-view exception. Courts can accomplish this through closer supervision of the "subsequent application" process or, alternatively, courts could allow criminal defendants to more easily challenge the government's good faith application of the plain-view exception through an evidentiary hearing or by adopting a burden-shifting analysis. Second, courts must hold the government to its burden of establishing necessity through strictly enforcing the government's obligation to provide a "full and complete statement" of investigatory facts indicating that a wiretap is necessary in a given case. Courts must reject the continuing use of a constitutionally-based *Franks* analysis to the necessity

297. *See, e.g.*, *Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *70.

requirement because this analysis weakens statutory protections. In reasserting its authority by adopting these changes, the judiciary can once again buttress against excessive wiretap use by prosecutors as Congress originally intended when it enacted Title III.

A. *Restraining the Plain-View Exception to the Predicate Offense Requirement*

A number of statutory requirements contained in Title III are specifically meant to discourage the use of wiretaps as a matter of course by law enforcement. The predicate offense requirement is one of these requirements.[298] As discussed above, however, the predicate offense requirement, along with its restrictive force, is in danger of becoming a dead letter.[299] In order to breathe new life into this requirement's ability to adequately protect privacy interests, the plain-view exception must be limited in some manner. To appropriately achieve this limitation, judicial supervision over wiretap investigations must be increased or, alternatively, after some minimal showing by the defendant, the burden must be placed on the government to justify its assertion of good faith where it seeks to use Title III's plain-view provision.

1. The Judicial Supervision Approach

One possible avenue to appropriately limit excessive use of wiretaps would be to increase judicial supervision over the ongoing wiretap investigation. This can be done fully in line with the statutory text, but several hurdles exist that make this approach unlikely to succeed.

First, it must be noted that the plain-view exception to the predicate offense requirement is statutorily based.[300] As such, it cannot be interpreted so narrowly as to be effectively read out of the statute itself. This does not mean, however, that the

298. *See* 18 U.S.C. § 2516 (2012).
299. *See supra* Parts III.B.1, IV.A.
300. *See* 18 U.S.C. § 2517(5).

use of this exception cannot be restricted at all. Congress itself thought that certain restrictions were appropriate by providing that any "plain view" evidence obtained during a wiretap investigation, if it is to be used at trial, must be brought to the a judge's attention "as soon as practicable."[301] Congress further believed that this subsequent application should establish the following:

> [i] that the original order was lawfully obtained, [ii] that [the original order] was sought in good faith and not as a subterfuge search, and [iii] that the [otherwise intercepted] communication was in fact incidentally intercepted during the course of a lawfully executed order.[302]

Courts could more appropriately enforce this provision in accordance with congressional intent by placing increased emphasis on the requirement that an investigative officer apply to use this evidence in a subsequent proceeding "as soon as practicable." By using the phrase "as soon as practicable," Congress implicitly suggested that the timing of this application was an important consideration.[303] Restricting the time frame in which such an application can be made would both fully comply with the statutory mandate and allow courts greater supervision over ongoing wiretap intercepts.

Close judicial supervision of ongoing electronic surveillance was specifically envisioned by Congress.[304] In passing Title III, Congress made an explicit congressional finding that "[t]o safeguard the privacy of innocent persons, the interception of [protected] communications . . . should remain under the control and supervision of the authorizing court."[305] This same

301. *See id.*

302. S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2189.

303. *See* 18 U.S.C. § 2517(5).

304. *See, e.g.*, United States v. Gigante, 538 F.2d 502, 503 (2d Cir. 1976) ("Congress, in enacting Title III . . . prescribed specific and detailed procedures to ensure careful judicial scrutiny of the conduct of electronic surveillance and the integrity of its fruits.").

305. Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968,

intent is shown in other statutory provisions of Title III, such as the re-authorization and extension provisions of §§ 2518(1)(f)[306] and 2518(5).[307]

Under the increased judicial supervision approach, although no bright-line rule would need to be adopted, a subsequent application to use evidence obtained by wiretap at trial should be submitted within a period of a few days. By permitting increased judicial supervision such as this, a judge can more accurately determine whether Title III is being used as a mere subterfuge to investigate a non-Title III offense. Put differently, being presented with the "plain view" evidence derived from wiretap intercepts on an ongoing basis allows a court to make a more reasoned determination of whether the primary focus of an investigation is on a Title III predicate offense or on a non-Title III offense. For example, if a wiretap intercepts troves of evidence concerning insider trading, but only very limited evidence of wire fraud, a judge is in a better position to determine whether wire fraud is being used as a mere gateway to investigate insider trading. In this situation, a judge may appropriately decide that the securities fraud investigation is the primary purpose of the wiretap investigation and revoke the issued warrant or refuse to extend it.

There are several major drawbacks to this approach. First, and perhaps most importantly, as Judge Holwell noted in the *Rajaratnam* case, the evidence used to prosecute wire fraud and the evidence used to prosecute a non-predicate offense, such as securities fraud, is often one and the same.[308] There is rarely a clear distinction between evidence indicative of securities fraud scheme that is carried out over interstate wires and evidence indicative of wire fraud. It would likely be difficult for a judge to discern the government's true intent at this stage of the investigation. It is not until textual, objective clues emerge later on that the government's investigatory

Pub. L. No. 90-351, tit. III, § 801(d), 82 Stat. 197, 211 (1968).

306. *See* 18 U.S.C. § 2518(1)(f).

307. *See* 18 U.S.C. § 2518(5).

308. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *19 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

intent becomes clearer.

There are also other problems with this approach that would likely undercut its effectiveness. For instance, allowing only a short period of time between intercept and the subsequent application to use this evidence means that the subsequent application would, in most cases, be made prior to an indictment. Therefore, this subsequent application would be submitted *ex parte* and the suspect would not have an adequate opportunity to contest it prior to it being approved by a court. Although this raises serious due process concerns, there may be ways that these concerns may be avoided or minimized. One possible approach would be to allow a challenge to this subsequent application after it has been approved. This way, the judicial approval of the subsequent application would act much like a typical search warrant. But because a judge's decision that is not based on a strict question of law is generally afforded considerable deference on review, this decision would likely be given a presumption of validity and the burden would be on the defendant to attack its veracity in some regard. A defendant would therefore attack this approval in the same or a similar manner as the defendants in *Rajaratnam* did, although such defendants would have to overcome a higher burden due to the presumption of validity afforded to this earlier decision. Another possible disadvantage to this approach is that it blurs the line between the prosecution and the judiciary. Courts are often apprehensive to closely scrutinize an ongoing investigation for fear of wading into areas better left to prosecutorial discretion.[309] It therefore remains unclear whether courts would embrace this supervisory power vigorously enough to adequately restrict the use of wiretaps. To date, courts have shown little willingness to reasonably restrict the use of § 2517(5)'s plain-view exception,[310] and there is no indication that courts would do so

309. *See generally* Angela J. Davis, *The American Prosecutor: Independence, Power, and the Threat of Tyranny*, 86 IOWA L. REV. 393, 408 (2001) ("The Supreme Court has consistently upheld the broad exercise of prosecutorial discretion—a power that affords prosecutors far-reaching control over the outcome of criminal cases."). Davis asserts in the context of wiretaps that "Supreme Court jurisprudence suggests that the Court will continue to defer to prosecutorial discretion." *Id.* at 460.

