NO. _____

In The
Supreme Court of the United States

RAJ RAJARATNAM,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Second Circuit

PETITION FOR A WRIT OF CERTIORARI

Paul D. Clement
Erin E. Murphy
Barbara A. Smith
BANCROFT PLLC
1919 M Street NW,
Suite 470
Washington, DC 20036
(202) 234-0090

Samidh Guha
AKIN GUMP STRAUSS HAUER & FELD LLP
One Bryant Park
New York, NY 10036
(212) 872-1000

Pratik A. Shah
Counsel of Record
Terence J. Lynam
James E. Sherry
Hyland Hunt
AKIN GUMP STRAUSS HAUER & FELD LLP
1333 New Hampshire Ave. NW
Washington, DC 20036
(202) 887-4000
pshah@akingump.com

Counsel for Petitioner

QUESTIONS PRESENTED

In the wake of the 2008 financial crisis, the government has conducted a targeted campaign to increase white-collar criminal prosecutions. Petitioner, one such target, is now serving a previously unprecedented 11-year prison term for insider trading, on top of a separate civil SEC prosecution netting nearly $94 million. The government secured Petitioner's conviction only by relying on two novel and legally suspect tools.

First, the Second Circuit uniquely permits jury instructions in criminal securities fraud cases that eviscerate the statute's causation and scienter requirements. Section 10(b) of the Securities and Exchange Act makes it unlawful to "use" or "employ" any "manipulative or deceptive device" "in connection with the purchase or sale" of a security. 15 U.S.C. § 78j(b). This Court has interpreted the statute to require a showing that the defendant traded "*on the basis of* material, nonpublic information" in order to obtain a conviction for insider trading. *United States v. O'Hagan*, 521 U.S. 642, 651-652 (1997) (emphasis added). Consistent with that understanding, the Eighth and Ninth Circuits require the government to show that a defendant *actually used* inside information. The Second Circuit alone operates under a drastically different regime: The government may secure a conviction so long as the defendant traded while in "knowing possession" of inside information—even if the defendant never used that information in any meaningful way. This conflicting standard guts the statute's causation requirement and effectively converts trading-in-possession into a strict liability offense. And it has

dramatic consequences for professional traders who, in the course of their wholly legitimate efforts to gather as much information as possible about publicly traded stocks, may come to possess some information originating from inside sources.

Second, the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2510-2522, requires the government to provide "full and complete statement[s]" regarding probable cause and the necessity of a wiretap to the authorizing judge. *Id.* § 2518(1)(b) and (c). The Second Circuit did not disturb the district court's finding that the government had made "nearly a full and complete *omission*" of required information that made meaningful judicial evaluation of the application "impossible." In contravention of Title III's mandate and this Court's precedent, however, the Second Circuit applied more lenient Fourth Amendment suppression standards to deny suppression here.

The questions presented are:

1. Whether, in order for a criminal securities fraud prosecution for trading on the basis of inside information to be consistent with Section 10(b) and our basic constitutional traditions, the government must prove, at a minimum, that the inside information was a substantial factor in the defendant's trading activities.

2. Whether wiretap evidence must be suppressed when the government omits and misstates information clearly critical to assessing the legality of a wiretap, instead of providing the "full and complete statement" required by Title III.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES:

CONSTITUTION AND STATUTES:

RULES:

OTHER AUTHORITIES:

In The
Supreme Court of the United States

NO. _____

RAJ RAJARATNAM,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Second Circuit

PETITION FOR A WRIT OF CERTIORARI

Petitioner Raj Rajaratnam respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Second Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-44a) is reported at 719 F.3d 139. The district court's order (Pet. App. 45a-126a) is unpublished, but a redacted version is available at 2010 WL 4867402.

JURISDICTION

The Court has jurisdiction under 28 U.S.C. § 1254(1). The judgment of the court of appeals was

entered on June 24, 2013. Petitioner timely filed a petition for rehearing and rehearing en banc, which was denied on November 18, 2013.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the U.S. Constitution is reprinted at Pet. App. 129a. The relevant portion of the Securities and Exchange Act, 15 U.S.C. § 78j, is reprinted at Pet. App. 130a-132a. The relevant sections of the Omnibus Crime Control and Safe Streets Act ("Title III"), 18 U.S.C. §§ 2510, 2515, 2516, 2518, are reprinted at Pet. App. 133a-162a.

STATEMENT OF THE CASE

A. Legal Framework

1. Like many aspects of securities fraud law, the law of insider trading is "a judicial oak which has grown from little more than a legislative acorn." *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 737 (1975). It is well established that "[t]he definition of the elements of a [federal] criminal offense is entrusted to the legislature." *Liparota v. United States*, 471 U.S. 419, 424 (1985) (citing *United States v. Hudson*, 11 U.S. (7 Cranch) 32 (1812)). Nonetheless, Congress has neither expressly criminalized nor expressly defined the offense of "insider trading." Instead, the federal courts, following the SEC's lead, have declared insider trading a violation of Section 10(b) of the Securities and Exchange Act of 1934, which makes it "unlawful … [t]o use or employ, in connection with the purchase or sale of any security … any manipulative or

deceptive device or contrivance." 15 U.S.C. § 78j(b); *see also* 17 C.F.R. § 240.10b-5(a) ("It shall be unlawful for any person … [t]o employ any device scheme, or artifice to defraud … in connection with the purchase … of any security.").

In the absence of a statutorily defined offense, courts have incrementally delineated—and inexorably expanded—the conduct that constitutes insider trading and the categories of individuals capable of committing the offense. Although insider trading originally was conceived as a limit on the trading activities of actual insiders—*i.e.*, individuals such as "officers, directors and controlling stockholders" who have access "to information intended to be available only for a corporate purpose," *Cady, Roberts & Co.*, 40 S.E.C. 907 (Nov. 8, 1961)—courts have since broadened the offense to include individuals "tipped" by corporate insiders, *see Dirks v. SEC*, 463 U.S. 646, 660 (1983), and anyone who trades on the basis of nonpublic information "misappropriated in breach of a fiduciary duty," *United States v. O'Hagan*, 521 U.S. 642, 647 (1997). Thus, as this common-law process has expanded "insider trading" liability beyond true insiders and their direct tippees, it has created the prospect of criminal liability based not only on the activities of those who trade in their own company's shares, but also on the day-to-day activity of securities professionals.

Throughout this expansion, however, one limit has remained constant: In keeping with Section 10(b)'s requirement that an individual "use" or

"employ" a manipulative or deceptive device, this Court always has recognized that the trading activity must be "on the basis of" inside information. *O'Hagan*, 521 U.S. at 651-652; *Dirks*, 463 U.S. at 653 n.10, 654, 658-659; *Chiarella v. United States*, 445 U.S. 222, 226, 229 (1980). Under this Court's current formulation, an individual commits a criminal offense under Section 10(b) when he (1) knowingly (2) trades (or tips) stock (3) *on the basis of* (4) material (5) nonpublic information that was (6) disclosed or misappropriated in breach of a fiduciary duty. *O'Hagan*, 521 U.S. at 650-52.

2. The wiretapping of private telephone calls is a search that requires prior judicial authorization under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 357 (1967). Congress enacted Title III to establish a "comprehensive scheme for the regulation of wiretapping and electronic surveillance" that would enforce congressional policy "strictly to limit the employment" of wiretapping. *Gelbard v. United States*, 408 U.S. 41, 46, 47 (1972).

Congress "set[] forth with meticulous care" the information that the government must provide the authorizing judge to obtain a wiretap. *Dalia v. United States*, 441 U.S. 238, 249 (1979). Among other things, the government must provide a "full and complete statement" regarding probable cause, 18 U.S.C. § 2518(1)(b), and 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," *id.* § 2518(1)(c).

Congress specified suppression as the required remedy for "any" communication that has been "unlawfully intercepted" in violation of Title III. 18 U.S.C. § 2518(10)(a)(i). Suppression under Title III thus is required whenever "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." *United States v. Giordano*, 416 U.S. 505, 527 (1974).

B. Factual Background and Procedural History

1. Petitioner is the founder and was the managing general partner of Galleon Management, once a large hedge fund. At its peak in 2008, Galleon managed more than $6 billion on behalf of its investors, which included public and private sector pension funds, university endowments, other managed funds, and individuals. Trial Tr. 3921-3924. As the principal portfolio manager for several of Galleon's largest funds, including its flagship Technology Fund, Petitioner personally managed billions of dollars of investors' money through active, research-driven investments in publicly traded securities. *Id.* 4700-4703.

The lifeblood of Galleon's business was market research and professional analysis. At its peak, Galleon employed more than 150 people—including approximately 20 professional portfolio managers, 35 stock analysts, and 30 traders—many with advanced degrees in technology and engineering. Trial Tr.

3918-3919. Those professionals assembled and analyzed publicly available information about the companies in which Galleon invested. *Id.* 3928-3930. In a typical month, Galleon's analysts would review thousands of publicly available "sell-side" analyst reports, news articles, and regulatory filings. *Id.* 3928-3936. Galleon's analysts also lawfully gathered information from the companies themselves, participating regularly in meetings, conference calls, and trade shows with company representatives. *Id*. In short, Galleon's analysts, traders, and portfolio managers, including Petitioner, were daily engaged in the "commonplace" work of professional stock analysts: They regularly "'ferret[ed] out and analyze[d] information,'" including "by meeting with and questioning corporate officers and others who are insiders," to make "judgments as to the market worth of a corporation's securities." *Dirks*, 463 U.S. at 658-659 (citation omitted).

The fruits of this research and analysis were shared among Galleon's analysts, traders, and portfolio managers through internally disseminated written reports and daily and weekly meetings. Trial Tr. 3918, 3934-3941, 3948-3951. On the basis of that rich and constantly evolving mosaic of information, all designed to reflect a better mix of information than was reflected in the market price, Petitioner placed trades in the Galleon funds he managed. By any measure, the pace and volume of Petitioner's trading were astounding. Between 2005 and 2009, Petitioner personally executed more than 36,000 trades in nearly 1000 different securities—transactions collectively worth more than $170

billion. *Id.* 4700-4702. That translates to nearly 30 trades per day—or four trades during every hour that the New York Stock Exchange was open—and more than $140 million per day. *Id.* 4702-4703. A tiny fraction (~0.3%) of those trading decisions—informed by the rigorous, fast-moving process described above, *id.* 4703—formed the basis of Petitioner's arrest, trial, and conviction for insider trading, for which he is serving 11 years in federal prison.

2. A federal criminal indictment charged Petitioner with securities fraud and conspiracy to commit securities fraud. The government built its case primarily around more than 2,200 cellular telephone conversations secretly recorded by the FBI over a period of nine months in 2008. Petitioner moved, pursuant to Title III and the Fourth Amendment, to suppress those conversations as obtained through an illegal wiretap. The district court found that Petitioner had made a "substantial preliminary showing" that the government's wiretap application "recklessly or knowingly misleadingly omitted several key facts." Order, No. 09 Cr. 1184, at 4 (S.D.N.Y. Aug. 12, 2010). The court ordered a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), which provides a suppression remedy under the Fourth Amendment when the government deliberately or recklessly submits a materially false or misleading affidavit to obtain a search warrant. *Id.* at 171-172. Following the evidentiary hearing, the district court found that the government had repeatedly violated its duty of "candor" to the court, had recklessly disregarded the falsity of its allegations of necessity, and had made misleading

statements and omissions throughout its affidavit. Pet. App. 46a-47a, 69a-76a, 88a-89a.

As to probable cause, the district court found that the government's wiretap application had improperly "omitted and misstated important information," including the "[p]articularly disturbing … omission of highly-relevant information … peculiarly probative of [the] credibility" of a key government informant. Pet. App. 46a, 71a. As to necessity, *i.e.*, whether conventional investigative techniques had been tried and failed, the district court found that the government "recklessly failed to disclose that the SEC had been conducting its own insider trading investigation of [Petitioner] upon which the government's criminal investigation substantially relied." *Id.* at 46a. The extensive, three-year-long SEC investigation—the results of which were being shared with the FBI and US Attorney's Office "regularly," *id.* at 90a—was "the most important part of the criminal investigation at the time of the wiretap application" and "employed entirely conventional investigative techniques." *Id.* Without that information, "reasoned evaluation of the necessity of employing wiretaps was impossible." *Id.* at 96a.

In particular, the court found, the "nearly … full and complete *omission* of what investigative procedures in fact had been tried … deprived [the authorizing judge] of the opportunity to assess what a conventional investigation of [Petitioner] could achieve." Pet. App. 93a. It left the district court "at a loss to understand how the government could have

ever believed that [the authorizing judge] could determine whether a wiretap was necessary" without being told about "the millions of documents, witness interviews, and the actual deposition of [Petitioner] himself" that the SEC's conventional techniques had obtained and were continuing to obtain. *Id.* at 88a-89a. The district court concluded that the government—with reckless disregard for the truth—had failed to disclose the "heart and soul" of its investigation "that must be presented to a court if it is to fulfill its function of determining [necessity]," instead making misleading representations about the futility of conventional techniques. *Id.* at 94a-96a, 98a-99a.

Notwithstanding those findings, the district court refused to suppress, concluding that the suppression analysis is governed not by the text of Title III, but rather by *Franks*. Pet. App. 64a-65a, n.12. Based on facts that "emerged from the [*Franks*] hearing"—facts entirely withheld from the government's wiretap application—the court concluded that the government had satisfied the probable cause and necessity requirements. *Id.* at 109a.

3. At trial, the government introduced into evidence 45 wiretap recordings, as well as documentary and testimonial evidence derived from the wiretaps. During its summation, the government repeatedly emphasized that the wiretaps were the "core evidence in this case" for "all the crimes" charged. Trial Tr. 5160, 5583.

Petitioner countered the government's evidence with extensive evidence of his own demonstrating that the allegedly illegal trades were based not on inside information, but instead on Galleon's contemporaneous research and analysis, including voluminous public information and analysis obtained from the more than 100 sell-side firms and other entities that Galleon dealt with daily. *See*, *e.g.*, Trial Tr. 3910-4049, 4070-4266, 4273-4373, 4686-4751. Specifically, the evidence showed that Petitioner, consistent with Galleon's analysis, often began building a position in certain securities—*e.g.*, the "short" position he took in Akamai before the company's quarterly earnings announcement (Counts 8-10)—*before* receiving any alleged inside information. *Id.* 3622-3623, 4022-4050, 4844-4852. The evidence also showed that Petitioner made trades *inconsistent* with the alleged tips he received, *e.g.*, his repeated sale of shares of ATI stock prior to its acquisition by AMD, *id.* 4070-4146, 4809-4816, or the "short" position he took in AMD stock prior to the public announcement of information favorable to AMD, *id.* 3970-3971.