310. *See supra* Part IV.A.

under this alternative approach. Ultimately, any approach relying on closer judicial supervision of an ongoing investigation is likely to prove ineffective.

2. The Burden Approach

A more reasonable and practical approach to restricting wiretap use to appropriate cases would be for courts to focus more heavily on whether the government acted in good faith, which is a necessary requirement to make use of the plain-view exception.[311] To appropriately limit the over-use of wiretaps, this would require courts to place the greatest burden on the government to justify its good faith, as opposed to placing the greatest burden on the defendant to challenge the government's good faith. As discussed above, the plain-view exception has been interpreted in such a way so as to effectively create a presumption of good faith on behalf of the government that, under most circumstances, is nearly impossible for a criminal defendant to overcome.[312] There are two possible standards courts could adopt to reverse this trend: first, courts could permit an evidentiary hearing into the government's good faith once a defendant makes an initial showing justifying such a hearing; and second, courts could adopt a burden-shifting analysis that forces the government to prove its good faith application of the plain-view exception after a simple prima facie showing by the defendant.

Under the evidentiary-hearing approach, a defendant would have the initial burden to establish his or her right to such a hearing. This would require the defendant to reasonably call into doubt whether the primary purpose of the wiretap application was to investigate a Title III predicate offense—i.e., a defendant must present specific, articulable reasons to believe that the government is using Title III as a subterfuge to investigate a non-predicate criminal offense. This initial

311. *See* United States v. Baranek, 903 F.2d 1068, 1070 (6th Cir. 1990); *see also* Derik T. Fettig, *When "Good Faith" Makes Good Sense: Applying* Leon*'s Exception to the Exclusionary Rule to the Government's Reasonable Reliance on Title III Wiretap Orders*, 49 HARV. J. ON LEGIS. 373, 408-09 (2012) (discussing the "good faith" exception).

312. *See supra* Part IV.A.

burden is justified in order to protect the government from unwarranted fishing expeditions by defendants seeking to explore the government's investigation for reasons unassociated with challenging the wiretap warrant. Due to the difficulty involved with presenting objective proof that the government acted in bad faith, a relatively low standard would be appropriate.

Any number of different standards could be adopted in this regard. One reasonable standard justifying an evidentiary hearing is as follows: first, the defendant would have to (1) show that the government knew that it would likely uncover evidence of a non-Title III offense, and (2) demonstrate some articulable reason to call into question whether the government's primary intent in using wiretaps was to investigate a Title III offense. This standard appropriately focuses on what the government knew at the time of its warrant application and on whether the government intended to leverage this knowledge by abusing Title III.

This standard for establishing a right to an evidentiary hearing has several advantages. To begin, this approach maintains the "incidental" standard adopted by the *Rajaratnam* court and many others.[313] It rejects, as many courts have already done, the notion that an interception must be "inadvertent" by requiring a showing greater than that which establishes that the interception of "plain view" evidence was an anticipated consequence.[314] In rejecting the "inadvertent" standard, the district court in *Rajaratnam* stated that such a standard would "bar the government from using wiretaps for wire fraud investigations whenever the fraud concerns securities."[315] Under this suggested standard, however, such a fear should be alleviated.

At the same time, this standard rejects the unjustified result that the more blatant the government is in disclosing that it intends to uncover evidence of other non-predicate

313. *See* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, *11-19 (S.D.N.Y. Nov. 24, 2010) (collecting cases), *aff'd*, 719 F.3d 139 (2d Cir. 2013); *see also supra* note 233 and accompanying text.

314. *See, e.g.*, United States v. McKinnon, 721 F.2d 19, 22-23 (1st Cir. 1983).

315. *See Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *19.

crimes the more successful it will be in using this evidence at trial. The government would therefore be presented with a choice; it could choose to disclose its knowledge that it will likely intercept "plain view" evidence of other crimes (in the warrant application itself), in which case a defendant can establish the first prong necessary to obtain an evidentiary hearing. Alternatively, the government could hide this fact. Ethical concerns aside, the government would be discouraged from concealing this knowledge for two additional reasons. First, there are added protections within the statute likely to expose this deception. For example, Title III requires that when a wiretap warrant is extended beyond thirty days, the government must provide "a statement setting forth the results thus far obtained from the interception."[316] If the government charges the defendant with a non-Title III offense, but intends to use evidence not disclosed in subsequent applications, the government's concealment becomes obvious. Second, this type of deception, if it is discovered, is in and of itself strong evidence of the bad faith likely to obviate the need for an evidentiary hearing.[317]

This standard for securing an evidentiary hearing also has the advantage of placing primary importance on the government's intent. After establishing that the government is aware that it will likely intercept evidence of a non-predicate crime, the standard for challenging the government's primary purpose of the wiretap investigation should be relatively low. But as in other similar contexts, conclusory allegations should be rejected, and a defendant should have to point to specific, articulable reasons for doubting the government's primary purpose. The *Rajaratnam* court acknowledged that charging a defendant with a Title III predicate offense may be evidence of good faith, but it refused to accept the contention that not charging a defendant with a predicate offense is evidence of

316. 18 U.S.C. § 2518(1)(f) (2012).

317. *See, e.g.*, *United States v. Goffer*, No. 11-3591-cr(L), 2013 WL 3285115, at *5 (2d Cir. July 1, 2013) ("This representation [that evidence of other, non-predicate-offense crimes would likely be uncovered in using a wiretap] ensured that the wiretaps were not obtained as a 'subterfuge' or to surreptitiously investigate crimes other than those about which they informed the court.").

bad faith.[318] Under the standard discussed above, however, failing to charge a defendant would be sufficient evidence to justify an evidentiary hearing. This is important because not charging a defendant with a Title III offense is often the only objective evidence a defendant will have to question the government's true intent. That is not to say, however, that other specific, articulable reasons could not be presented. Of course, courts should not be in the position of encouraging prosecutors to over-charge a defendant for acts that the prosecutor, within his or her discretion, truly believes should not be charged as certain offenses. At the same time, however, permitting an evidentiary hearing under these circumstances would appropriately place the government in the position to justify its use of "plain view" evidence. As Judge Holwell recognized, "[t]he government's charging decisions depend on a variety of factors."[319] But, if the government is truly acting in good faith, government agents should easily be able to articulate its reasons for charging a defendant with a non-Title III predicate offense, while at the same time not charging the defendant with the underlying offense justifying the use of a wiretap.

Under this approach, if after an evidentiary hearing the court believes by a preponderance of the evidence that the government was primarily interested in investigating a non-Title III offense, such as securities fraud, then evidence derived from the wiretap warrant should be suppressed. In such a situation, the third prong of § 2518(10)(a) would apply, which permits suppression where "the interception was not made in conformity with the order of authorization or approval."[320] A wiretap warrant implicitly authorizes the incidental intercept of "plain view" evidence. If a wiretap intercept of "plain view" evidence is not done "incidentally," however, it does not comport with the judicial authorization. In addition, suppression may also be required under the first prong of § 2518(10)(a).[321] As discussed above, this section authorizes

318. *See Rajaratnam*, 2010 U.S. Dist. LEXIS 143175, at *13 n.5.
319. *Id.*
320. 18 U.S.C. § 2518(10)(a)(iii).
321. *Id.* at § 2518(10)(a)(i)

suppression where there has been a failure to comply with a substantive statutory provision meant to limit the use of wiretaps.[322] Arguably, if the primary purpose of using a wiretap is to investigate a non-predicate offense, the predicate offense requirement itself is not adequately complied with.

An alternative to the evidentiary-hearing approach would be to adopt a burden-shifting analysis. In many ways, this approach would be similar to the evidentiary-hearing approach. Pursuant to this standard, a defendant would first have the obligation to make a prima facie case that the government was acting in bad faith. Therefore, the defendant would have to present evidence that (1) the government knew it was likely to intercept "plain view" evidence of additional crimes, and (2) this was the government's primary purpose in using a wiretap. A standard similar to that which would warrant an evidentiary hearing under that alternative approach would also be appropriate here. If a defendant succeeds in presenting a prima facie case that calls into question whether the government acted in good faith through the two criteria above, the burden would then shift to the government to come forward with evidence that it was primarily, or at least equally, interested in investigating the crime justifying the use of a wiretap. If the government cannot make such a showing, the wiretap evidence should be suppressed. If the government satisfies this burden, then the burden would again shift back to the defendant to prove that the government's justification is pretextual. The level of proof necessary to establish that the government's explanation was pretextual would be greater than that required to establish a prima facie case.

Both the evidentiary-hearing and burden-shifting approaches have the advantage of placing the greatest burden on the government (after a small initial burden is overcome by the defendant). The statute itself envisions that the government would have the burden of establishing the application of the plain-view exception of § 2517(5).[323] Most obviously, Title III permits the use of this evidence only where it is "authorized or approved by a judge of competent

322. *See supra* Part IV.B.
323. *See* 18 U.S.C. § 2517(5).

jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter."[324] By requiring the government to make this application, Title III implicitly places the burden on the government to prove the applicability of this exception. Legislative history supports this interpretation: "[a] subsequent application would *include a showing* that" this exception was properly used.[325]

From a doctrinal standpoint, the evidentiary-hearing and the burden-shifting approaches would be very similar. In practice, there are benefits and drawbacks to either approach. For example, an evidentiary-hearing approach permits more accurate fact-finding because a defendant is directly allowed to obtain evidence through cross-examination. In contrast, the burden-shifting approach offers the defendant less opportunity to question government witnesses or obtain documents. Of course, these approaches are simply suggestions, and courts can ultimately combine these approaches or find other adequate ways to guard against the abuse of Title III.

All of this being said, one could argue that securities-fraud and other types of white-collar criminal schemes are exactly the type of crimes that Congress envisioned would be investigated using covert electronic surveillance. In passing Title III, Congress found that "[o]rganized criminals make extensive use of wire and oral communications in their criminal activity" and that "[t]he interception of such communications . . . is an indispensable aid to law enforcement and the administration of justice."[326] Those engaging in an insider-trading scheme, where one party passes information to another so that they may unlawfully trade on this inside knowledge, are certainly "organized criminals," although perhaps not in the traditional sense of being associated with mafia activity. Indeed, since the late 1960s, Congress has continuously added to the list of predicate offenses, indicating

324. *See id.*

325. S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2189 (emphasis added) (citations omitted).

326. Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968, Pub. L. No. 90-351, tit. III, § 801(c), 82 Stat. 197, 211 (1968).

an expansive trend.[327] Ultimately, however, adding securities fraud to the list of predicate offenses is a job for Congress, and the restrictions placed on what types of crimes may be investigated using wiretaps must be enforced by the courts. It is not the province of our judicial system to weaken the protections for individual privacy enacted by Congress.

In the end, there are numerous possible approaches courts could adopt to adequately protect against Title III becoming a subterfuge through which prosecutors and other government authorities investigate non-predicate offenses: courts could increase judicial supervision over wiretap intercepts on an ongoing basis, adopt one of several approaches permitting a criminal defendant to more easily challenge the government's assertion of good faith, adopt a mix of these approaches, or develop other alternatives. The primary focus of these efforts, however, almost certainly must be on limiting the use of the plain-view exception of § 2517(5).[328] By limiting the application of this exception, privacy interests will be better protected by discouraging government authorities from using wiretaps as a matter of course.

B. *A Return to the* Giordano *Standard and Strict Compliance With the Necessity Requirement*

In addition to breathing new life into the limitations of the plain-view exception to the predicate offense requirement, courts must also adequately enforce the requirement that the government provide a "full and complete statement" of the facts indicating that a wiretap is necessary.[329] As recent cases indicate, courts have essentially been ignoring controlling Supreme Court precedent dating back to the 1970s in determining whether the government has satisfied its burden

327. *See, e.g.*, Omnibus Crime Control and Safe Streets (Wiretap) Act of 1968, Pub. L. No. 90-351, tit. III, § 801(c), 82 Stat. 197, 211 (1968); Organized Crime Control Act of 1970, Pub. L. No. 91-452, tit. VIII, IX, XI, §§ 810, 902(a), 1103, 84 Stat. 924, 936, 940, 941, 947, 952, 959 (1970); Border Tunnel Prevention Act of 2012, Pub. L. No. 112-127, § 4, 126 Stat. 370, 371 (2012); *cf.* 18 U.S.C. § 2516(1).

328. *See* 18 U.S.C. 2517(5).

329. 18 U.S.C. § 2518(1)(b).

of establishing the necessity of using a wiretap.[330] By inappropriately applying a constitutional standard to an entirely statutorily-created requirement, courts have unjustifiably shifted the burden to criminal defendants to disprove necessity, which allows the government to abuse the wiretap application process. Rather than appropriately placing the burden of proof on the government to establish the necessity of a wiretap, applying a *Franks* analysis shifts the burden to a criminal defendant to prove (1) that the government did not provide a "full and complete statement" in knowing, intentional, or reckless disregard of its obligations and (2) that the falsity or omission at issue was material to the issuing judge's determination of necessity.[331] This threatens the delicate balance between privacy and law-enforcement interests that Congress initially sought to achieve.[332] A return to a more demanding standard based upon the statutory text is required to once again achieve the appropriate balance.

As the Supreme Court in *Giordano* counseled, suppression of a wiretap secured under Title III does not turn upon Fourth Amendment standards, but rather, suppression should always be determined on the basis of the statutory text.[333] Moreover, in *Chavez* the Court noted that "strict adherence" to Title III's requirements should be demanded.[334] Although it is entirely appropriate to apply certain constitutional standards within the framework of Title III—e.g., the standard for probable cause—this is only because the statutory text itself and the legislative history of Title III provides for the application of these standards.[335] Recently, however, courts have been applying the constitutional standard for the sufficiency of a warrant affidavit to the non-constitutionally based requirement of necessity.[336] This threatens the balance

330. *See supra* Part VI.

331. *See* Franks v. Delaware, 438 U.S. 154, 155-56 (1978).

332. *See supra* note 7 and accompanying text.

333. United States v. Giordano, 416 U.S. 505, 524 (1974) (Suppression under Title III "does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of Title III.").

334. *See United States v. Chavez*, 416 U.S. 562, 580 (1974).

335. *See Giordano*, 416 U.S. at 527.