Over Petitioner's objection, and despite the requirement that trades be "on the basis of" inside information, *see O'Hagan*, 521 U.S. at 651-652, the district court instructed the jury that it need find only that inside information was "a factor, however small" in Petitioner's trading activity. Trial Tr. 5624.

4. After almost three weeks of deliberation, the jury found Petitioner guilty of nine counts of securities fraud and five counts of conspiracy to

commit securities fraud. Petitioner subsequently was sentenced to 132 months of imprisonment, a $10 million fine, and a forfeiture of $53.8 million.

5. The Second Circuit affirmed.

a. As to the "factor, however small" instruction, the court of appeals deemed itself bound by circuit precedent holding that the government need not prove causation at all in an insider trading case, but rather need only prove that the defendant traded while in "knowing possession" of inside information. Accordingly, the court concluded that, if anything, the district court's instruction was an error that inured to Petitioner's benefit. Pet. App. 40a-41a. The court of appeals attempted to distinguish *CSX Transportation, Inc. v. McBride*, 131 S. Ct. 2630, 2644 n.14 (2011), which stated that a "no matter how small" causation standard is incompatible with "traditional notions of proximate causation under the ... *securities fraud statutes*," by suggesting that this Court intended to refer only to civil securities fraud actions, not criminal prosecutions. Pet. App. 42a.

b. Relying again on circuit precedent, the court of appeals rejected Petitioner's argument that suppression should be governed by Title III rather than judicially-crafted Fourth Amendment standards. Pet. App. 22a-26a. Although this Court squarely held otherwise in *United States v. Giordano*, 416 U.S. 505 (1974), the Court attempted to distinguish *Giordano* on the ground that it was decided before *Franks*. Pet. App. 25a-26a.

Turning to the district court's finding that the government had acted with reckless disregard for the truth in omitting information about the SEC investigation, the court of appeals stated that the district court erred in "fail[ing] to consider the actual states of mind of the wiretap applicants." Pet. App. 29a. Although it acknowledged the district court's finding that the omitted information was "clearly critical," the court of appeals declared that insufficient. Relying on, *inter alia*, the district court's finding that the government had no deliberate intent to deceive and the government's professed reasons for nondisclosure (reasons the district court found "unpersuasive," *id.* at 98a), the court of appeals concluded that omission of the SEC investigation did not meet *Franks*' *mens rea* threshold. *Id.* at 31a-34a.

Finally, "substantially for the reasons stated in the District Court's analysis," which relied on *Franks*-hearing evidence not presented in the wiretap application, the court of appeals adopted the district court's conclusion that none of the government's misstatements and omissions was material. Pet. App. 34a-36a.

c. The Second Circuit denied rehearing en banc.

REASONS FOR GRANTING CERTIORARI

Petitioner is serving an 11-year sentence for a securities crime that appears in no federal statute, based on the Second Circuit's virtually non-existent standard of causation, which flatly contradicts decisions of this Court and other circuits. Indeed, Petitioner's conviction was made possible only by the

lower courts' acceptance, at the government's urging, of two legal arguments that are fundamentally at odds with both the governing statutes and decisions of this Court and other courts of appeals. This Court should grant certiorari to review the Second Circuit's misguided decision tilting the legal playing field in securities fraud prosecutions—most of which are likely to proceed within the Second Circuit—decidedly in the government's favor.

First, the Court should review the Second Circuit's minority position that trading while in "knowing possession" of inside information violates Section 10(b)—even if that information concededly played no role in the trading decision. As other circuits have explained in rejecting that view, the Second Circuit's rule effectively reads both causation and scienter out of the statute. Section 10(b) targets *fraudulent* acts, and this Court's cases forbid trading "on the basis of" inside information. Yet the Second Circuit has criminalized trading-in-possession without regard to fraudulent intent or whether the information was used in the trading decision.

The "factor, however small" variant that the district court applied here fares no better, and underscores the conflict with this Court's cases. This Court recently stated explicitly that such an exceedingly relaxed causation standard has no place in securities fraud cases. At a bare minimum, the government must prove that inside information played a "substantial role" in trading activity to obtain a securities fraud conviction. Anything less amounts to a presumption of causation in the

government's favor, which this Court has repeatedly refused to allow in criminal cases. Indeed, the SEC has adopted a burden-shifting variant of the "knowing possession" standard in civil cases, recognizing what amounts to narrow affirmative defenses for those who trade while in possession of inside information. The SEC's felt need for such affirmative defenses demonstrates the over-inclusiveness of the Second Circuit's trading-in-possession rule. And needless to say, such burden-shifting does not suffice in criminal cases.

That the Second Circuit alone persists in applying its "knowing possession" standard makes the need for this Court's review all the more pressing. That may be a workable (albeit legally invalid) standard when applied to corporate insiders, but not when applied to professional traders, who of course are concentrated in the Second Circuit. Professional traders perform the economically vital function of assembling better information about publicly traded stocks—information that in turn is conveyed to the market through trading activity. As a practical matter, it is virtually impossible to acquire better information than reflected in the market without occasionally coming into possession of information that could have come from a corporate insider. The Second Circuit's standard thus leaves professional traders under the constant threat of over-zealous prosecutors, who often have no real-world experience with trading practices and little incentive for self-restraint in a climate where many stockholders suffered from market declines, while a few hedge funds and professional traders flourished.

None of this is to suggest that prosecutors must be indifferent to exploitation of inside information by professional traders, but criminal law cannot simply ignore statutory causation demands or the need for clear prophylactic statutory safe harbors of the kind that a common-law crime cannot provide.

Second, this Court should review the Second Circuit's improper expansion of Title III by reading language out of the statute. In recognition of the particularly intrusive nature of wiretaps, Congress crafted a specific set of core requirements for the government to obtain one, and has mandated suppression if the government does not comply. The government plainly violated these requirements, chiefly by failing to disclose to the issuing judge "clearly critical" information regarding the ongoing SEC investigation that rendered meaningful evaluation of the wiretap application "impossible." Pet App. 96a. The Second Circuit's conclusion that these violations did not warrant suppression under more lenient constitutional suppression standards is impossible to reconcile with Title III and this Court's decision in *Giordano*, and widens circuit conflicts.

As the government continues to devote increased resources to bringing insider-trading prosecutions, the need to ensure that these prosecutions are conducted within the bounds of the law is paramount. This Court should grant certiorari and reject the government overreaching that the Second Circuit has approved.

I. The Second Circuit's Minority Position That A Securities Fraud Conviction Requires No Proof That The Defendant *Actually Used* Inside Information Conflicts With Decisions Of This Court And Other Circuits.

A. Courts of appeals are in open conflict on whether causation is an element of an insider-trading offense.

Section 10(b) makes it unlawful to "use" or "employ" any "manipulative or deceptive device," "in connection with the purchase or sale of" any registered security. 15 U.S.C. § 78j(b). As is plain on the face of the statute, one must actually use or employ a manipulative or deceptive device in order to fall within its terms. Thus, in cases involving both trading by insiders and misappropriation by outsiders of inside information, this Court repeatedly has made clear that a defendant violates Section 10(b) only if he actually "*uses the information* to purchase or sell securities." *O'Hagan*, 521 U.S. at 656 (emphasis added)); *see also, e.g.*, *Dirks*, 463 U.S. at 654 ("an insider will be liable … for inside[r] trading only where he fails to disclose material nonpublic information *before trading on it*" (emphasis added)); *Chiarella*, 445 U.S. at 229 ("federal courts have found violations of § 10(b) where corporate insiders *used* undisclosed information for their own benefit" (emphasis added)).

Any other conclusion would make little sense. Although "Section 10(b) is aptly described as a catchall provision," it is axiomatic that "what it

catches must be fraud." *Chiarella*, 445 U.S. at 234-235. Trading "on the basis of material, nonpublic information," *O'Hagan*, 521 U.S. at 652, rises to that high level only when it is, in fact, trading *on the basis* of that information. Indeed, the whole point of rules preventing trading on inside information is "to eliminate '*use of* inside information for personal advantage.'" *Dirks*, 463 U.S. at 662 (emphasis added). When someone merely possesses inside information, but does not actually use it to make trading decisions, there is no fraud for Section 10(b) to prevent.[1]

Nonetheless, at the SEC's urging, the Second Circuit suggested—first in dicta, later in holdings—that Section 10(b) is violated whenever someone trades while in "knowing possession" of inside information. *United States v. Teicher*, 987 F.2d 112, 119-20 (2d Cir. 1993). In doing so, the court did not merely contend that an *inference* of actual use may arise in such situations. Instead, it posited that trading while in "knowing possession" of inside information is *per se* unlawful—even if, for instance,

---

[1] The legislative history of the Securities and Exchange Act reflects the same view. *See, e.g.*, H.R. Rep. No. 73-1383 at 13 (1934) ("Men charged with the administration of other people's money must not *use* inside information for their own advantage." (emphasis added)); S. Rep. No. 73-1455 at 68 (1934) ("it is rendered unlawful for persons [e]ntrusted with the administration of corporate affairs or vested with substantial control over corporations to *use* inside information for their own advantage" (emphasis added)).

the defendant concededly only "execute[d] a previously and legitimately planned transaction" and made no use of the inside information. *Id.* at 119-20. Taking its cue from the SEC, the court deemed it too difficult for the government "to distinguish between legitimate trades" and illegal ones, and thus suggested that, "[a]s a matter of policy," the government should be relieved of this burden in its criminal prosecutions. *Id.* at 121. The court did not definitively answer the question in *Teicher*, however, as it ultimately resolved the case on other grounds. *Id.*

Since *Teicher*, courts and commentators repeatedly and unanimously have rejected the "knowing possession" standard it embraced. *See, e.g.*, *SEC v. Adler*, 137 F.3d 1325, 1336 (11th Cir. 1998) (rejecting in civil context); *United States v. Smith*, 155 F.3d 1051, 1069 (9th Cir. 1998) (rejecting in criminal context); *United States v. Anderson*, 533 F.3d 623, 630 (8th Cir. 2008) (same); Carol B. Swanson, *Insider Trading Madness: Rule 10b5-1 and the Death of Scienter*, 52 U. KAN. L. REV. 147, 209 (2003); Donald C. Langevoort, *Rereading Cady, Roberts: The Ideology and Practice of Insider Trading Regulation*, 99 COLUM. L. REV. 1319, 1334 (1999); Bryan C. Smith, *Possession Versus Use: Reconciling the Letter and the Spirit of Insider Trading Regulation Under Rule 10b-5*, 35 CAL. W. L. REV. 371, 386 (1999); Allan Horwich, *Possession Versus Use: Is There a Causation Element in the Prohibition on Insider Trading?*, 52 BUS. LAW. 1235, 1268 (1997); *cf. SEC v. Lipson*, 278 F.3d 656, 660 (7th Cir. 2002) ("[t]he weight of authority … supports the

[proposition] that the Commission ha[s] the burden … of proving that inside information ha[s] played a causal role in [the] decision to sell").

As Judge O'Scannlain explained for the Ninth Circuit in *Smith*, *Teicher*'s analysis is fundamentally flawed. *See Smith*, 153 F.3d at 1066-69. It is inconsistent with the text of the statute and Rule 10b-5, both of which focus on "*manipulative or deceptive*" activities. 15 U.S.C. § 78j(b) (emphasis added); *see* Rule 10b-5 (making it "unlawful," *inter alia*, "[t]o employ any device, scheme, or artifice *to defraud*" or engage in conduct "which operates or would operate *as a fraud or deceit*" (emphasis added)). It is inconsistent with this Court's repeated statements in cases such as *O'Hagan*, *Dirks*, and *Chiarella* that insider trading requires the actual *use* of inside information. *See Smith*, 153 F.3d at 1067 (collecting quotations). And it is particularly inappropriate in the criminal context, where strict liability crimes are strongly disfavored and even rebuttable presumptions in the government's favor are forbidden. *Id.* at 1069. In short, an actual "use test best comports with precedent and Congressional intent." *Adler*, 137 F.3d at 1337; *see also Anderson*, 533 F.3d at 630 (same).

Notwithstanding this intervening weight of authority rejecting the "knowing possession" standard, in 2008, the Second Circuit casually and unapologetically elevated *Teicher*'s dicta to a holding. *See United States v. Royer*, 549 F.3d 886, 899 (2d Cir. 2008). Without even acknowledging the contrary decisions of its sister circuits—let alone their detailed

debunking of *Teicher*'s reasoning—the court simply declared the matter "previously resolved" by *Teicher*, and stated that "[n]othing that has developed since persuades us of any different result." *Id.* at 899. As a result, in the Second Circuit alone, it is now a crime punishable by 20 years in prison, 15 U.S.C. § 78ff, to trade while in "knowing possession" of inside information—even if that information undisputedly played no meaningful role in the defendant's trading decisions.

B. The Second Circuit's minority position is manifestly wrong.

Not only is the jurisdiction where the vast majority of professional trading activities occur operating under a different legal standard from the rest of the Nation, but the standard under which it is operating is deeply flawed. The Second Circuit's "knowing possession" standard reads both causation and scienter out of the statute. Section 10(b) plainly contemplates "a mental state embracing intent to deceive, manipulate, or defraud." *Smith*, 155 F.3d at 1068. Yet, under the Second Circuit's standard, a defendant would be guilty of violating Section 10(b) even if the inside information did not impact his preexisting trading strategy—indeed, even if he made trading decisions that *directly contradicted* the information. That is no hypothetical. *See* p. 10, *supra.*

That result is fundamentally at odds not only with securities-fraud law, but with basic tenets of criminal law. "The existence of a *mens rea* is the rule of, rather than the exception to, the principles of

Anglo-American criminal jurisprudence." *Dennis v. United States*, 341 U.S. 494, 500 (1951). In keeping with that rule, this Court long has viewed with suspicion government arguments that would produce strict liability crimes and has not hesitated to "read a state-of-mind component into an offense even when the statutory definition did not in terms so provide." *United States v. United States Gypsum Co.,* 438 U.S. 422, 437 (1978). Yet, by eliminating causation altogether, the Second Circuit has read *out* of the statute the fraudulent intent that Congress so clearly intended.