336. *See supra* note 25 and accompanying text; *see also supra* Part

Congress sought to achieve in passing Title III. As the Fourth Circuit warned in a slightly different context, "In the fast-developing area of communications technology, courts should be cautious not to wield the amorphous [Fourth Amendment] standard in a manner that nullifies the balance between privacy rights and law enforcement needs struck by Congress in Title III."[337]

To avoid interfering with the balance Congress sought in passing Title III, courts should focus more on whether the government succeeded or failed in satisfying the statutory requirement of providing "a full and complete statement" to the issuing judge[338] rather than focusing on whether the government would be able to establish the appropriateness of a warrant despite factual misrepresentations or omissions—a primary concern under a Fourth Amendment challenge. This is a somewhat subtle change, but a nevertheless important one. By slightly reframing the appropriate question to answer—focusing more on whether the government satisfied its initial statutory burden of being both forthright and honest, rather than on what a theoretically corrected affidavit would have looked like—courts can adhere more closely to the purposes underpinning Title III and better protect individual privacy.

It is important to note that, in addition to applying a *Franks* analysis to the issue of necessity, courts have also adopted a *Franks* analysis in the context of Title III's probable cause requirements.[339] This, however, is unsurprising, and it is likely a correct application of a constitutional doctrine within the context of Title III. After all, § 2518(10)(a)(i) permits suppression for violations of the Fourth Amendment,[340] and the legislative history of Title III also indicates that § 2518(10)(a) was meant to "largely reflect[] existing law."[341] The necessity

III.B.3.

337. *In re* Askin, 47 F.3d 100, 105-06 (4th Cir. 1995) (citing Katz v. United States, 389 U.S. 347, 351-52 (1967)).

338. *See* 18 U.S.C. § 2518(1)(c) (2012).

339. *See, e.g.*, United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *23-52 (S.D.N.Y. Nov. 24, 2010).

340. *See* United States v. Giordano, 416 U.S. 505, 527 (1974).

341. *See id.* at 529 n.17 (quoting S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182).

requirement, however, is not a requirement under the Fourth Amendment and therefore did not represent "existing law" at the time of its adoption. Thus, it makes little sense to take a statutory requirement and supplant it with a constitutional doctrine in this context. This is especially true when considered against the underlying purpose of the necessity requirement and Title III in general.

In addressing the application of a *Giordano* analysis to the necessity requirement, the Second Circuit recently reasoned, relying on language from the legislative history of Title III, that because Title III "was not intended 'generally to press the scope of the suppression role beyond [then current] search and seizure law,'" cases such as *Franks* and *United States v. Leon* that were decided after the passage of Title III could apply to the statute's provisions.[342] This analysis, however, completely ignores the primary lesson taught by *Giordano*—that suppression under Title III "does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of Title III . . . ."[343] The *Giordano* court specifically addressed the language in the legislative history relied upon the Second Circuit. The Supreme Court noted that this language seemed to be in conflict with other language in the legislative history indicating that § 2518(10)(a) was intended "to guarantee that the standards of [Title III] will sharply curtail the unlawful interception of wire and oral communications."[344] Based on both of these legislative statements, the Court concluded that "it would not extend existing search-and-seizure law for Congress to provide for the suppression of evidence obtained in violation of explicit statutory prohibitions."[345] The *Rajaratnam*

342. United States v. Rajaratnam, 719 F.3d 139, 152 (2d Cir. 2013) (quoting S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185).

343. *Giordano*, 416 U.S. at 524; *see also* Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001) ("Congress made [Title III] the primary vehicle by which to address violations of privacy interests in the communications field. . . . All such constitutional questions are pretermitted.").

344. *Giordano*, 416 U.S. at 528 (internal quotation and citations omitted).

345. *Id.*

court ignored the Supreme Court's reconciliation of the legislative history. Moreover, the Second Circuit's analysis further ignored an important lesson from *Chavez*: that "strict adherence" to the statutory text should be mandated.[346]

The *Rajarantam* court's conclusory reasoning was also applied in an earlier Second Circuit case, *United States v. Bianco*,[347] which the *Rajaratnam* court cited to approvingly.[348] In *Bianco*, the court again ignored the main precept of *Giordano* and further reasoned that "[i]f anything, *Franks* enhances the protection of the defendants, by applying to the wiretap statute an important constitutional principle that has been accepted by all courts."[349] Unexplained, however, is how this can possibly increase the protection of a defendant by applying this standard under Title III, when the defendant is protected by *Franks regardless* of the existence of Title III. Moreover, as noted by the Second Circuit in *Rajaratnam*, the *Franks* decision actually "narrowed the circumstances in which . . . [courts] apply the exclusionary rule," it does not expand protections available to defendants.[350]

One of the purposes of adopting Title III was to provide protections *greater* than those afforded by the Fourth Amendment. For example, Congress provided for, *inter alia*, heightened particularity requirements, a necessity requirement, minimization requirements, and requirements meant to hold public officials accountable for excessive wiretap use.[351] The Supreme Court has specifically stated that the necessity requirement "is simply designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime."[352]

346. United States v. Chavez, 416 U.S. 562, 580 (1974).

347. 998 F.2d 1112, 1126 (2d Cir. 1993), *abrogated on other grounds by* Groh v. Ramirez, 540 U.S. 551 (2004).

348. United States v. Rajaratnam, 719 F.3d 139, 151-52 (2d Cir. 2013).

349. *Bianco*, 998 F.2d at 1126.

350. *Rajaratnam*, 719 F.3d at 152 (quoting *Bianco*, 998 F.2d at 1126).

351. *See generally supra* Part III.

352. United States v. Kahn, 415 U.S 143, 153 n.12 (1974) (citation omitted); *see also* United States v. Martinez, 588 F.2d 1227, 1232 (9th Cir. 1978) ("Th[e] 'necessity' requirement exists to limit the use of wiretaps because of their highly intrusive nature and to 'assure that wiretapping is not resorted to in situations where traditional investigative techniques would

Because the necessity requirement is meant to restrict the use of wiretaps to appropriate cases, it is the very type of requirement that the *Giordano* Court deemed to have a "central role in the statutory scheme."[353] This is in contrast to the probable cause requirements of Title III, which the government would have to comply with regardless of whether Title III specifically mandated it. In other words, the probable cause requirement of Title III is not central to its legislative purpose because any government authority applying for a warrant—including a wiretap warrant—would have to supply evidence of probable cause regardless of the strictures of Title III.[354] The probable cause requirements of Title III therefore do not protect against the excessive use of wiretaps beyond what the Federal Constitution itself prohibits. As such, the probable cause requirement does not play a "central role in the statutory scheme," unlike the necessity requirement, which provides greater protection for individual privacy than the Constitution does.

One prerequisite to a lawful wiretap is pre-application approval by a designated government official.[355] The *Giordano* court, however, also implicitly concluded that knowledgeable approval by a judicial officer was a prerequisite for a lawful intercept.[356] In considering whether an extension order permitting the electronic surveillance of additional suspects were appropriate, the Court stated that:

> It is urged in dissent that the information obtained [unlawfully] may be ignored and that the remaining evidence submitted in the extension application was sufficient to support the extension order. But whether or not the application, without the facts obtained from monitoring Giordano's telephone, would

suffice to expose the crime." (quoting *Kahn*, 415 U.S. at 153 n.12)).

353. *See Giordano*, 416 U.S. at 527-28.

354. *See supra* Part III.B.2.

355. *See Giordano*, at 512-23.

356. *See id.* at 515-516 ("The mature judgment of a particular, responsible Department of Justice official is interposed as a critical precondition to any judicial order.").

> independently support original wiretap authority, *the Act itself forbids extensions of prior authorizations without consideration of the results meanwhile obtained.*[357]

Here, the Court again placed importance on judicial pre-screening. Failure to appropriately obtain judicial screening in and of itself would be a violation of a substantive provision central to the statutory scheme that would likely require suppression.[358] Unlike a clerical error, such as misstating the authorizing official, as was the case in *Chavez*, failure to provide a "full and complete statement" of the facts

357. *Id.* at 533 (emphasis added).

358. *See In re* Application for Interception of Wire Commc'ns, 2 F. Supp. 2d 177, 179 (D. Mass. 1998). In this case, a district court, after learning that federal authorities had not been completely forthcoming in other wiretap warrant applications in other cases added a handwritten requirement in the margin of an order approving the use of a wiretap, which stated: "This order is entered on the express representation that there are no other informants presently known to the government knowledgeable of the matters contained herein. If that representation is inaccurate, this order is of no force and effect." *Id.* at 177. The Government sought to have the court reconsider this language, but the court rejected this attempt, reasoning that:

> The independent determination by a judicial officer—rather than by a law enforcement officer—of the necessity of electronic surveillance undergirds the very constitutionality of Title III. Indeed, it is this independent judicial assessment that ensures that electronic surveillance is consistent with the dictates of the Fourth Amendment. The Court's order makes it clear, without impugning the integrity of the individual agents making this application, that it will not tolerate the willful or reckless submission of misleading or incomplete information in support of an application to conduct electronic surveillance. The government will not have met its burden of justifying this intrusive technique, unless its agents have been candid with one another and with the Court. The Court's order further puts the United States on notice that, should the Court come to learn of any deception in this regard, its order allowing such an application will have no force or effect.

Id. at 179 (internal citations omitted). *Cf.* United States v. Spagnuolo, 549 F.2d 705, 711 (9th Cir. 1977) (permitting an insufficient warrant application "will effectively deny the district judge his statutory role").

establishing necessity does indeed "affect the fulfillment of . . . the reviewing or *approval* functions required by Congress."[359]

Moreover, nothing in *Giordano* or its progeny suggests that the court would have recognized an exception for satisfying the judicial approval requirement after the fact—i.e., the court required strict compliance with the substantive provisions.[360] For example, nothing in *Giordano* indicates that the Court would have reached the opposite conclusion had the Attorney General submitted an affirmation or an affidavit swearing under oath that he would have approved the wiretap application if it had been presented to him prior to filing. It would have made little sense to supply a judicially-crafted

359. United States v. Chavez, 416 U.S. 562, 575 (1974) (emphasis added). The *Spagnuolo* court noted:

> To delay the wiretap order while ordinary techniques are employed or to undertake to educate a district judge to enable him to appreciate their level of experience no doubt appears to such agents as a waste of time and resources. Their perception may be accurate, but Congress has deprived it of decisive influence. The particularized showing here described is necessary. The district judge, not the agents, must determine whether the command of Congress has been obeyed.

Spanguolo, 549 F.2d at 710-11.

360. As Professor Robert Blakey, who was actively involved in the passage of Title III, argues in his *amicus curiae* brief in front of the Second Circuit in the *Rajaratnam* case:

> The prior judicial review that Congress found to be central to Title III and that was determined to be indispensable to protecting the rights enunciated in *Berger* and *Katz* is simply impossible when the government fails to provide a full and complete disclosure of necessity. Without that statement, an authorizing judge cannot appropriately determine whether a wiretap should issue. The government's failure to meet the statutory test constituted a blatant violation of a provision of Title III that plays a central role in the statutory scheme.

Brief of *Amicus Curiae* Professor G. Robert Blakey in Support of Appellant at 21, United States v. Rajaratnam, No. 11-4416-cr, 2013 WL 3155848, at *1 (2d Cir. June 24, 2013) (No. 11-4416-cr), 2012 WL 453986, at *21 (quoting *Giordano*, 416 U.S. at 528) (internal quotation marks omitted).

exception such as this. The primary purpose of the statute is to protect individual privacy against the excessive use of intrusive surveillance measures. The harm to individual privacy resulting from a wiretap occurs at the moment of interception; once a private conversation is intercepted, the harm to privacy interests has already come to fruition. Thus, permitting a *post hoc* justification should not be permitted because the harm sought to be avoided has already occurred.[361] A *Franks* analysis, which in practical effect allows for justification of the necessity requirement after the interception has already occurred, therefore does little, if anything, to protect the relevant privacy interests. In order to give life to the purpose of the necessity requirement, a more demanding standard is necessary.

To a certain degree, adopting a *Franks* analysis for the requirement of necessity makes sense within the structure of the statutory scheme. In addition to supplying a "full and complete statement" of facts establishing necessity, Title III also demands that a wiretap applicant provide a "full and complete statement" of the facts establishing probable cause.[362] On a textual basis, this would seem to indicate that the same standard should be applied when evaluating whether the government has satisfied its statutory application

361. *Cf.* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 317-18 (1972). The court stated:

> It may well be that, in the instant case, the Government's surveillance of [defendant's] conversations was a reasonable one which readily would have gained prior judicial approval. . . . The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised. . . . The independent check upon executive discretion is not satisfied, as the Government argues, by extremely limited post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.

Id. (internal quotation marks and citations omitted).

362. *Compare* 18 U.S.C. § 2518(1)(c) (2012) *with id.* § 2518(1)(b).

requirements. Undercutting this reading of the statute, however, is that the same "full and complete statement" standard applies to the warrant extension provisions of § 2518(1)(e).[363] The Supreme Court has already indicated that including facts obtained from previous electronic surveillance in an extension application is a substantive provision—i.e., it is central to the statutory purpose.[364] Perhaps a stronger structural argument can be made for applying a *Franks* analysis to the necessity requirement by looking at § 2518(3).[365] This subsection provides that upon a wiretap application, a judge may issue an *ex parte* order only where the judge finds, based on the facts submitted, 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 [in the case of a "roving" wiretap], 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.[366]

Here, the necessity requirement is on the same footing as the

363. *See id.* § 2518(1)(e).
364. *See Giordano*, 416 U.S. at 533.
365. *See* 18 U.S.C. § 2518(3).
366. 18 U.S.C. § 2518(3)(a)-(d).

constitutional requirements of probable cause and particularity. However, as noted earlier, Title III actually has greater particularity requirements than under the Fourth Amendment.[367] Both of these above interpretative arguments are also vitiated by the underlying purpose of each statutory requirement. As explained above, the probable cause requirement was meant to maintain the status quo, while the necessity requirement was meant to afford greater protection to privacy interest.[368]

Courts have also been quick to note that "it is not [a court's] province to engage in *de novo* review of a[] [warrant] application; instead, we test it in a practical and commonsense manner to determine whether the facts which it sets forth are minimally adequate to support the findings made by the issuing judge."[369] This is certainly correct; a determination of wiretap necessity is analogous to a factual finding that reviewing courts are apprehensive to second-guess. Therefore, a court should not lightly overturn an issuing judge's determination that "necessity" is present in a given case. This does not mean, however, that a court should abstain from deciding whether or not an issuing judge's decision was based on misleading or incomplete information. It also does not mean that a reviewing court should give similarly greater discretion where a judge's determination is made on the basis of this misleading or incomplete data. As the Sixth Circuit succinctly put it:

> Generally, in reviewing the validity of an electronic surveillance order, we will accord great deference to the determinations of the issuing judge. However, this deference does not logically apply where the issuing judge is given misleading information in the wiretap

367. *See generally supra* Part III.