Even the SEC, which has been the prime advocate for eliminating its burden of proving causation, has recognized that it is not really the case "that there is no 'causation' element to an insider trading prosecution." *Smith*, 155 F.3d at 1066. Rule 10b5-1, which expressly adopts a "knowing possession" standard, *accepts* that trading must be "on the basis of" inside information to violate Section 10(b), but then defines that phrase in a manner that deprives it of its clear meaning—defining "on the basis of" to mean only that "the person making the purchase or sale *was aware of the material nonpublic information* when the person made the purchase or sale." 17 C.F.R. § 240.10b5-1(b) (emphasis added). That alone renders the rule dubious enough. *See, e.g.*, *Safeco Ins. Co. of America v. Burr*, 551 U.S. 47, 63 (2007) ("[i]n common talk, the phrase 'based on' indicates a but-for causal relationship"). Moreover, the SEC itself recognizes that a trading-in-possession standard is too over-inclusive to work: The Rule establishes a series of strictly limited "affirmative

defenses" through which a person can demonstrate that, even though he was in "knowing possession" of inside information, his trading was *not* "on the basis of" that information. 17 C.F.R. § 240.10b5-1(b). The SEC thus recognizes that it cannot really pursue people, even civilly, for trading that had nothing to do with their possession of inside information. And yet that is precisely what the Second Circuit's standard allows in criminal cases.

Although district courts within its jurisdiction have been reluctant to apply a strict "knowing possession" standard, the Second Circuit remains unyielding. Here, for instance, the Second Circuit noted that even the district court's parsimonious instruction—that the inside information be "a factor, however small," in Petitioner's trading—"went beyond" what circuit law requires. Pet. App. 41a. Of course, even that minimal effort to reinject some concept of causation—no matter how lax—into Second Circuit law is flatly inconsistent with the statute and this Court's precedent. In approving a "no matter how small" causation standard for negligence claims under the Federal Employers' Liability Act (FELA), the Court expressly distinguished that "relaxed standard of causation" from the "traditional notions of proximate causation" that apply to "*securities fraud statutes*," the text of which does not "assign liability in language akin to FELA's" sweeping language. *CSX Transp.,* 131 S. Ct. at 2644 n.14 (emphasis added); *see also id.* at 2636 ("FELA's language on causation … is as broad as could be framed."). The "traditional notions of proximate causation," *id.*, applicable in the securities

fraud context instead make clear that, at a bare minimum, inside information must be a "*significant* factor" in the trading decision, *Smith*, 155 F.3d at 1066 (emphasis added).

If a "no matter how small" standard is too "relaxed" for Section 10(b) cases, then a "factor, however small" instruction likewise must fail. Yet when Petitioner emphasized *CSX* below, the panel's only response was to insist that *CSX* must have been referencing "suits for *civil* fraud—not *criminal* fraud prosecutions." Pet. App. 43a. That is doubly wrong. First, the same statute governs both civil *and* criminal securities fraud, so it would hardly make sense to treat the same conduct as violating Section 10(b) in one context but not the other. *See Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 173 (1994) ("the text of the statute controls … the scope of conduct prohibited by § 10(b)"); *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) ("we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context"). Second, even if there were some basis for applying two different causation standards to Section 10(b), the rule of lenity would demand application of the more lenient one in the criminal context. *See Burrage v. United States*, 134 S. Ct. 881, 891 (2014).

That general rule applies with special force to Section 10(b), which provides little guidance on what exactly it renders criminal. "[A] criminal statute must give fair warning of the conduct that it makes a crime[.]" *Bouie v. City of Columbus*, 378 U.S. 347,

350 (1964). Yet, here, the governing statute does not even articulate that trading by an outsider while in knowing possession of inside information is a crime—let alone a strict liability crime. Surely if such a crime does exist, Congress must be the one to say so—especially given the serious prison sentences and massive financial penalties at stake. 15 U.S.C. § 78ff.

The lack-of-notice problem with a "knowing possession" or "factor, however small" standard is particularly acute when it comes to professional traders, who are concentrated in the Second Circuit. It is one thing to tell corporate executives and other insiders that they cannot trade in the company stock when they are in possession of inside information. Indeed, Congress has adopted a prophylactic approach to trading by insiders in statutory provisions other than Section 10(b). *E.g.*, 15 U.S.C. § 78p(b). But for professional traders, it places their livelihood in criminal jeopardy. Professional traders like Petitioner are tasked with developing better information than available to others, which, in turn, improves market efficiency. They are bombarded with hundreds of bits of information of varying degrees of reliability and uncertain origins every day. That makes it virtually impossible to wholly avoid coming into contact with information that arguably originated from an inside source. Only a causation standard at least as demanding as "substantial factor" can mitigate the otherwise constant threat of criminal liability.

None of this is to say that the authorities cannot develop additional tools to ensure that professional traders do not trade "on the basis" of inside information. To pick just one example, it is reasonably debatable whether there should be clear prophylactic rules limiting or prohibiting analyst contact with corporate insiders. But such prophylactic rules must recognize that the line between inside information and legitimate information not yet incorporated into the stock price is a fine one. When, as here, no such clear prophylactic prohibitions exist, a test that imposes criminal penalties on a trade where inside information played any role—no matter how small—or no role at all is incompatible with the statute and basic fairness.

C. The causation standard is exceptionally important.

Whether the government must prove causation, and under what standard, in a criminal prosecution for trading "on the basis" of inside information is a question of exceptional importance. "[C]larity and certainty in the criminal law" are a must in any context. *Burrage*, 134 S. Ct. at 891 (rejecting government's argument to apply something less than but-for causation to a criminal statute). Securities fraud is no exception.

As this Court has recognized, "it is essential … to have a guiding principle for those whose daily activities must be limited and instructed by the SEC's inside-trading rules." *Dirks*, 463 U.S. at 664. "Unless the parties have some guidance as to where

the line is between permissible and impermissible disclosures and uses, neither corporate insiders nor analysts can be sure when the line is crossed." *Id.* at 658 n.17. That is particularly true of professional traders. Refraining from trading in a company is a realistic option for corporate insiders who make their living doing something other than analyzing and trading securities. Refraining from trading is simply not an option for securities professionals; they need clear rules.

To be sure, eliminating causation, and thereby criminalizing trading-in-possession, has the virtue of drawing a bright line. But that comes at the expense of an extraordinarily "inhibiting influence on the role of market analysts" whose jobs necessarily entail seeking out as much information about the market as they can lawfully obtain—a function that "the SEC itself [has] recognize[d] is necessary to the preservation of a healthy market." *Dirks*, 463 U.S. at 658. It is "commonplace" for analysts to do their job "by meeting with and questioning corporate officers and others who are insiders." *Id.* If the mere receipt of inside information—even information that is not sought and has no material effect on trading plans—is enough to foreclose them from trading, then it will be nearly impossible for market analysts to continue to do their jobs effectively. And, of course, the "factor, however small" variant here has all the same faults, but without even the bright-line virtue.

As the government made clear, by prosecuting and harshly punishing Petitioner's conduct, it intended to "send[] a clear and unambiguous message

to the public—and specifically to the financial community." Gov't Sentencing Memorandum, 2011 WL 4021120, at *23 (S.D.N.Y. Sept. 9, 2011); *see also, e.g.*, Anna Driggers, *Raj Rajaratnam's Historic Insider Trading Sentence*, 49 AM. CRIM. L. REV. 2021, 2021, 2041 & n.9 (2012) (Petitioner's "unprecedented sentence, coupled with the novel measures taken by prosecutors," was intended to "send a message to Wall Street"). And the Second Circuit's non-existent causation standard, or the district court's feeble variant below, empowers prosecutors to threaten truly draconian punishments. For example, the threat of a securities fraud prosecution under that standard can be combined with aggressive theories of money laundering and respondeat superior liability to demand billions in civil forfeitures, even from those not personally charged with securities fraud. *See, e.g.*, Peter J. Henning, *Going After Steven Cohen's Wallet*, N.Y. TIMES, July 26, 2013.

Needless to say, in the aftermath of the market collapse in late 2008, hedge funds and other professional traders, especially those that turned a profit, are profoundly unpopular. In that climate, meaningful tests of scienter and causation before a trader is sent to prison are essential. And yet the Second Circuit has adopted a test that essentially criminalizes trading-in-possession. As a result, the home to our Nation's financial industry stands alone in applying a standard that courts and commentators alike have concluded is inconsistent with the statute, this Court's precedents, and basic principles of criminal law. That untenable situation warrants this Court's review.

II. The Second Circuit's Refusal To Suppress Despite The Government's "Nearly … Full And Complete *Omission*" Of Critical Information From The Wiretap Application Conflicts With Title III, This Court's Precedent, And The Law Of Other Circuits.

The Second Circuit did not disturb the district court's finding that the government made "nearly a full and complete *omission*" of required information in its wiretap application, Pet. App. 93a, by failing to disclose the SEC investigation, its relationship to the prosecutors' investigation, and related information "clearly critical" to the issuing judge's evaluation of the necessity for a wiretap. *Id.* at 31a-32a. But the Second Circuit nonetheless refused to apply the statutory remedy of suppression, opting instead to apply more permissive judicially-fashioned standards for suppression under the Fourth Amendment's exclusionary rule. *Id.* at 22a-26a. That ruling transgresses the plain terms of the statute, as definitively construed in *United States v. Giordano*, 416 U.S. 505 (1974). And it dilutes even the Fourth Amendment standards, in acknowledged conflict with decisions of other courts of appeals.

A. Title III mandates suppression based on the district court's undisturbed findings.

1. The "overriding congressional concern" in adopting Title III was "the protection of privacy." *Gelbard*, 408 U.S. at 48. Congress authorized wiretaps only "upon compliance with stringent conditions" that implement the congressional policy,

above and beyond Fourth Amendment constraints, "strictly to limit the employment of those techniques." *Id.* at 46-47. Chief among those is Title III's requirement that the government's application provide a "full and complete statement" regarding the probable cause for and necessity of a wiretap, in light of other investigative procedures that have been tried and failed or are likely to fail. 18 U.S.C. § 2518(1)(b) and (c). By allowing wiretaps only when conventional investigative techniques are unworkable, Congress made "doubly sure that the statutory authority" to wiretap would "be used with restraint," rather than "routinely employed as the initial step in criminal investigation." *Giordano*, 416 U.S. at 515. Title III further demands that the judge's probable cause and necessity determinations be made "on the basis of the facts submitted by the applicant," 18 U.S.C. § 2518(3), before the warrant's issuance.

To enforce its commands, Title III mandates suppression if the government "fail[s] 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." *Giordano*, 416 U.S. at 527; *see* 18 U.S.C. § 2518(10)(a). This congressionally commanded suppression remedy is "not limited to constitutional violations" and "does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights." *Giordano*, 416 U.S. at 524, 527; *see also United States v. Jones*, 132 S. Ct. 945, 963 (2012)

(Alito, J., concurring in the judgment) ("Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing" wiretaps, but instead "enacted a comprehensive statute[.]").

This Court held in *Giordano* that the absence of the "prior, informed judgment" of Justice Department officials requires automatic suppression under Title III because it is a "critical precondition to any judicial order." 416 U.S. at 515, 516. That holding *a fortiori* renders the absence of the "prior" and "informed judgment" of the Article III judge issuing that "judicial order" a ground for statutory suppression. Congress's decision to confine federal wiretap authorizations to Article III judges—despite the commonplace role of magistrate judges in authorizing search warrants—underscores the special importance that Congress attached to fully informed and independent judicial review in this context. Surely the "prior, informed judgment" of the authorizing judge, based on full and truthful information, was at least as important to Congress in limiting the use of wiretaps as the Executive Branch's internal-review process.

2. The Second Circuit did not dispute that the government plainly failed to provide the authorizing judge with a "full and complete statement" regarding the necessity of the wiretap. Rather than provide a "full and complete statement" of the "investigative procedures [that] have been tried," 18 U.S.C. § 2518(1)(c), the wiretap application made "nearly a full and complete *omission*" of that information. Pet. App. 93a. Most significantly, the affidavit omitted

description of the SEC investigation long underway and the extensive evidence it had successfully developed utilizing conventional investigation techniques. That SEC investigation was "the most important part," the "sum and substance," "the nuts and bolts," and the "heart and soul" of the criminal investigation in this case. *Id.* at 93a-96a. That "glaring" omission "deprived [the authorizing judge] of the opportunity to assess what a conventional investigation of [Petitioner] could achieve," *id.* at 88a, 93a, and thus rendered "impossible" informed, prior judicial review of the necessity of the wiretap, *id.* at 96a.

The government's probable cause statement likewise deprived the authorizing judge of the ability to evaluate fully the basis for the wiretap. The government misstated or omitted "highly-relevant information" and proffered a "literally false statement" bearing on the credibility of the key informant. Pet. App. 71a, 75a. The government, for example, insisted that the informant had "not yet been charged with any crimes" when in fact the government was aware that she had been convicted of wire fraud. *Id.* at 70a-72a. The government also distorted the content of consensual calls to omit exculpatory details. *Id.* at 73a-75a.

B. The Second Circuit's atextual denial of suppression conflicts with this Court's precedent and the law of other circuits.

1. Despite accepting the district court's finding that the government omitted known and critical information that precluded the issuing judge from

making a reasoned determination of whether a wiretap was necessary, in clear violation of Title III, the Second Circuit nonetheless denied suppression. The Second Circuit did not base its denial on Title III's text—nor could it, as the statute mandates suppression of "any" communication "unlawfully intercepted." 18 U.S.C. § 2518(10)(a)(i); *see Giordano*, 416 U.S. at 524. Instead, the court supplanted Title III's suppression inquiry with rules judicially crafted under the Fourth Amendment for addressing the government's submission of misleading affidavits. Pet. App. 27a-36a. Invoking *Franks v. Delaware*, 438 U.S. 154 (1978), the court concluded that suppression must turn not on whether the government complied with Title III, but rather on whether there is "sufficient content in the warrant affidavit" shorn of reckless or deliberate falsehoods to support issuance of a warrant. *Id.* at 172.

The Second Circuit's substitution of the *statutory* suppression inquiry under Title III with the *constitutional* suppression inquiry under *Franks* cannot be reconciled with this Court's precedent. *Giordano* expressly rejected the argument that Section 2518(10)(a)(i) refers only to communications intercepted in violation of *constitutional* requirements. 416 U.S. at 526, 527, 529. Instead, the Court concluded that Title III required automatic suppression of communications intercepted in violation of a *statutory* requirement. That is because "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." *Id.* at 527. Accordingly, the only question after *Giordano* is whether violation of Title III's "full and complete" statement requirement—frustrating "informed, prior" judicial review of a wiretap's necessity—"directly and substantially implement[s] [the] congressional intention to limit the use of intercept procedures to those situations clearly calling for" it. That question answers itself.