368. *See supra* notes 329-46 and accompanying text.

369. *See* United States v. Cole, 807 F.2d 262, 268 (1st Cir. 1986) (internal quotation marks and citations omitted); *see also* United States v. Torres, 901 F.2d 205, 231 (2d Cir. 1990) (quoting United States v. Scibelli, 549 F.2d 222, 226 (1st Cir. 1977) (collecting cases)), *abrogation recognized by* United States v. Al Jaber, 436 F. App'x 9, 12 (2d Cir. 2011).

application or supporting affidavits.[370]

Taking all of this into consideration, courts should adopt a more stringent standard to appropriately protect against abuse of the wiretap application process. An appropriate standard would in some sense look similar to a *Franks* analysis, but it would stop short of requiring a showing that the omitted or misstated fact was material, which essentially shifts the burden to the defendant to disprove necessity. Once a defendant has presented specific, articulable reasons to cast doubt on the veracity of the facts used to establish necessity in the government's application, a *Franks*-type evidentiary hearing should be granted.

At this stage, the defendant challenging the wiretap application should have the burden to come forward with sufficient evidence to justify a hearing. Placing this initial, but relatively light, burden on the defendant to present some minimal level of proof of falsity prevents courts from going on endless, unfruitful excursions into government investigations. It therefore takes into account considerations of judicial efficiency. Based on policies underlying the Fourth Amendment, a wiretap warrant is generally presumed valid.[371]

370. United States v. Rice, 478 F.3d 704, 709 (6th Cir. 2007) (internal quotation marks and citation omitted). *Cf.* United States v. Canfield, 212 F.3d 713, 717 (2d Cir. 2000) ("In this situation, the issuing judge's probable cause determination is not due any deference because he did not have an opportunity to assess the affidavit without the inaccuracies.").

371. *See* Franks v. Delaware, 438 U.S. 154, 171 (1978); *see also* United States v. Zapata, Nos. 96-1457, 97-1013, 96-1536, 96-1573, 1998 WL 681311, at *2 (2d Cir. Jan. 30, 1998) ("Wiretap orders are presumed valid . . . ."). *Cf.* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 316-17 (1972). There, the court stated:

> These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks.

An even stronger case for assumed validity of a warrant can be made as it specifically relates to a wiretap warrant because of the added layers of protection provided by Title III. By the time a wiretap application is submitted for judicial approval, the Attorney General or one of his or her designated officials has already pre-approved the application, and therefore the government has already made an internal institutional determination that a wiretap is necessary. This pre-approval is not required by the Fourth Amendment. This added layer of protection gives further reason not to question the government's good faith absent at least some minimal evidence to the contrary. For these reasons, a standard similar to that required to obtain an evidentiary hearing under *Franks* is also appropriate to use where a defendant challenges whether the government has supplied a "full and complete statement" concerning the requirement of necessity. This standard is the following:

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.[372]

> The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

Id. (internal citation omitted).

372. *See Franks*, 438 U.S. at 172.

The burden at this hearing would then shift to the government to prove by a preponderance that they had acted appropriately and supplied a "full and complete statement" of necessity based on all of the facts developed at that hearing.[373] If after the conclusion of the hearing the government has not met its burden and the court determines that the government recklessly, knowingly, or intentionally omitted or misrepresented pertinent facts in its affidavit, all evidence derived from the subsequently issued wiretap should be suppressed. Unlike the analysis under *Franks*, the inquiry should end there; whether the omitted or misrepresented information is "material" should not be considered. This approach would place increased emphasis on appropriately obtaining judicial approval, and it would keep the burden of proof entirely on the government to prove that it complied with the statutory procedures. Both of these results are more in line with the statutory text and legislative history than is the current status quo.

This approach would be similar (with one important difference) to what the appellant sought in *United States v. Heilman*,[374] and which the Third Circuit declined to adopt.[375] There, the defendant argued that a *Franks* analysis is inapplicable to a wiretap challenge to the necessity requirement, and that instead of a *Franks* hearing, he should be entitled to a "necessity hearing."[376] Although not fully defining what such a hearing would entail, the defendant suggested that it would "include[] an inquiry into any material misstatements or omissions regarding necessity as part of the reviewing court's duty to assess necessity."[377] The defendant in *Heilman* argued that he should be entitled to a "necessity hearing" simply by alleging that the government illegally

373. Even under a *Franks* analysis, additional information not contained in the warrant affidavit may be used to determine the government's state of mind. *See, e.g.*, United States v. Finley, 612 F.3d 998, 1003 n.7 (8th Cir. 2010).

374. 377 F. App'x 157 (3d Cir. 2010).

375. *See id.* at 183-84.

376. *See id.*

377. *Id.*

searched him.[378] As the Third Circuit correctly noted, however, such a hearing should not be granted in the absence of at least some initial showing of falsity.[379]

378. *Id.* at 184. The court articulated that:

> Pursuant to § 3504, if defendants claim that evidence against them was acquired as a result of prior, unlawful surveillance, the Government must confirm or deny whether that unlawful surveillance occurred. Napoli interprets the Government's statutory obligation to confirm or deny the existence of the unlawful surveillance as to mandate a necessity hearing. This interpretation, however, is completely divorced from a plain reading of the text. Nothing in the text indicates that defendants are entitled to a hearing if they allege that the Government illegally searched them by electronic means.

Id. (internal citation omitted).

379. *See id.* While the Third Circuit refused to decide whether *Franks* is appropriate to apply to the necessity requirement, two cases from the Second Circuit have rejected a similar argument. In *United States v. Bianco*, the Second Circuit held that a *Franks* analysis is appropriate to apply to the "impracticality" provision for obtaining a "roving" wiretap under Title III, which similarly requires a "full and complete statement" on the question of "'why such specification [of the place where the communication is to be intercepted] is not practical.'" United States v. Bianco, 998 F.2d 1112, 1125 (2d Cir. 1993), *abrogation recognized by* United States v. Galpin, No. 11-4808-cr, 2013 WL 3185299, at *7 (2d Cir. June 25, 2013). The court rejected the defendant's argument that it "should look directly to the exclusionary rule of the statute, rather than to focus on fourth-amendment considerations or a *Franks* analysis." *Id.* at 1125. In doing so, the court reasoned that the suppression provision was "not intended 'generally to press the scope of the suppression role beyond [then] present search and seizure law,'" *id.* at 1126 (citing S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185; Scott v. United States, 436 U.S. 128, 139 (1978)), and because Title III predated *Franks*, applying such an analysis would actually strengthen the protections of Title III. *See Bianco*, 998 F.2d at 1126. This analysis, however, completely ignored *Giordano* and the legislative history indicating that the necessity requirement was intended to provide *greater* protections than that which is provided by the Fourth Amendment. *See* United States v. Giordano, 416 U.S. 505, 526 (1974) ("[P]redecessor bills [to Title III] specified a fourth ground for suppression—the lack of probable cause—which was omitted in subsequent bills, apparently on the ground that it was not needed because official interceptions without probable cause would be unlawful within the meaning of [§ 2518(10)(a)(i)]."); *see also* United States v. Amanuel, 615 F.3d 117, 125-27 (2d Cir. 2010) (noting that Title III suppression is more expansive than the exclusionary rule). The *Rajaratnam* court also rejected these arguments, but did so by relying on *Bianco*, concluding that defendants'

In addition to being more closely aligned with the statutory text, the "necessity hearing" approach better protects the privacy interests at stake. As noted above, individual privacy is harmed at the moment a private conversation is intercepted by a third party, such as an investigating government official.[380] Although this harm may be aggravated by repeating the contents of that conversation at a later time—e.g., by playing a recording of the intercepted conversation in open court—a private conversation no longer remains private from the moment another person eavesdrops or otherwise interferes. This truth is reflected in many areas of the law. In the Fourth Amendment context, holding a conversation with a known third-party present will destroy one's reasonable expectation of privacy.[381] Similarly, the attorney-client privilege is destroyed where a third party is exposed to the contents of an attorney's legal advice given to his or her client.[382] Privacy interests can be protected effectively only where preventative measures are in place; it is exceedingly difficult to protect privacy retroactively. Congress established a number of preventative measures when it enacted Title III, and the necessity requirement is one of them. Therefore, it should be vigorously enforced.

In this regard it is important to remember exactly the privacy interests at stake. It is feasibly possible to retroactively protect the privacy rights of each individual criminal defendant to a limited extent. This is the very premise underlying the exclusionary rule; an unconstitutional invasion into a private, protected area results in suppression. A *Franks* analysis also accomplishes this goal by suppressing evidence where, had the

arguments were "foreclosd by settled precedent." United States v. Rajaratnam, 719 F.3d 139, 151 (2d Cir. 2013) (citing *Bianco*, 998 F.2d 1112).

380. *See supra* notes 88-89, 150 and accompanying text; *see also supra* Part III.B.4.

381. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927))).

382. *See* 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2311, at 601-03 (John T. McNaughton rev. ed. 1961) (attorney-client communications in presence of third party not the agent of the attorney are not protected by the privilege).

government been fully truthful in its application, necessity of a wiretap would not have been established. But, retroactive protection of privacy rights has limitations. To begin, the remedy of suppression cannot undo an already-completed invasion of a person's privacy. Instead, it merely serves as the next best alternative—protecting against further aggravation of the initial unlawful intrusion. Similarly, the suppression remedy has a limited reach in terms of who it protects. Only a criminal defendant successfully challenging the use of certain evidence directly benefits from the exclusion of that evidence. Others, however, indirectly benefit from suppression based on its deterrent effect on law enforcement.

Title III is concerned with privacy interests much broader than those represented by persons who find themselves subject to criminal prosecution. Less than one-quarter of all authorized wire intercepts in 2011 resulted in the discovery of incriminating evidence.[383] The vast majority of these intercepts therefore involved innocent, non-criminal communications. Many of these same intercepts also likely listened in on, not just innocent conversations by suspected criminals, but also conversations between a suspected criminal and wholly-innocent individuals. An illustrative case is *United States v. Goffer*,[384] another recent insider trading prosecution, where investigators using a wiretap listened in on private marital conversations between the defendant and his wife.[385] Over the course of a sixty day period, federal agents intercepted 180 calls between the defendant and his wife dealing "almost exclusively with personal and family matters," none of which were incriminating.[386] The court called the actions of federal investigators "disgraceful" and an "unnecessary, and apparently voyeuristic, intrusion into the [defendant and his wife's] private life."[387] The invasion of privacy at stake where

383. *See* 2011 WIRETAP REPORT, *supra* note 5, at 21 tbl.4. On average, 868 out of 3,716 intercepts were incriminating, which equates to an incriminating-interception rate of 23.36%.

384. 756 F. Supp. 2d 588 (S.D.N.Y. 2011), *aff'd*, No. 11-3951-cr(L), 2013 WL 3285115, at *5 (2d Cir. July 1, 2013).

385. *Id.* at 591.

386. *Id.*

387. *Id.* at 594-595.

the government uses wiretaps is in contrast to a more typical Fourth Amendment violation of a person's privacy, the collateral consequences of which are relatively limited. For example, a warrantless home invasion by police affects the privacy rights of the handful of other people who may live at the residence. A wiretap investigation spanning 30 days, on the other hand, has the capacity to ensnare possibly dozens of innocent people making contact with the target of the wiretap.[388] This broad threat to privacy was the very reason Congress sought to limit the use of wiretaps beyond the protections afforded by the Constitution. Because of the broader scope of privacy interests at stake, the indirect benefit of police deterrence afforded by the remedy of suppression is of paramount importance when it comes to the covert interception of private conversations. Thus, requiring a less demanding standard on the defendant to suppress wiretap evidence is also appropriate as a matter of sound policy.

At the same time, to balance appropriately privacy and law-enforcement concerns, courts should avoid applying a negligence standard to the government's failure to provide a "full and complete statement" of the facts indicating necessity. Adopting a negligence standard to omissions or misrepresentations would not further the interests of individual privacy and would therefore be an unjustified boon to criminal defendants. Assuming that the government negligently omitted certain facts concerning necessity from a wiretap application, other protections exist for individual privacy. Most importantly, pre-application approval is required by the Attorney General or another appropriately designated official.[389] This government official must conclude prior to submitting a warrant application that using a wiretap is necessary.[390] Therefore, negligently or carelessly omitting or misrepresenting certain facts in a wiretap application is more

388. *See, e.g.*, Brief for Defendant-Appellant at 9, United States v. Rajaratnam, 719 F.3d 139 (2d Cir. 2013) (No. 11-4416-cr), 2012 WL 389959, at *9 (stating the warrant and renewal applications in this case spanned nine months and "record[ed] over 2,200 private conversations between Appellant and at least 130 of his colleagues, employees, friends, and family").

389. *See* United States v. Giordano, 416 U.S. 505, 528 (1974).

390. *Id.* at 527-28.

analogous to *Chavez*, where the Supreme Court held that improperly identifying the government official who pre-approved the application does not require suppression.[391]

Another important consideration is that the line between recklessness and negligence in regard to a wiretap affidavit will often be determined by the caliber of the omitted or misrepresented facts in the larger context of the investigation. The *Rajaratnam* case again provides a poignant example. There, the government failed to reveal that its investigation of one of the defendants dated back to the late 1990s, which to the district court was a "glaring" omission.[392] Do to the sheer magnitude of the omission at issue, the district court concluded that the government had acted recklessly.[393] On appeal, however, the Second Circuit was less convinced as to the magnitude of this omission, concluding that the government had acted, at most, negligently.[394] The Second Circuit noted that "reckless disregard" can at times "be *inferred* from the omission of critical information in a wiretap application" because "[s]ubjective intent, after all, is often demonstrated with objective evidence."[395] This does not mean, however, that this inference "can be automatically drawn simply because a reasonable person would have included the omitted information, and the inference is particularly inappropriate where the government comes forward with evidence indicating that the omission resulted from nothing more than negligence, or that the omission was the result of a considered and reasonable judgment that the information was not necessary to the wiretap application."[396] Thus, the size and scope of the

391. *See* United States v. Chavez, 416 U.S. 562, 565 (1974); *see also* United States v. Donovan, 429 U.S. 413, 436 n.23 (1977).