The Second Circuit's sole justification for disregarding *Giordano*'s suppression inquiry was that *Giordano* was decided before *Franks* and other decisions "narrow[ing] the circumstances in which … the exclusionary rule" applies as a matter of *constitutional* law. Pet. App. 26a. Again, that has no bearing on the scope of Title III's *statutory* suppression remedy. This Court could not have been clearer in *Giordano*: Title III suppression "does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights." 416 U.S. at 524.

The legislative history of Title III eliminates any doubt about that. The Senate Report confirms that Congress intended to tie the scope of Title III's suppression remedy to *then* "'present search and seizure law.'" *Giordano*, 416 U.S. at 528 (quoting S. Rep. No. 90-1097, 96 (1968)). As the Court recognized, it was entirely consistent with then "existing search-and-seizure law for Congress to provide for the suppression of evidence obtained in

violation of explicit statutory prohibitions." *Id.* at 528-529. The Court further emphasized the Report's statement that Section 2518(10)(a) "provides for suppression of evidence directly or indirectly obtained 'in violation of the chapter' and that the provision 'should serve to guarantee that the standards of the new chapter will sharply curtail the unlawful interception of wire and oral communications.'" *Id.* at 528 (quoting S. Rep. No. 90-1097 at 96). The Second Circuit's decision does just the opposite.[2]

2. The *Franks* analysis, which requires deliberate or reckless falsehoods as a predicate for suppression, is particularly inapt because *Giordano* rejected the argument that suppression under Title III is warranted only for "willful" statutory violations. *See* 416 U.S. at 525 n.15; *id.* at 529 n.18. The Second Circuit's adoption of *Franks* thus impermissibly imports a *mens rea* element foreign to Title III's suppression remedy.

Indeed, the Second Circuit compounded its error in evaluating the government's mental state by diluting even the *Franks* standard, in conflict with

---

[2] The Second Circuit's conclusion that any limitations on the constitutional exclusionary rule that post-date the enactment of Title III are necessarily incorporated into Title III stands in considerable tension with the conclusion of the Sixth and D.C. Circuits that Title III does not incorporate the good-faith exception delineated in *United States v. Leon*, 468 U.S. 897 (1984). *See United States v. Glover*, 736 F.3d 509, 516 (D.C. Cir. 2013), *pet. for reh'g en banc filed* Jan. 22, 2014; *United States v. Rice*, 478 F.3d 704, 712 (6th Cir. 2007).

the law of other circuits. The district court found that government agents withheld voluminous information "clearly critical" to the issuing judge's determination and that their reasons for doing so were "unpersuasive." Pet. App. 98a-99a. The Second Circuit did not disturb those factual findings, but nevertheless reversed the district court's related conclusion that the government had acted with reckless disregard for the truth. As the Second Circuit acknowledged, *id.* at 30a-31a, its ruling conflicts with decisions of the Third and Eighth Circuits, which both hold that "omissions are made with reckless disregard if an officer withholds a fact in his ken that any reasonable person would have known … was the kind of thing the judge would wish to know." *Wilson v. Russo*, 212 F.3d 781, 788 (3d Cir. 2000) (internal quotation marks and alteration omitted); *United States v. Jacobs*, 986 F.2d 1231, 1234 (8th Cir. 1993). The Second Circuit's contrary conclusion is particularly troubling here given that its primary evidentiary basis for displacing the district court's recklessness finding was self-serving testimony of government agents that they did not intend to mislead. Pet. App. 32a. The result of this doubly diluted standard was the admission of wiretaps despite the government's "glaring" omission of materials any judge would want to review.

3. The Second Circuit's conclusion under *Franks* that the government's omissions were "not material" cannot save its judgment. Pet. App. 34a-35a. The Second Circuit simply adopted the district court's finding that a Title III wiretap *would* have been warranted had the government submitted a

hypothetical affidavit constructed from information supplied several years later. *See, e.g.*, *id.* at 109a (evaluating necessity based on "reasons [that] emerged from the hearing"). But this, too, doubly dilutes the suppression standard—again widening a conflict among the courts of appeals.

Even under *Franks*, the government may not sustain a wiretap affidavit *ex post* using facts that it chose to conceal *ex ante*. Instead, a court must subtract the "material that is the subject of the alleged falsity or reckless disregard" and sustain the warrant only if "there *remains* sufficient content" from the original affidavit to satisfy warrant requirements. *Franks*, 438 U.S. at 171-172 (emphasis added). The Second Circuit's contrary approach conflicts with that of the Seventh and Ninth Circuits, which analyze suppression by considering only the fully truthful allegations included in the affidavit itself. *See Baldwin v. Placer Cty.*, 418 F.3d 966, 971 (9th Cir. 2005); *United States v. Harris*, 464 F.3d 733, 739 (7th Cir. 2006). Indeed, in *Harris*, the Seventh Circuit rejected exactly the type of *post hoc* supplementation of omitted information that the Second Circuit embraced here. 464 F.3d at 739.

A post-wiretap do-over is incompatible with both Title III and the Fourth Amendment, neither of which allows the government effectively to compile an entirely new affidavit based on information never provided to the authorizing judge. *Cf. United States v. United States Dist. Court for E. Dist. of Mich.*, 407 U.S. 297, 317 (1972) (rejecting argument that

government may sustain a wiretap based on *post hoc* judicial affirmation that the wiretap "was a reasonable one which readily would have gained prior judicial approval"). Nor may the government satisfy Title III's pre-warrant command to provide a "full and complete statement" to the authorizing judge by scraping together enough truthful facts from its misleading affidavit, with the benefit of hindsight, to escape suppression. *See Giordano*, 416 U.S. at 533 (rejecting argument that a court should ignore the tainted elements of an application to determine whether remainder would have supported wiretap authority).

More fundamentally, the Second Circuit's materiality holding reveals the basic incompatibility of its analysis with Title III. The court did not reject the district court's finding that the government's failure to inform the authorizing judge of the ongoing SEC investigation made "reasoned evaluation" of its wiretap application "impossible." Pet. App. 96a. And yet the Second Circuit nonetheless concluded that this omission somehow was not material. Both of those things cannot be true under Title III. The statute's "full and complete statement" requirement does not tolerate "nearly a full and complete *omission*" of "clearly critical" information at the "heart and soul" of the government's investigation. *Id.* at 93a-98a. Any legal analysis that suggests otherwise necessarily fails.

4. The Second Circuit's stark departure from Title III's framework is of particular importance in the insider trading and securities fraud context.

Congress confined wiretap authority to "certain major types of offenses and specific categories of crime," and securities fraud is not one of them. 18 U.S.C. §§ 2510 (note), 2516(1). The government therefore must shoehorn the insider-trading activity it seeks to investigate into some other crime, as it did here. *See* Pet. App. 53a (wiretap application predicated on investigation of wire fraud and money laundering, neither of which were ultimately charged).

Perhaps for this reason, or perhaps because "conventional techniques have … proven adequate in the past," this case is the first in which wiretaps have been used to investigate insider trading. Pet. App. 106a. But it will not be the last. This is only the opening salvo of the government's "aggressive use of wiretaps" as a "wake up call for every hedge fund manager and every Wall Street trader and every corporate executive." Press Release, Oct. 16, 2009[3]; Administrative Office of U.S. Courts, 2012 Wiretap Report, Table 7 (wiretap authorizations more than doubled from 2002 to 2012). The Second Circuit, of course, will be home to most of these "aggressive" wiretaps.

* * * * *

The net effect of the Second Circuit's decision is quite remarkable. Criminal statutes are supposed to be enacted by Congress and presumptively require a

---

[3] *Available at* http://www.justice.gov/usao/nys/hedgefund/hedgefundinsidertradingremarks101609.pdf.

showing of *mens rea* to protect the accused. Yet here the Second Circuit has taken what amounts to a common-law crime and essentially eliminated the government's burden to show scienter or causation. Congressional limitations on extraordinary law enforcement tools should be strictly enforced to protect privacy and honor congressional intent. Yet here the Second Circuit applied inapposite law to graft onto Title III *mens rea* and heightened materiality requirements before any unlawfully gathered evidence is suppressed. The combined effect of these errors is to invert the normal presumptions that demand clear warning of what conduct is criminal and require government officers to turn square corners when they seek to use sensitive and privacy-endangering tools. This Court's review is badly needed to restore balance to the Second Circuit and address the multiple conflicts created or exacerbated by the decision below.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Paul D. Clement
Erin E. Murphy
Barbara A. Smith
BANCROFT PLLC

Pratik A. Shah
Counsel of Record
Terence J. Lynam
Samidh Guha
James E. Sherry
Hyland Hunt
AKIN GUMP STRAUSS
HAUER & FELD LLP

Counsel for Petitioner

February 18, 2014

APPENDIX TO THE PETITION FOR A WRIT OF CERTIORARI

TABLE OF CONTENTS

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2012

(Argued: October 25, 2012 Decided: June 24, 2013)

Docket No. 11-4416-cr

UNITED STATES OF AMERICA,

Appellee,

v.

RAJ RAJARATNAM,

Defendant-Appellant.

Before: CABRANES, SACK, and CARNEY, *Circuit Judges*

Defendant-appellant Raj Rajaratnam appeals from an October 25, 2011 judgment of the United States District Court for the Southern District of New York (Richard J. Holwell, *Judge*), convicting him, after a jury trial, on five counts of conspiracy to commit securities fraud, in violation of 18 U.S.C. § 371, and nine counts of securities fraud, in violation of 15 U.S.C. § 78j(b) and 78ff, 17 C.F.R. §§ 240.10b-5 and 240.10b5-2, and 18 U.S.C. § 2. The five charged conspiracies took place between 2003 and 2009 and consisted of Rajaratnam trading securities based on material, non-public information ("inside information") he received from certain individuals about various publicly-traded companies.

Rajaratnam raises two issues for us to consider on appeal. The first issue is whether the District Court should have suppressed the evidence obtained by the government's wiretap of Rajaratnam's cell phone. Specifically, Rajaratnam argues that the District Court erred by applying the analytical framework set forth in *Franks v. Delaware*, 438 U.S. 154 (1978), to determine whether suppression was warranted, and by concluding that the alleged misstatements and omissions in the government's wiretap application did not require suppression.

The second issue concerns the District Court's instruction to the jury that it could convict Rajaratnam of securities fraud if the "material non-public information given to the defendant was a factor, however small, in the defendant's decision to purchase or sell stock." Rajaratnam contends that this instruction was in error and requires us to vacate the substantive counts of conviction for securities fraud (Counts 6 through 14).

Rajaratnam's arguments are not persuasive. In affirming his judgment of conviction, we conclude that: (1) the District Court properly analyzed the alleged misstatements and omissions in the government's wiretap application under the analytical framework prescribed by the Supreme Court in *Franks*; (2) the alleged misstatements and omissions in the wiretap application did not require suppression, both because, contrary to the District Court's conclusion, the government did not omit information about the SEC investigation of Rajaratnam with "reckless disregard for the truth," and because, as the District Court correctly

concluded, all of the alleged misstatements and omissions were not "material"; and (3) the jury instructions on the use of inside information satisfy the "knowing possession" standard that is the law of this Circuit.

Affirmed.

PATRICIA ANN MILLETT (Terence Joseph Lynam, Samidh Guha, Hyland Hunt, James Eamonn Sherry, *on the brief*), Akin Gump Strauss Hauer & Feld LLP, New York, NY, Washington, DC, and Dallas, TX, *for Raj Rajaratnam*.

ANDREW L. FISH (Reed Brodsky, *on the brief*), Assistant United States Attorneys, *for* Preet Bharara, United States Attorney for the Southern District of New York, New York, NY, *for the United States of America*.

Lawrence S. Lustberg, Alicia L. Bannon, Gibbons
P.C., Newark, NJ, *for Amici Curiae Retired Federal Judges*.

Vinoo P. Varghese, Varghese & Associates, P.C., New York, NY, *for Amici Curiae National Legal Aid & Defender Association and the Bronx Defenders*.

Tai H. Park, Park & Jensen LLP, New York, NY;

G. Robert Blakey, Notre Dame Law School,
Notre Dame, IN, *for Amicus Curiae Professor G. Robert Blakey*.

JOSÉ A. CABRANES, *Circuit Judge*:

In this "insider information" securities fraud case, we consider two issues on appeal raised by defend-ant-appellant Raj Rajaratnam. The first issue is whether the United States District Court for the Southern District of New York (Richard J. Holwell, *Judge*) should have suppressed the evidence obtained by the government's wiretap of Rajaratnam's cell phone. Specifically, Rajaratnam argues that the District Court erred by applying the analytical framework set forth in *Franks v. Delaware*, 438 U.S. 154 (1978), to determine whether suppression was warranted, and by concluding that the alleged misstatements and omissions in the government's

wiretap application did not require suppression.[1]

The second issue concerns the District Court's instruction to the jury that it could convict Rajaratnam of securities fraud if the "material non-public information given to the defendant was a factor, however small, in the defendant's decision to purchase or sell stock." Rajaratnam contends that this instruction was in error and requires us to vacate the substantive counts of conviction for securities fraud (Counts 6 through 14).

Rajaratnam's arguments are not persuasive. In affirming the judgment of conviction, we conclude that: (1) the District Court properly analyzed the alleged misstatements and omissions in the government's wiretap application under the analytical framework prescribed by the Supreme Court in Franks; (2) the alleged misstatements and omissions in the wiretap application did not require

---

[1] In his capacity then as a United States District Judge, Judge Gerard E. Lynch approved the first wiretap application on March 7, 2008. As the wiretap authorization expired after a 30-day period, the government filed subsequent wiretap applications. Ultimately, eight wiretap applications were approved by six judges of the United States District Court for the Southern District of New York, including: Judge Lynch, Judge Denise Cote, Judge Deborah A. Batts, Judge Laura Taylor Swain, Judge Richard J. Sullivan, and Judge Denny Chin. Like the parties and the District Court below, because "[t]he first 30 days of wiretapping Rajaratnam yielded enough evidence of criminal conduct to justify renewals of the wiretap," we focus only on the initial wiretap application approved by Judge Lynch. *See United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 WL 4867402, at *7 n.11 (S.D.N.Y. Nov. 24, 2010).

suppression, both because, contrary to the District Court's conclusion, the government did not omit information about the SEC investigation of Rajaratnam with "reckless disregard for the truth," and because, as the District Court correctly concluded, all of the alleged misstatements and omissions were not "material"; and (3) the jury instructions on the use of inside information satisfy the "knowing possession" standard that is the law of this Circuit.

BACKGROUND

Rajaratnam founded and managed the Galleon Group ("Galleon"), a family of hedge funds. When Galleon was at its pinnacle, the fund employed dozens of portfolio managers, analysts, and traders, and invested billions of dollars of client funds.

In 2011, Rajaratnam was indicted on five counts of conspiracy to commit securities fraud, in violation of 18 U.S.C. § 371, and nine counts of securities fraud, in violation of 15 U.S.C. § 78j(b) and 78ff, 17 C.F.R. §§ 240.10b–5 and 240.10b5–2, and 18 U.S.C. § 2. The conduct underlying the five charged conspiracies took place between 2003 and 2009 and consisted of Rajaratnam trading securities based on inside information he received from certain individuals about various publicly-traded companies. The alleged conspiracies involved inside information passed unlawfully to Rajaratnam from: (1) Anil Kumar, a senior partner at McKinsey & Company, Inc. (Counts 4 and 13); (2) Rajiv Goel, an executive of Intel Corporation (Counts 3, 6, 7, and 14); (3) Danielle Chiesi, a portfolio manager at another hedge

fund (Counts 5, 8, 9, and 10); (4) Roomy Khan, a former Galleon employee (Count 2); and (5) other former and current Galleon employees, including one by the name of Adam Smith (Count 1). Joint App'x 268–97.

A. The Wiretap Application

Beginning in 2007, the United States Attorney's Office for the Southern District of New York ("USAO") and the Federal Bureau of Investigation ("FBI") began investigating Rajaratnam based on suspicions that he was using inside information in executing certain securities transactions. On March 7, 2008, the government sought authorization to wiretap Rajaratnam's cell phone. The wiretap application was submitted to then-United States District Judge Gerard E. Lynch and sworn to by then-Assistant United States Attorney ("AUSA") Lauren Goldberg. It included a 53–page affidavit sworn to by FBI Special Agent B.J. Kang.[2] The wiretap application stated that its purpose was to identify Rajaratnam's network of alleged inside sources, to learn how the asserted conspirators operated, and to provide admissible evidence for possible criminal prosecutions. *See id.* at 72.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§

---

[2] For ease of reference, we refer to the government's wiretap application and its accompanying affidavit as "the wiretap application." See note 1, *ante*.

2510–2522, requires that wiretap applications provide "a full and complete statement of the facts and circumstance relied upon by the applicant" to establish probable cause, *id.* § 2518(1)(b), and a "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous," id. § 2518(1)(c).[3] Accordingly, the wiretap application submitted by the government to Judge Lynch addressed (1) why "probable cause" existed to wiretap Rajaratnam's cell phone; and (2) why the proposed wiretap was

---

[3] In full, 18 U.S.C. § 2518(1)(b)-(c) provides:

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

. . .

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

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

"necessary."

To establish "probable cause," the wiretap application set forth, *inter alia*, statements made by Rajaratnam to Roomy Khan (identified as "CS–1"), as well as summaries of conversations between Khan and Rajaratnam that Khan had recorded, which indicated that Rajaratnam and Khan were exchanging material, non-public information used to trade securities. *See* Joint App'x 77–81. To establish "necessity," the wiretap application stated, *inter alia*, that "normal investigative techniques," such as physical surveillance, federal grand jury subpoenas for witness testimony, review of trading records, witness interviews, use of confidential informants, and placement of undercover agents, had been tried and had "failed or reasonably appear[ed] unlikely to succeed if tried." *Id*. at 58, 102–12.

On the basis of these representations, Judge Lynch authorized the wiretap of Rajaratnam's cell phone on March 7, 2008. Seven subsequent wiretap applications were also approved. *See* note 1, *ante*. On October 16, 2009, based in large part on evidence obtained from the wiretap of Rajaratnam's cell phone, Rajaratnam was arrested and charged with multiple counts of securities fraud. He was indicted two months later. A Superseding Indictment was returned on February 9, 2010, and a Second Superseding Indictment was returned on January 20, 2011.

B. Rajaratnam's Suppression Motion

On May 7, 2010, Rajaratnam filed a motion to

suppress the evidence obtained through the wiretap of his cell phone, claiming that the wiretap application contained certain misstatements and omissions. As relevant here, Rajaratnam took issue with the statements supplied on the government's wiretap application regarding both "probable cause" and "necessity."

On the question of "probable cause," Rajaratnam argued that the government made misstatements and omissions regarding the reliability of Roomy Khan. In particular, he observed that the wiretap application stated that Khan "ha[d] not yet been charged with any crimes," Joint App'x 77, and "ha[d] been cooperating with the FBI since approximately November 2007," *id*. at 77 n.4. In fact, in 2001, Khan was indicted and pleaded guilty to felony wire fraud and, in 2002, she began cooperating with the government in an earlier investigation involving Rajaratnam. Rajaratnam also asserted that the wiretap application included two paraphrased summaries of recorded conversations between Khan and Rajaratnam that mischaracterized the actual recorded conversations, as we describe in detail below. *See* Background Part C.ii.a., *post*.

On the question of "necessity," Rajaratnam argued that the wiretap application improperly omitted the fact that Rajaratnam and Galleon had been the subject of an ongoing SEC investigation, which led to, *inter alia*, depositions of Rajaratnam and several other Galleon employees and production for the SEC of approximately four million documents—documents that had thereafter been

conveyed to the USAO.

C. The Franks Hearing

i. The Analytical Framework of Franks v. Delaware

The District Court then decided whether to hold a hearing for the purpose of considering Rajaratnam's suppression motion. In doing so, it noted that "[w]here a defendant makes a preliminary showing that the government's affidavit misstated or omitted material information, Franks instructs a district court to hold a hearing to determine" whether the alleged misstatements or omissions in the warrant or wiretap application were made intentionally or with "reckless disregard for the truth" and, if so, whether any such misstatements or omissions were "material." *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 WL 4867402, at *7–8 (S.D.N.Y. Nov. 24, 2010); *see United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008). In other words, "[t]o suppress evidence obtained pursuant to an affidavit containing erroneous information, the defendant must show that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause [or necessity] finding." *United States v. Canfield*, 212 F.3d 713, 717–18 (2d Cir. 2000) (internal quotation marks omitted); *see also United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003) (noting that "[i]n order to invoke the Franks doctrine, [a defendant] must show that there were *intentional* and *material*

misrepresentations or omissions in [the] warrant affidavit." (emphases supplied)).

To determine whether misstatements are "material," a court must "set[ ] aside the falsehoods" in the application, *United States v. Coreas*, 419 F.3d 151, 155 (2d Cir. 2005), and determine "[w]hether the untainted portions [of the application] suffice to support a probable cause [or necessity] finding," *United States v. Nanni*, 59 F.3d 1425, 1433 (2d Cir. 1995). If the untainted portions of the application are sufficient to support the probable cause or necessity findings, then the misstatements are not "material" and suppression is not required.

Although omissions "are governed by the same rules" as misstatements, *United States v. Ferguson*, 758 F.2d 843, 848 (2d Cir. 1985), "the literal Franks approach [does not] seem[ ] adequate because, by their nature, omissions cannot be deleted"; therefore "[a] better approach . . . would be to . . . insert the omitted truths revealed at the suppression hearing," *United States v. Ippolito*, 774 F.2d 1482, 1487 n.1 (9th Cir. 1985). Accordingly, we have held that "[t]he ultimate inquiry is whether, after putting aside erroneous information and [correcting] material omissions, there remains a residue of independent and lawful information sufficient to support [a finding of] probable cause [or necessity]." *Canfield*, 212 F.3d at 718 (internal quotation marks omitted); *see also United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980) ("[W]e [are] required to determine whether, if the omitted material had been included in the affidavit, the affidavit would still establish probable cause [or necessity] . . . . If it would not, we

would be required to void the warrant and suppress the evidence seized pursuant to it.").

ii. The Hearing

On August 12, 2010, the District Court found that Rajaratnam had "made a substantial preliminary showing" that the government recklessly omitted "several key facts" relating to the "necessity" of wiretapping. *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 WL 3219333, at *2 (S.D.N.Y. Aug. 12, 2010). The Court therefore ordered a Franks hearing on the "necessity" issue. *Id.* However, the District Court rejected Rajaratnam's argument that any misstatements or omissions were material to the existence of probable cause. *Id.* at *1 n.2. Accordingly, the Court did not hold a *Franks* hearing on the "probable cause" issue.[4]

At the *Franks* hearing, which began on October 4, 2010, the District Court heard testimony from (1) Linda Beaudreault, counsel to Galleon and Rajaratnam; (2) Andrew Michaelson, an SEC staff

---

[4] Even though Judge Holwell denied Rajaratnam's request for a *Franks* hearing regarding probable cause, Rajaratnam asked the District Court to reconsider its prior probable cause determination. In its November 24, 2010 Memorandum Opinion and Order, the District Court explained why the alleged misstatements and omissions regarding probable cause were not material. *See Rajaratnam*, 2010 WL 4867402, at *11–13. In particular, Judge Holwell found that "[a]dding . . . all [the evidence] up, and correcting the affidavit to account for the government's misstatements and omissions, the Court believes that there were enough facts for Judge Lynch to have found probable cause." Id. at *13.

attorney who, after the wiretap was authorized, became a Special United States Attorney in order to participate in the investigation by the USAO; (3) FBI Special Agent Kang, the wiretap application affiant; and (4) former AUSA Goldberg, who filed the March 7, 2008 wiretap application.

The *Franks* hearing focused on the alleged misstatements and omissions in the wiretap application. Accordingly, we briefly describe those asserted misstatements and omissions as well as the evidence about the states of the mind of the government agents who filed the wiretap application.[5]

a. Misstatements and Omissions Involving Roomy Khan (CS–1): "Probable Cause"

As noted, Khan served as a cooperating witness for the government and recorded various phone conversations with Rajaratnam, some of which were summarized in the wiretap application and cited as evidence of probable cause.

The District Court determined that the government's wiretap application made two misstatements with regard to Khan's background. First, the wiretap application stated that Khan "has not yet been charged with any crimes," Joint App'x

[5] Even though the District Court concluded that Rajaratnam had failed to demonstrate that a *Franks* hearing was needed on the issue of probable cause, we describe below all the alleged misstatements, including those relating to the "probable cause" determination.

77, when, in fact, she had a prior felony fraud conviction, *see Rajaratnam*, 2010 WL 4867402, at *10. Second, the application stated that Khan "has been cooperating with the FBI since approximately November 2007," Joint App'x 77 n.4, when, in fact, she had cooperated in an earlier insider trading investigation of Rajaratnam which began in the late 1990s, *see Rajaratnam*, 2010 WL 4867402, at *10.

Moreover, the District Court found to be misleading two statements that the government had paraphrased from recorded conversations between Khan and Rajaratnam. With regard to the first paraphrased conversation, the wiretap application stated that, when Khan asked Rajaratnam whether he was "getting anything on Intel," Rajaratnam said "that Intel*148 would be up 9 to 10% and then guide [sic] down 8% and that margins would be good." Joint App'x 79. In fact, Rajaratnam had qualified his predictions about Intel's margins by saying, "I think."[6] *Rajaratnam*, 2010 WL 4867402, at *11. The wiretap application also paraphrased a second conversation between Khan and Rajaratnam as follows:

> During this call, CS–1 [i.e., Khan] asked whether RAJARATNAM had heard anything on Xilinx. RAJARATNAM responded that he

[6] The paraphrased portion of the conversation also omitted "a piece of the conversation in which Rajaratnam said that he thought margins the next quarter 'will be below,' and explained that he took this view '[b]ecause of [sic] the volumes are down, right?'" Rajaratnam, 2010 WL 4867402, at *11 (quoting transcripts of the recorded conversations).

> thought this quarter would be okay, but next quarter would not be so good . . . . RAJARATNAM then said that he expected Xilinx to be "below the street." CS–1 asked whether he got "it" from someone at the company and RAJARATNAM said yes, *somebody who knows*.

Joint App'x 80–81 (emphasis supplied). This paraphrase, however, differed from Rajaratnam's actual answer to Khan's question; instead of saying "somebody who knows," Rajaratnam had in fact said, "Yeah I mean, somebody who knows his stuff." *Rajaratnam*, 2010 WL 4867402, at *11. The District Court found this actual response to be "more equivocal than the government's paraphrase . . . ." *Id.*

b. Omissions Involving the Earlier SEC Investigation: "Necessity"

In addition to the misstatements and omissions involving Khan, the wiretap application also omitted certain information, which was relevant to the issue of "necessity," regarding the ongoing investigation of Rajaratnam being conducted by the SEC.[7] Judge Holwell noted that the *Franks* hearing

[7] The government contends that the wiretap application "disclosed, among other things, information provided to the [USAO and FBI] by the SEC and by Khan" and notes that the wiretap application "reli[ed] on documents collected or information provided by the SEC in seven different places." Gov't's Br. 23. Although the wiretap application refers to the fact that the SEC had passed along some information pertinent

established that the wiretap application did not disclose "that the SEC had for several years been conducting an extensive investigation into the very same activity the wiretap was intended to expose[,] using many of the same techniques the affidavit casually affirmed had been or were unlikely to be successful." *Id.* at *15. Judge Holwell called this a "glaring omission," and stated that he was "at a loss to understand how the government could have ever believed that Judge Lynch could determine whether a wiretap was necessary . . . without knowing about the most important part of th[e] investigation—the millions of documents, witness interviews, and the actual deposition of Rajaratnam himself . . . ." *Id.*

Specifically, the SEC investigation had consisted of the following. In September 2006, the SEC began an investigation of Sedna Capital Management LLC, a hedge fund managed by Rajaratnam's brother. As a result of that investigation, the SEC began focusing on Galleon and Rajaratnam. Beginning in early 2007, the SEC started an on-site investigation of Galleon, through which the SEC: (1) received four million pages of documents and subpoenaed records; (2) interviewed Rajaratnam twice and eighteen Galleon employees as

---

to the criminal investigation of Rajaratnam, *see, e.g.*, Joint App'x 99 ("Based on conversations with the [SEC], I have learned that Santhanam is a risk manager and portfolio manager at Galleon."), it does not suggest the extent of the SEC investigation, the fact that interviews and depositions were taken of Galleon employees, including Rajaratnam, or the fact that the SEC gained access to millions of documents.

well; and (3) formally deposed Rajaratnam under oath. *See id.* at *15–16. In March 2007, the SEC briefed the USAO and the FBI about the investigation and gave these entities access to its investigation files.

The District Court was troubled not only by the fact that the wiretap application did not disclose the existence of the SEC investigation, but also by the apparent consequence that this omission made other statements in the application misleading. *See id.* at *17–18. For example, the wiretap application asserted that interviewing or arresting Rajaratnam or other target subjects "is too risky at the present time," Joint App'x 108–09, despite the fact that the SEC had already interviewed and deposed Rajaratnam. Similarly, the application asserted that requesting additional trading records "would jeopardize the investigation" because "clearing firms . . . sometimes alert the traders to the requests," *id.* at 108,[8] even though the SEC had obtained more than four million documents from Galleon.[9]

c. The States of Mind of the Wiretap Applicants

Finally, at the *Franks* hearing, the government presented testimony designed to demonstrate that

---

[8] The wiretap application did state that "certain" trading records had been reviewed. *See* Joint App'x 108.

[9] The District Court's analysis necessarily assumes that notice of an investigation by *civil* authorities would be viewed by Rajaratnam, or the general public, as notice of an investigation by *criminal* authorities. We doubt that this is the case.

the alleged "omission" in the wiretap application regarding the SEC investigation, such as it may have been, was not made with "reckless disregard for the truth." In particular, former AUSA Goldberg testified that "[n]obody tried to hide" the existence of the SEC investigation. *Franks* Tr. 773. Goldberg also expressed her view that "it would be obvious to anyone reading the affidavit that the SEC was" giving certain information to prosecutors and agents investigating criminal charges. *Id.*; *see also* Gov't's Br. 23 (noting that "Special Agent Kang's affidavit referenced" in seven different places the USAO's and FBI's "reliance on documents collected or information provided by the SEC"). Moreover, the government asserts that, because of recent court decisions arising out of the improper use of civil SEC investigations for criminal prosecutions, the USAO "took pains not to direct the SEC's investigative actions" and, in a similar vein, "did not view the SEC Staff investigation as an alternative law enforcement means to investigate Rajaratnam and his associates." *Id*. at 24 (citations omitted).

iii. The District Court's Decision on Rajaratnam's Suppression Motion

On November 24, 2010, the District Court denied Rajaratnam's suppression motion. *See Rajaratnam*, 2010 WL 4867402, at *28. In analyzing the government's wiretap application under *Franks*, the District Court made three central findings.

First, on the issue of "probable cause," the District Court held that a Franks hearing was unnecessary because the alleged misstatements and

omissions in the wiretap application regarding Khan's prior conviction and cooperation as well as the assertedly misleading paraphrased conversations between Khan and Rajaratnam were not material.[10] Although the District Court found "[p]articularly disturbing . . . the omission of highly-relevant information regarding Khan's prior criminal record," it held that other indicia of Khan's reliability,[11] along with the accurate statements in the wiretap application, "suffice[d] for probable cause" purposes. *Id*. at *11–13.

Second, on the issue of "necessity," the District Court held that the omission of the SEC's investigation of Rajaratnam was made with "reckless

---

[10] The District Court concluded that a Franks hearing was not warranted on the "probable cause" issue because the alleged misstatements and omissions were not "material." *Rajaratnam*, 2010 WL 3219333, at *1 n.2 (rejecting Rajaratnam's argument that the misstatements or omissions were material to the existence of probable cause). It is unclear, however, whether the District Court made a finding regarding whether the misstatements and omissions on the issue of probable cause were made with "reckless disregard for the truth." Although Judge Holwell noted that these deficiencies in the wiretap application "[do not] win high marks for candor" and "evince a lack of [the] frankness that should be found in all ex parte applications," he made no explicit finding that these deficiencies were made with reckless disregard for the truth. *Rajaratnam*, 2010 WL 4867402, at *10–11.

[11] These "indicia" of reliability included the fact that: (1) Khan was a "known in-formant"; (2) she made statements against "her own penal interest"; and (3) the government was able to corroborate some of her statements. Rajaratnam, 2010 WL 4867402, at *12.

disregard for the truth."[12] *See id.* at *19. The District Court summarized its standard for determining whether "reckless disregard" existed as follows: "Rajaratnam must prove that the drafters of the affidavit either intentionally omitted the information or that the omitted information was clearly critical to the affidavit, thereby raising an inference of recklessness." *Id.* at *9 (relying on *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996) (noting that recklessness "may be inferred when omitted information was clearly critical to assessing the legality of the search" (internal quotation marks omitted))).

Third, although the District Court determined that information regarding the SEC investigation was omitted with "reckless disregard for the truth," it concluded that suppression was not warranted because Rajaratnam had failed to show that the omission was "material" to the Court's determination of "necessity." In particular, the District Court held that,

> while the SEC investigation . . . was the bedrock of the prosecutor's own criminal investigation, the SEC investigation had nevertheless failed to fully uncover the scope of Rajaratnam's alleged insider trading ring and was reasonably unlikely to do so because

[12] Although the District Court held that information about the SEC investigation had been omitted with "reckless disregard for the truth," it "comfortably conclude[d] that no one acted with the deliberate intent to mislead Judge Lynch." *Rajaratnam*, 2010 WL 4867402, at *19.

> evidence suggested that Rajaratnam and others conducted their scheme by telephone. Accordingly, disclosure of all the details of the SEC's investigation . . . would ultimately have shown that a wiretap was necessary and appropriate.

Id. at *1.

D. Other Procedural History

Rajaratnam's trial began on March 8, 2011. On May 11, 2011—after a seven-week trial and twelve days of deliberation—the jury returned a verdict convicting Rajaratnam on all nine counts of securities fraud and all five counts of conspiracy to commit securities fraud. On October 13, 2011, Judge Holwell sentenced Rajaratnam to a term of 132 months' imprisonment, followed by 2 years of supervised released.[13] Judge Holwell also ordered Rajaratnam to forfeit $53,816,434 and pay a $10,000,000 fine.

This appeal followed.

DISCUSSION

I. Applying the Analytical Framework of *Franks* to a Title III Wiretap Application

Rajaratnam first argues that the District Court erred by using the analytical framework set

[13] Rajaratnam does not challenge any aspect of his sentence on appeal.

forth in *Franks v. Delaware*, 438 U.S. 154 (1978)—which involved a warrant application for a physical search, not a wiretap—to determine whether the alleged misstatements and omissions in the government's wiretap application required suppression. In particular, he takes issue with the "post hoc factual justification," Rajaratnam's Br. 30, that the *Franks* framework allows—*i.e.*, (1) removing misstatements from the application, *see Coreas*, 419 F.3d at 155; and (2) "insert[ing] the omitted truths revealed at the suppression hearing" after the fact, *Ippolito*, 774 F.2d at 1487 n.1, to determine whether the application would have been granted in any event. Simply put, he asserts that the statute authorizing Title III wiretaps requires suppression because the government's wiretap application did not provide the "full and complete statement" regarding probable cause and necessity, as required by 18 U.S.C. § 2518(1)(b)–(c).

Rajaratnam's argument is foreclosed by settled precedent. In *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), *abrogated on other grounds by Groh v. Ramirez*, 540 U.S. 551 (2004), we noted our agreement "with the district court's application of *Franks* and with its findings" where the government submitted a Title III application for a "roving bug"[14] but omitted information concerning the location where the communications were to be intercepted, as

[14] A "roving bug" is "interception by electronic means of oral communications without specifying in advance exactly where or when the interception would occur." *Bianco*, 998 F.2d at 1117–18.

required under Title III.[15] *Id.* at 1126. Like Rajaratnam, the defendant in *Bianco* specifically asserted that *Franks* was inapplicable and that its application would vitiate Title III's "full and complete" statement requirement. *Id.* at 1125–26. Despite this argument, we held that the "[u]se of the *Franks* standard is consistent with the purposes of [Title III]," and "[i]f anything, *Franks* enhances the protection of . . . defendants, by applying to the wiretap statute an important constitutional principle that has been accepted by all courts." *Id.* at 1126. And in *United States v. Miller*, 116 F.3d 641 (2d Cir. 1997), we applied the analytical framework of *Franks* to a Title III wiretap application that "omitted material information that had been provided by informants who were cooperating with the State." *Id.* at 664. In particular, we held that "[a] challenge to the veracity of such an affidavit will succeed only when it establishes intentional or reckless omissions or false statements that are 'necessary to the finding of probable cause' supporting the wiretap authorization."[16] *Id.* (quoting *Franks*, 438 U.S. at

---

[15] In particular, 18 U.S.C. § 2518(1)(b)(ii) requires: (1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information . . . (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted . . . .

[16] In addition to these two precedents of our Court, *every* Court of Appeals to have considered this question has relied on *Franks* to analyze whether alleged misstatements and omissions in

156, 98 S. Ct. 2674).

Finally, we note that the cases relied on by Rajaratnam—*United States v. Giordano*, 416 U.S. 505 (1974), and *United States v. Gigante*, 538 F.2d

---

Title III wiretap applications warrant suppression. *See, e.g., United States v. Poulsen*, 655 F.3d 492, 505 (6th Cir. 2011) (affirming a district court's denial of a Franks hearing where defendant had failed to make a preliminary showing that a Title III wiretap application affiant had "made any of the purportedly false statements intentionally or with reckless disregard for their truth" (quotation marks omitted)); *United States v. Becton*, 601 F.3d 588, 597–98 (D.C. Cir. 2010) (applying *Franks* to a challenge to a Title III wiretap application); *United States v. Small*, 423 F.3d 1164, 1172 (10th Cir. 2005) ("This court reviews alleged misrepresentations and omissions in a wiretap application under . . . *Franks v. Delaware*." (citation omitted)); *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1110 (9th Cir. 2005) ("To obtain a Franks hearing, defendants must make a preliminary showing that the wiretap applications contained material misrepresentations or omissions."); *United States v. Guerra–Marez*, 928 F.2d 665, 670 (5th Cir. 1991) ("Where, as here, the affidavit falls . . . within the dictates of section 2518, application of the Franks standard is . . . appropriate."); *United States v. Leisure*, 844 F.2d 1347, 1354–57 (8th Cir. 1988) ("noting that affidavits in support of electronic surveillance orders are to be judged by the same standards as conventional search warrants" and applying Franks to a Title III wiretap application); *United States v. Cole*, 807 F.2d 262, 268 (1st Cir. 1986) ("We have read carefully the wiretap application and the testimony adduced at the Franks hearing. We find that the district court properly applied the test required under *Franks v. Delaware* . . . ."); *United States v. Williams*, 737 F.2d 594, 602 (7th Cir.1984) ("In challenging [the Title III wiretap application's] affidavit in the district court, the defendants' task was de-fined by [Franks]: they had to prove that the . . . allegations were intentional lies or made with reckless disregard for the truth.").

502 (2d Cir. 1976)—are not to the contrary. Both cases were decided before the Supreme Court's decision in *Franks* and "[a]t that time there was no good-faith or other exception to the judicially crafted exclusionary rule for violations of the fourth amendment." *Bianco*, 998 F.2d at 1126. When Title III was enacted, it was not intended "generally to press the scope of the suppression role beyond [then current] search and seizure law." S. Rep. No. 90–1097, at 96 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185. But thereafter, *Franks* and other cases, including *United States v. Leon*, 468 U.S. 897 1984), "narrowed the circumstances in which . . . [courts] apply the exclusionary rule." *Bianco*, 998 F.2d at 1126. Although courts were once thought to face a "dilemma of whether [or not] to apply the *Franks* standard to Title III cases," *Bianco*, 998 F.2d at 1126, that supposed dilemma has been definitively resolved, and every Court of Appeals to consider the issue has concluded that the analytical framework of *Franks* is an appropriate standard against which to review allegedly deficient Title III wiretap applications.[17]

In light of these precedents of our Court and our sister Circuits, we hold that the District Court did not err by applying the analytical framework of *Franks* to determine whether the government's wiretap application required suppression.

---

[17] *See* note 16, *ante*.

II. Applying Franks to the Government's Wiretap Application

As noted, Title III requires government agents who file a wiretap application to provide "a full and complete statement of the facts and circumstances relied upon by the application" to establish probable cause, 18 U.S.C. § 2518(1)(b), and a "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous," *id.* § 2518(1)(c). We consider the relevant standard of review and apply it in turn to the District Court's "necessity" and "probable cause" determinations.

A. Standards of Review

It is an axiom of appellate procedure that we review legal questions *de novo* and questions of fact for clear error. *See Pierce v. Underwood*, 487 U.S. 552, 558 (1988). That axiom holds true in the context of *Franks* hearings, *see Awadallah*, 349 F.3d at 65; *United States v. Moore*, 968 F.2d 216, 220–21 (2d Cir. 1992), and therefore our review is similar for each of the issues in this appeal. For instance, whether a person acted with "reckless disregard for the truth" is "a factual question of intent, and we therefore review the court's decision for clear error," *United States v. Trzaska*, 111 F.3d 1019, 1028 (2d Cir. 1997), but a district court's understanding of the "reckless disregard" standard is reviewed *de novo*. Similarly, we review for "clear error" the factual findings that underpin a district court's assessment of probable cause, but we review *de novo* whether a set of facts

satisfies the probable cause standard. *See Ornelas v. United States*, 517 U.S. 690, 699 (1996). Along the same lines, whether a misstatement or omission is "material"—*i.e.*, "[w]hether the untainted portions [of the affidavit] suffice to support a probable cause [or necessity] finding," *Canfield*, 212 F.3d at 717 (citation omitted)—is a mixed question of law and fact reviewed *de novo*, *see Awadallah*, 349 F.3d at 65, but any under-lying factual findings are reviewed for "clear error." An appellate court recognizes "clear error" only when it "is left with a definite and firm conviction that a mistake has been committed." *Brown v. Plata*, 131 S. Ct. 1910, 1930 (2011) (internal quotation marks omitted).

B. "Necessity": Did the District Court Err in Concluding that the Wiretap Application Omitted Information About the SEC Investigation with "Reckless Disregard for the Truth"?

Rajaratnam maintains that the District Court correctly concluded that government agents omitted information about the SEC investigation of Rajaratnam from the wiretap application with "reckless disregard for the truth." In turn, the government argues that the District Court incorrectly applied the "reckless disregard" standard.

The Supreme Court in *Franks* held that misstatements or omissions caused by "negligence or innocent mistake[s]" do not warrant suppression. 438 U.S. at 171. This inquiry, which looks to the mental states of mind of government officials, is said to be a "subjective" test rather than an "objective"

one. *See, e.g., Farmer v. Brennan*, 511 U.S. 825, 838–40 (1994) (discussing the difference between "subjective" and "objective" tests). Whether an individual had a particular mental state "is a question of fact subject to demonstration in the usual ways, including inference from circumstantial evidence," *id.* at 842, but courts must not "confus[e] a mental state with the proof of its existence," *id.* (quotation marks omitted).

Relying on our decision in *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996), the District Court stated that "with respect to material omissions from the March 7, 2008 affidavit, Rajaratnam must prove that the drafters of the affidavit either intentionally omitted the information or that the omitted information was clearly critical to the affidavit, thereby raising an inference of recklessness." *Rajaratnam*, 2010 WL 4867402, at *9. Based on our review of the record, we conclude that the District Court erred in applying the "reckless disregard" standard because the District Court failed to consider the actual states of mind of the wiretap applicants.

A wiretap applicant does not *necessarily* act with "reckless disregard for the truth" simply because he or she omits certain evidence that a reviewing court, in its judgment, considers to be "clearly critical." Rather, the reviewing court must be presented with credible and probative evidence that the omission of information in a wiretap application was "designed to mislead" or was "made in reckless disregard of whether [it] would mislead." *Awadallah*, 349 F.3d at 68 (emphasis and internal quotation

marks omitted). As we have said:

> "An affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation. However, every decision not to include certain information in the affidavit is 'intentional' insofar as it is made knowingly. If . . . this type of 'intentional' omission is all that *Franks* requires, the *Franks* intent prerequisite would be satisfied in almost every case . . . . [Rather,] *Franks* protects against omissions that are *designed to mislead*, or that are made in *reckless disregard of whether they would mislead*, the magistrate."

Id. at 67–68 (quoting *United States v. Colkley*, 899 F.2d 297, 300–01 (4th Cir. 1990) (alterations in *Awadallah*; emphases in *Colkley*)). In a similar vein, the Seventh Circuit has explained:

> To prove reckless disregard for the truth, the defendants [must] prove that the affiant in fact entertained serious doubts as to the truth of his allegations. Because states of mind must be proved circumstantially, a factfinder may infer reckless disregard from circumstances evincing obvious reasons to doubt the veracity of the allegations.

United States v. Whitley, 249 F.3d 614, 621 (7th Cir. 2001) (internal quotation marks and alterations omitted); *see also United States v. Williams*, 718 F.3d 644, 649–50, No. 11–3129, 2013 WL 2149897, at *5

(7th Cir. May 20, 2013) (applying the subjective standard for recklessness to omissions from an affidavit). *But see Wilson v. Russo*, 212 F.3d 781, 788 (3d Cir. 2000) ("[O]missions are made with reckless disregard if an officer withholds a fact in his ken that '[a]ny reasonable person would have known . . . was the kind of thing the judge would wish to know.' " (quoting *United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993))).

Of course, the "reckless disregard" aspect of a *Franks* inquiry can sometimes be inferred from the omission of critical information in a wiretap application. *See Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991) ("Recklessness *may* be inferred where the omitted information was clearly critical to the probable cause determination." (emphasis supplied) (internal quotation marks omitted)). Subjective intent, after all, is often demonstrated with objective evidence. But such an inference is not to be automatically drawn simply because a reasonable person would have included the omitted information, *cf. Farmer*, 511 U.S. at 842, 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.

In this case, Judge Holwell's view that the SEC investigation was "clearly critical" is the only basis for his conclusion that the government omitted certain information about that investigation with

"reckless disregard for the truth." But as we now review *all* of the evidence presented at the *Franks* hearing, it points in the opposite direction. And, despite the inferences that Judge Holwell drew from the omitted "clearly critical" information, when discussing the subjective state of mind of each affiant, he too "comfortably conclude[d] that no one acted with the deliberate intent to mislead Judge Lynch." *Rajaratnam*, 2010 WL 4867402, at *19.

The evidence presented at the *Franks* hearing showed that no one in the USAO acted with "reckless disregard for the truth" by not detailing the SEC investigation of Rajaratnam. Former AUSA Goldberg testified that, when she "was drafting the affidavit, it never occurred to [her], never crossed [her] mind to put a section in [the wiretap application] that [discussed the] SEC investigation . . . . [because] [she] didn't think about the SEC investigation as an alternative technique that was available to FBI agents, because [the USAO] can't direct them what to do." *Franks* Tr. 819. Similarly, FBI Special Agent Kang testified that he "didn't think about including [the SEC investigation] in a criminal affidavit. . . . We just didn't really think about it." Although the District Court believed that this civil investigation by the SEC was relevant to the issue of necessity, the evidence presented at the *Franks* hearing in no way suggested that omitting certain information about SEC investigation was "designed to mislead" or was made with "reckless disregard of whether [it] would mislead." *Awadallah*, 349 F.3d at 68 (internal quotation marks and emphasis omitted). Indeed, the evidence indicates that the wiretap application was reviewed by

supervisors at the USAO, none of whom thought that additional information about the SEC's civil investigation needed to be included.

On a more fundamental level, we cannot conclude that the government omitted certain information about the SEC investigation with "reckless disregard for the truth" when it is clear that fully disclosing the details of that investigation would only have *strengthened* the wiretap application's "necessity" showing.[18] The District Court tacitly recognized this fact, stating that "[m]any of the same documents that were used to compile the SEC chronologies strongly suggested that Rajaratnam had been careful to exchange nearly all of his inside information by telephone." *Rajaratnam*, 2010 WL 4867402, at *21; *cf. United States v. Young*, 822 F.2d 1234, 1237 (2d Cir. 1987) ("[W]iretapping is particularly appropriate when the telephone is routinely relied on to conduct the criminal enterprise under investigation." (quotation marks omitted)). The District Court made the point explicitly in discussing whether the government should have pursued additional "normal investigative procedures" before seeking a Title III wiretap:

> Could or should the government have done

---

[18] In addition to its relevance to the "materiality" inquiry, whether an omission would have strengthened or weakened the wiretap application is also probative of whether the omission occurred with "reckless disregard for the truth." Indeed, it is difficult to imagine a situation where the government would intentionally or "with reckless disregard" omit information that would *strengthen* its "probable cause" or "necessity" showing.

> more with conventional techniques to test whether a wiretap was "necessary"? It is hard to make that argument with regard to document subpoenas, search warrants, and other forms of documentary investigation. Over four million documents from targets and third parties had already been gathered. *Analysis of the documentary evidence was fairly sophisticated and while this revealed much circumstantial evidence of insider trading it also confirmed what one would expect: insider trading is typically conducted verbally*. Thus it seems reasonably unlikely that additional documents would have produced qualitatively different evidence.

Rajaratnam, 2010 WL 4867402, at *22 (emphasis supplied). In other words, the evidence does not support the inference that the government omitted information from a wiretap application with "reckless disregard for the truth," and such an inference seems ever more inappropriate where the information omitted would only have further supported the government's position.

After reviewing the evidence in the record—especially the *Franks* hearing testimony regarding the states of mind of the government agents—and applying the correct understanding of reckless disregard, we conclude that the record does not support the finding that the omission of the SEC investigation in the Title III wiretap application was made with "reckless disregard for the truth."

In any event, even if we were to assume,

arguendo, the opposite conclusion—that government officials omitted information about the SEC investigation with "reckless disregard for the truth"—we are persuaded that this omission was not material, substantially for the reasons stated in the District Court's analysis on that issue. *Rajaratnam*, 2010 WL 4867402, at *21–24 (holding that the wiretap application, as corrected, was sufficient to support a finding of "necessity").

C. "Probable Cause": Did the District Court Correctly Determine that the Wiretap Application's Misstatements About Khan and "Paraphrasings" Did Not Require Suppression?

Rajaratnam argues that the District Court also erred by concluding that the alleged deficiencies in the wiretap application regarding probable cause were not "material," and therefore that suppression was not required.[19] Specifically, he argues that the

---

[19] We note that Rajaratnam challenges the District Court's conclusion as to materiality generally and does not specifically challenge the District Court's determination that he did not make a preliminary showing that the wiretap application included material misstatements or omissions sufficient to justify a *Franks* hearing as to probable cause. We also recognize uncertainty both in our own Circuit and in our sister Circuits as to whether to review the denial of a *Franks* hearing for clear error or *de novo*. *See Falso*, 544 F.3d at 126 n.21. Moreover, it is unclear whether either of these standards is appropriate, inasmuch as that we generally review discretionary decisions on whether a district court ought to conduct a hearing for "abuse of discretion." *See United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992). Nonetheless, we need not decide the appropriate

"probable-cause determination comes up short when the materially false and misleading allegations of probable cause are eliminated, because the government's recklessly false and misleading claims about Roomy Khan and her conversations with [Rajaratnam] were the heart of its probable cause allegations." Rajaratnam's Br. 50.

We disagree because, even assuming, *arguendo*, that these alleged misstatements and omissions regarding Roomy Khan and the two paraphrased conversations between Khan and Rajaratnam were indeed made with "reckless disregard for the truth,"[20] we agree with the District Court that they were not "material," substantially for the reasons stated in the District Court's analysis on that issue. *See Rajaratnam*, 2010 WL 4867402, at *11–13 ("Adding it all up, and correcting the affidavit to account for the government's misstatements and omissions, the Court believes that there were enough facts for Judge Lynch to have found probable

---

standard of review here, because we conclude, for the reasons stated above, that the District Court did not err in denying a *Franks* hearing as to probable cause under any of these standards.

[20] As noted above, *see* note 10, *ante*, the District Court did not conduct a Franks hearing on the "probable cause" issue because it determined that Rajaratnam had not made a sufficient preliminary showing that the alleged misstatements and omissions were "material." *Rajaratnam*, 2010 WL 3219333, at *1 n.2. Because it is unclear whether the District Court determined that the misstatements and omissions regarding probable cause were made with "reckless disregard for the truth," we only consider whether those misstatements and omissions were "material."

cause.").[21]

III. Were the Jury Instructions on the Use of Inside Information Erroneous?

Finally, Rajaratnam argues that his convictions on the substantive securities fraud counts (Counts 6 through 14) should be vacated because the District Court instructed the jury that it could convict Rajaratnam if the "material non-public information given to the defendant *was a factor, however small*, in the defendant's decision to purchase or sell stock." Joint App'x 433 (emphasis supplied). In particular, he asserts that the emphasized fragment of the jury instructions allowed the jury to convict him without finding the necessary causal connection between the inside information he possessed and the trades he executed. On appeal, our review of jury instructions for legal error is *de novo*. *See United States v. Robinson*, 702 F.3d 22, 30 (2d Cir. 2012).

"Insider trading—unlawful trading in securities based on material non-public information—is well established as a violation of section 10(b) of the Securities Exchange Act of 1934 and Rule 10b–5."[22] *SEC v. Obus*, 693 F.3d 276, 284 (2d Cir. 2012).

---

[21] Indeed, although the District Court found "[p]articularly disturbing . . . the omission of highly-relevant information regarding Khan's prior criminal record," *Rajaratnam*, 2010 WL 4867402, at *11, it held that other indicia of Khan's reliability along with the accurate statements in the wiretap application "suffice[d] for probable cause" purposes, *id*. at *13.

[22] In relevant part, § 10(b) of the Securities Exchange Act of 1934 provides:

There are two theories of insider trading: (1) a "classical theory" involving corporate insiders, and (2) a "misappropriation theory" involving "persons who are not corporate insiders but to whom material non-public information has been entrusted in confidence and who breach a fiduciary duty to the source of the information to gain personal profit in the securities market." *Id*. The second of these theories is at issue in this case. As relevant here, it "holds that a person commits fraud 'in connection with' a securities

---

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange—

. . .

(b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [Securities and Ex-change] Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

15 U.S.C. § 78j (emphasis supplied). Pursuant to its § 10(b) rulemaking authority, the SEC adopted Rule 10b–5, which, as relevant here, provides:

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

(a) To employ any device, scheme, or artifice to defraud,

. . . or

(c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person,

in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b–5 (emphasis supplied).

transaction, and thereby violates § 10(b) and Rule 10b–5, when he misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information." *United States v. O'Hagan*, 521 U.S. 642, 652 (1997).[23]

---

[23] The Supreme Court further explained the misappropriation theory as follows: "In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information." *O'Hagan*, 521 U.S. at 652; *see also* 17 C.F.R. § 240.10b5–2(b) (defining "duties of trust or confidence" under Section 10(b) and Rule 10b–5 as circumstances where "a person agrees to maintain information in confidence" or where "the person communicating the material nonpublic information and the person to whom it is communicated have a history, pattern, or practice of sharing confidences, such that the recipient of the information knows or reasonably should know that the person communicating the material nonpublic information expects that the recipient will maintain its confidentiality"). In other words, the misappropriation theory focuses on the relationship between the trader and the insider and "is thus designed to protect the integrity of the securities markets against abuses by 'outsiders' to a corporation who have access to confidential information that will affect the corporation's security price when revealed, but who owe no fiduciary or other duty to that corporation's shareholders." *Id*. at 653 (internal quotation marks and brackets omitted).

As relevant here, we have also clarified that "Section 10(b) and Rule 10b–5 also reach situations where the insider or misappropriator tips another who trades on the information." *Obus*, 693 F.3d at 285. Accordingly, "[w]hen an unlawful tip occurs, the tippee is . . . liable if he knows or should know that the information was received from one who breached a fiduciary duty (such as an insider or a misappropriator) and the tippee

In *United States v. Teicher*, 987 F.2d 112 (2d Cir. 1993), we stated, *in dicta*, that a "knowing possession" standard satisfied the "in connection with" requirement of § 10(b) and Rule 10b–5, *see* note 22, *ante*, despite the defendant's argument that a "causal connection" was required between the inside information and the executed transaction. *Id.* at 120-21. In discussing the appropriate standard, we noted that "[a] number of factors weigh in favor of a 'knowing possession' standard," including that: (1) "§ 10(b) and Rule 10b–5 require only that a deceptive practice be conducted in connection with the purchase or sale of a security"; (2) "a knowing possession standard com-ports with the oft-quoted maxim that one with a fiduciary or similar duty to hold material nonpublic information in confidence must either disclose or abstain with regard to trading"; and (3) "a knowing possession standard has the attribute of simplicity." *Id.* at 120 (internal quotation marks omitted).

Fifteen years later, in *United States v. Royer*, 549 F.3d 886 (2d Cir. 2008), we elevated the dicta of *Teicher* to the law of the Circuit, when we "ad-here[d] to the knowing possession standard articulated in *Teicher*," which "was the product of sustained and detailed consideration . . . ." *Id.* at 899. In doing so, we noted that no developments since *Teicher* persuaded us to resolve the issue differently and, "[o]n the contrary, the SEC['s] subsequent[ ] enact[ment] [of] Rule 10b5–1," counseled in favor of

---

trades or tips for personal benefit with the requisite scienter." *Id.* (relying on *Dirks v. SEC*, 463 U.S. 646, 660 (1983)).

applying the knowing possession standard.[24] *Id*.

Like the jury instructions in *Royer*,[25] the phrase deployed by Judge Holwell ("was a factor, however small") was "if anything *more favorable*," *id*. at 899 n.12 (emphasis supplied), to Rajaratnam than the "knowing possession" standard that is the law of this Circuit. Instead of instructing the jury that "[i]t is sufficient if the government proves that the defendant [ ] purchased or sold securities while knowingly in possession of the material nonpublic information," *Teicher*, 987 F.2d at 119, the instructions given by Judge Holwell, if anything, went beyond the "knowing possession" standard because they required that the inside information be "a factor, however small, in the defendant's decision to purchase or sell stock," Joint App'x 433.[26]

---

[24] In relevant part, Rule 10b5–1(b) provides:

[A] purchase or sale of a security of an issuer is "on the basis of" material non-public information about that security or issuer if the person making the purchase or sale was aware of the material nonpublic information when the person made the purchase or sale.

17 C.F.R. § 240.10b5–1(b).

[25] Specifically, the jury instructions contested in *Royer* stated: "A purchase or sale of a security is 'on the basis of' material non-public information about that security, if the person making the purchase or sale was aware of the material non-public information when the person made the purchase or sale, *and the information in some way informed the investment decision*." 549 F.3d at 899 n.12 (emphasis in original).

[26] Indeed, any alleged error in the jury instructions in this case operated to the benefit of Rajaratnam and was therefore harmless. *See Neder v. United States*, 527 U.S. 1, 9–10 (1999)

Undeterred by these precedents, Rajaratnam argues that the Supreme Court's recent decision in *CSX Transportation, Inc. v. McBride*, 131 S. Ct. 2630 (2011), casts doubt on the law of our Circuit. We are not persuaded. In *CSX Transportation*, the Supreme Court held that, under the Federal Employers' Liability Act ("FELA"), a railroad worker need only demonstrate that the rail-road's negligence "played a part—no matter how small—in bringing about the injury." *Id*. at 2644. Rajaratnam relies on *CSX Transportation* because the Court noted that the statutory causation requirement in the FELA—that the injury "result[ ] in whole or in part from [the defendant's] negligence"—was "as broad as could be framed," *id*. at 2636, and it contrasted the FELA causation requirement with "traditional notions of proximate causation under the RICO, antitrust, and *securities fraud statutes*," *id*. at 2644 n.14 (emphasis supplied). In substance, Rajaratnam contends that the Supreme Court's reasoning in *CSX Transportation* implies that securities fraud cases require some causation element greater than the formulation that the inside information "played a part—no matter how small."

To the contrary, the Supreme Court's statements about the FELA causation requirement and the causation requirement in "securities fraud statutes," do not call into question our decisions in *Royer* and *Teicher*. Indeed, the Supreme Court's reference to "securities fraud statutes" in *CSX*

(collecting cases applying harmless-error review to jury instructions in criminal cases).

Transportation was accompanied by a citation to *Dura Pharmaceuticals, Inc. v. Broudo*, 544 U.S. 336 (2005), which addressed suits for *civil* fraud—not *criminal* fraud prosecutions. *Compare id.* at 343 ("Judicially implied private securities fraud actions resemble in many (but not all) respects common-law deceit and misrepresentation actions."), *with Neder v. United States*, 527 U.S. 1, 25 (1999) ("By prohibiting the 'scheme to defraud,' rather than the completed fraud, the elements of reliance and damage would clearly be inconsistent with the statutes Congress enacted."). Moreover, as noted above, the District Court's jury instructions are consistent with SEC Rule 10b5–1, which clarifies that "a purchase or sale of a security of an issuer is 'on the basis of' material nonpublic information . . . if the person making the purchase or sale *was aware* of the material nonpublic information when the person made the purchase or sale." 17 C.F.R. § 240.10b5–1(b) (emphasis supplied).

CONCLUSION

To summarize, we hold that:

(1) The District Court properly analyzed the misstatements and omissions in the government's Title III wiretap application under the analytical frame-work prescribed by the Supreme Court in *Franks v. Delaware*, 438 U.S. 154 (1978);

(2) The alleged misstatements and omissions in the wiretap application did not require suppression, because (a) contrary to the District Court's conclusion, the government did not omit information about the SEC investigation of Rajaratnam with

"reckless disregard for the truth," and (b) as the District Court correctly concluded, all of the alleged misstatements and omissions in the wiretap application were not "material";

(3) The District Court's jury instructions on the use of inside information—which instructed the jury that it could convict Rajaratnam if the "material non-public information given to the defendant was a factor, however small, in the defendant's decision to purchase or sell stock"—satisfied the "knowing possession" standard that is the law of this Circuit. For the reasons stated, we **AFFIRM** the District Court's October 25, 2011 judgment of conviction.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, -against- RAJ RAJARATNAM and DANIELLE CHIESI, Defendants.	09 Cr. 1184 (RJH) **MEMORANDUM OPINION AND ORDER**

Richard J. Holwell, District Judge:

Defendants Raj Rajaratnam ("Rajaratnam") and Danielle Chiesi ("Chiesi") have moved to suppress the Title III material gathered by the government's wiretaps of their respective phones. Each makes four separate arguments for suppression in full or part: (1) the government was not entitled to use wiretaps to investigate insider trading, a crime not specified in Title III; (2) the government's application and supporting affidavits failed to establish probable cause; (3) the government's application and supporting affidavits failed to establish the inadequacy of conventional investigative procedures and, therefore, the "necessity" of using wiretaps; and (4) the government failed to minimize various conversations.

The Court concludes that defendants' arguments do not justify suppression and therefore denies both motions. Because Title III authorizes the government to use wiretaps to investigate wire fraud, the government was authorized to use wiretaps to investigate a fraudulent insider trading scheme using interstate wires even though Title III does not specifically authorize wiretaps to investigate insider trading alone.

With regard to probable cause, Chiesi has failed to show that the government's wiretap application contained material misstatements or omissions, or was otherwise deficient in showing probable cause. Rajaratnam has shown that the government's application omitted and misstated important information regarding the credibility of a key government informant, Roomy Kahn, but suppression is not required because the remainder of the affidavit demonstrated ample reason to find probable cause.

Chiesi has likewise failed to make a preliminary showing that the government's wiretap application was deficient in showing that a wiretap was necessary. As for Rajaratnam, necessity presents a closer question. Earlier this year, the Court found that Rajaratnam had made a substantial preliminary showing that the government recklessly failed to disclose that the SEC had been conducting its own insider trading investigation of Rajaratnam upon which the government's criminal investigation substantially relied. A four-day hearing last month confirms in the Court's judgment that the government failed to disclose the nature and extent

of the SEC investigation even though (1) that investigation was the most important part of the criminal investigation at the time of the wiretap application and (2) that investigation employed entirely conventional investigative techniques. Given that an issuing court relies on the government candidly to disclose the full nature and scope of its investigation in order to determine whether a wiretap is necessary, the omissions here are troubling to say the least. But that is not the end of the matter. The hearing also demonstrated that, while the SEC investigation used conventional techniques and was the bedrock of the prosecutor's own criminal investigation, the SEC investigation had nevertheless failed to fully uncover the scope of Rajaratnam's alleged insider trading ring and was reasonably unlikely to do so because evidence suggested that Rajaratnam and others conducted their scheme by telephone. Accordingly, disclosure of all the details of the SEC's investigation that the government recklessly omitted would ultimately have shown that a wiretap was necessary and appropriate.

Finally, the government complied with its statutory responsibility to minimize recording calls unrelated to the crimes the government had probable cause to suspect.

BACKGROUND

The United States Attorney's Office for this district ("USAO") and the FBI began the criminal investigation resulting in the indictment of

Rajaratnam in 2007.[1] The investigation of Chiesi apparently did not begin until later, sometime in mid–2008. In connection with these investigations, the government sought and obtained authorization to wiretap Rajaratnam's and Chiesi's phones.

The government first sought authorization to wiretap Rajaratnam's cell phone in an application submitted to Judge Lynch on March 7, 2008. (Gov't Opp'n to Rajaratnam Ex. 1–A.) Attached to that sworn application was a 53–page affidavit of FBI Special Agent B.J. Kang ("Kang"). (Gov't Opp'n to Rajaratnam Ex. 1–C.) Judge Lynch granted the application for a 30–day wiretap, finding (1) probable cause that Rajaratnam and others were involved, *inter alia,* in wire fraud the extent of which would be revealed through the interception of telephone communications, and (2) that a wiretap was necessary in that normal investigative techniques were or would be unlikely to succeed in uncovering the fraud. (Gov't Opp'n to Rajaratnam Ex. 1–D.) The government began intercepting communications over Rajaratnam's phone on or about March 10. Thereafter, the government applied for authorization to continue intercepting Rajaratnam's phone for another 30 days. (Gov't Opp'n to Rajaratnam Exs. 2–A, 2–C.) On April 8, Judge Cote granted that application. (Gov't Opp'n to Rajaratnam Ex. 2–D.)

---

[1] The USAO and the FBI are referred to separately and together as "the government" or, occasionally, "the prosecutor" or "the criminal authorities." The Securities and Exchange Commission is referred to as the SEC throughout.

The government applied for reauthorization six more times, between May and November of 2008, each application based substantially on intercepts over Rajaratnam's phone, and each application authorized by a judge in this district. (Gov't Opp'n to Rajaratnam Exs. 3–D, 4–1, 5–D, 6–D, 7–D, 8–D.)

On August 13, 2008, the government applied for authorization to wiretap three phones that Chiesi subscribed to and used. (Gov't Opp'n to Chiesi, Exs. 1–A, 1–B, 1–C.) Judge Sullivan granted the request that day. (Gov't Opp'n to Chiesi Ex. 1–D.) He approved a second 30–day application on September 12, 2008. (Gov't Opp'n to Chiesi Ex. 2–D.)

On October 16, 2009, Rajaratnam, Chiesi, and others were arrested and charged with multiple counts of conspiracy and securities fraud. The original indictment was returned against both defendants on December 15, 2009, and a superseding indictment was returned on February 9, 2010 (Gov't Opp'n to Rajaratnam Ex. 12).

Both defendants moved to suppress the evidence that the government obtained through the wiretaps on their phones. In connection therewith, Rajaratnam requested a hearing under *Franks v. Delaware,* 438 U.S. 154 (1978) (a *"Franks* hearing"). In *Franks,* the Supreme Court held that, despite the "presumption of validity with respect to the affidavit supporting [a] search warrant", a defendant can challenge an affidavit "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the

affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause . . . ." *Id.* at 155–56.[2] The Court denied Rajaratnam's request for a *Franks* hearing regarding probable cause but found that he had "at least established good grounds for holding a *Franks* hearing regarding the veracity of the [Kang] affidavit and the issue *vel non* of whether the necessity requirement has been satisfied." *United States v. Rajaratnam,* 2010 WL 3219333, at * *1–2 (S.D.N.Y. Aug. 12, 2010). The Court reserved judgment on other aspects of the defendants' motion to suppress. (July 27, 2010 Hr'g Tr. at 157.) In his post-hearing submission, Rajaratnam asked the Court to reconsider its prior holding regarding probable cause. (*See* Rajaratnam Post Hr'g Br. at 47–49.)[3]

DISCUSSION

Rajaratnam's and Chiesi's motions raise essentially the same arguments. First, they argue that Title III does not authorize the use of wiretaps to

---

[2] In *Franks v. Delaware,* 438 U.S. 154 (1978), the Supreme Court further held that, "[i]n the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Id.* at 156.

[3] Citations abbreviated "Br.", "Opp'n", or "Rep. Br." refer to the parties' initial submissions. Citations to papers' abbreviated "Post Hr'g Br.", "Post Hr'g Opp'n" or "Post Hr'g Reply Br." refer to the parties' submissions following the *Franks* hearing.

investigate insider trading, an offense not specifically mentioned in the statute. They also argue that the government's wiretap affidavits in this case failed to establish (i) probable cause to use a wiretap and (ii) that wiretapping was necessary to the government's investigation. Finally, both argue that the government did not properly minimize its interceptions, which they say justifies suppression in part or full. The Court addresses each of these arguments in turn.

I. Use of Title III to Investigate Insider Trading

When a court authorizes a wiretap, Title III requires that it "specify the offenses in connection with which the permission was granted . . . ." *United States v. Masciarelli,* 558 F.2d 1064, 1067 (2d Cir. 1977); *see* 18 U.S.C. § 2518(1)(b)(i), (3)(b), 4(c). Wiretaps may only be authorized to investigate offenses specified in Section 2516. *See* 18 U.S.C. § 2516. Still, the statute recognizes that "a law enforcement officer lawfully engaged in a search for evidence of one crime" may happen upon evidence of another crime not specified in the court's authorization order-and perhaps not specified in Section 2516 either. *Masciarelli,* 558 F .2d at 1067. When that happens, "the public interest militates against [the officer's] being required to ignore what is in plain view." *Id.* Thus Title III contains what is in some sense a plain-view exception, which allows the government to offer evidence of other crimes when that evidence is obtained during the course of an investigation for an authorized offense. *See id.;* 18 U.S.C. § 2517(5). Specifically, Section 2517(5)

provides that:

> [w]hen 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 used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

18 U.S.C. § 2517(5).[4]

Under the terms of Section 2517(5), the government can only use wiretap evidence of crimes "other than those specified" in the authorization order or in Section 2516 by obtaining judicial approval "as soon as practicable." The section "does not specify the exact form an application for subsequent approval should take, nor exactly what procedures a court should follow in giving or denying its authorization." *United States v. Gerena,* 653 F.

[4] Section 2517(3) allows for the disclosure of wiretap evidence "while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof." 18 U.S.C. § 2517(3).

Supp. 974, 978 (D. Conn. 1987). Thus courts in this circuit have looked to Congress's intent in enacting the provision, and have consistently applied the following test: the government must show that "the original order was lawfully obtained, that it was sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order." *United States v. Marion,* 535 F.2d 697, 700 (2d Cir. 1976) (quoting S. Rep. No. 90–1097, at 12 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2189). Courts treat these standards less as independent prongs than as various ways of stating the government's obligations. The government must obtain wiretap warrants in good faith—that is, in connection with an offense for which Title III permits wiretapping-not as a subterfuge for gathering evidence of other offenses. If the government does so, any other evidence it happens to intercept will have been intercepted incidentally. *See United States v. Levine,* 690 F. Supp. 1165, 1171 (E.D.N.Y. 1988).

In this case, the government's actions do not reflect subterfuge. The wiretap applications candidly detailed the nature of the scheme for which wiretaps were sought. They described the evidence of an insider trading conspiracy that involved Rajaratnam and Chiesi; they stated that the evidence established probable cause of