392. *See, e.g.*, United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, *36, 58 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

393. This consideration is distinct from the second prong of a *Franks* analysis concerning materiality.

394. *See* United States v. Rajaratnam, 719 F.3d 139, 155-56 (2d Cir. 2013).

395. *Id.* at 154 (internal citations omitted).

396. *Id.*; *see also* United States v. Rice, 478 U.S. 704, 715-18 (2007) (Bell, C.J., dissenting) (arguing that the Government's omissions were merely negligent, not reckless).

omission are often critical considerations. Although the government should not have to give minutely detailed information about its investigation to obtain a wiretap warrant, it generally must give a broad and comprehensive overview—i.e., "a full and complete statement"—of the investigation. Applying a negligence standard would permit a defendant to attack a wiretap affidavit based upon omissions not particularly relevant to a full, inclusive determination of necessity. This would contradict the congressional intent that a necessity determination be made in a common sense manner.[397] Therefore, a negligence standard would require specificity in a wiretap warrant not intended by Congress.

Of course, many of these same considerations are also to some extent inherent in the materiality determination of a *Franks* analysis. Determining the line between negligence and recklessness, however, is analytically distinct from a materiality determination. Importantly, the focus on the recklessness/negligence paradigm is placed on how the government acted and what its state of mind was. These considerations are the appropriate focus of a Title III suppression analysis, as they place a heavier burden on the government to act "by the book" of Title III. In contrast, the focus of the materiality determination under the Fourth Amendment and *Franks* is whether the certain intentional, knowing, or reckless actions of the government officials were important in the larger context of determining the appropriateness of issuing a warrant.[398]

In sum, where a defendant argues that the government failed to satisfy the necessity requirement of Title III by failing to provide a "full and complete statement" of relevant facts, courts should refocus their analysis on what was provided in the wiretap affidavit itself and how the government acted. Where the defendant can present specific and articulable reasons to doubt the truthfulness or completeness of the wiretap application, an evidentiary hearing should be granted.

397. *See* S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2190.

398. *See, e.g.*, United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *70 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013).

The burden at this stage should be on the government to prove that they obtained appropriate judicial pre-screening. After the conclusion of this evidentiary hearing, if the government cannot establish that it was thorough and honest in its wiretap affidavit (or merely negligent) regarding the facts of its investigation that are related to the issue of necessity, a court should order suppression. Unlike the current standard adopted by numerous Circuit Courts of Appeal,[399] the second prong of a *Franks* analysis should be disregarded. Recklessly, knowingly, or intentionally failing to provide a "full and complete statement" of the facts concerning necessity is enough on its own to warrant suppression. By acting knowingly, intentionally, or recklessly the government cannot establish that a judge was presented with a "full and complete statement" of facts, and therefore the government cannot establish that Title III's mandatory judicial screening requirement was complied with. This standard is more in line with congressional intent and governing Supreme Court precedent. Equally as important, this standard better protects individual privacy and properly rebalances this concern with law-enforcement interests.

VI. Conclusion

As a number of recent white-collar criminal prosecutions indicate, the privacy interests that Congress sought to protect by adopting a comprehensive scheme for obtaining a wiretap warrant are becoming increasingly at risk. By weakening the standard needed to obtain a wiretap and to subsequently use this evidence during a later prosecution, courts have encouraged the increased use of wiretaps. This is in stark contrast to the role Congress originally intended the courts to play in restricting the use of wiretaps to appropriate cases. A return to a more serious enforcement regime for Title III's restrictive, substantive provisions will more adequately protect the privacy of innocent individuals.

Recent trends show that prosecutors are poised to use wiretaps in the investigation of nearly any white-collar crime,

399. *See supra* note 275-77 and accompanying text.

regardless of whether these crimes are generally subject to wiretap investigations under Title III. Similarly, a review of cases shows that courts have been ignoring the specifically provided suppression provisions of Title III in favor of a constitutionally-based approach when determining whether to suppress fruits of a wiretap warrant for failing the necessity requirement. Both of these trends encourage prosecutors to abuse the wiretap application process. Increased wiretap use in turn causes an increase in the number of innocent individuals who will have their conversations intercepted by government officials. These dangers have long been recognized. As Justice Brandeis declared in his *Olmstead* dissent, "writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping."[400]

Two important changes are needed to rebalance the privacy interests Congress originally intended to protect in enacting the warrant application procedures of Title III. First, there must be stronger restrictions placed on the use of the plain-view exception to the predicate offense requirement. There are a number of ways to accomplish this. Courts could reassert their supervisory role over government investigators engaging in covert electronic surveillance in part by restricting the time the government has to submit a subsequent application to use "plain view" evidence at trial. Ultimately, however, this approach is unlikely to be successful. A more reasonable approach would be to develop a procedure for a criminal defendant to challenge the government's assertion of good faith use of this exception. Permitting an evidentiary hearing once the defendant has made some minimal showing that challenges the government's good faith or adopting a burden-shifting analysis are both appropriate means to accomplish this end. Next, courts should more strictly enforce the necessity requirement of Title III by placing increased importance on knowledgeable judicial pre-approval. The constitutional standard of *Franks v. Delaware* should be rejected in favor of a statutorily-based analysis more in line with *United States v. Giordano* and its progeny. The focus of

400. Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

this analysis should be on whether the government has satisfied its obligation to provide a "full and complete statement" of facts showing that a wiretap is necessary. With these changes courts can reverse the trend toward expanded wiretap use.

In a modern world that is becoming increasingly reliant on social media, protecting the privacy of individuals is becoming a steeper uphill battle. Many have become complacent about privacy concerns due to their use—and their family and friends' use—of social media such as Facebook, Twitter, Gmail, YouTube, etc. Social media outlets such as these have increasingly opened up people's lives to others. Although there are undoubtedly benefits to this increased connectivity, some are slowly starting to become aware of the dangers associated with it as well. For example, several states have recently passed legislation prohibiting prospective employers from asking interviewees for their Facebook passwords.[401] As technology advances, however, we should not lose sight of older methods of communication, such as the telephone, and the risks posed to individual privacy when the government surreptitiously intercepts these communications.

A job candidate is undoubtedly more sympathetic than an accused criminal defendant. Many would argue that there should be no privacy rights for those engaging in a criminal enterprise. Whether or not this is true, the privacy interests at stake extend far beyond the rights of those subject to criminal prosecution. Wiretaps have the ability to intercept conversations from dozens of innocent individuals. It is therefore important not to lose the forest for the trees. The unsympathetic nature of fallen Wall Street insiders should not interfere with a dogged adherence to the pursuit of protecting

401. *See* Ed Yohnka, *Another State Acts to Protect Facebook Passwords from Employers*, ACLU.ORG, (Aug. 3, 2012, 1:24 PM), http://www.aclu.org/blog/technology-and-liberty/another-state-acts-protect-facebook-passwords-employers; Steven Greenhouse, *Even if it Enrages Your Boss, Social Net Speech is Protected*, N.Y. TIMES, January 22, 2013, at A1, *available at* http://www.nytimes.com/2013/01/22/technology/employers-social-media-policies-come-under-regulatory-scrutiny.html?pagewanted=all&_r=0 ("On Jan. 1, California and Illinois became the fifth and sixth states to bar companies from asking employees or job applicants for their social network passwords.").

individual privacy more broadly. As Chief Justice Warren succinctly observed fifty years ago: "[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual."[402] Perhaps this is true now more than ever.

402. Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring).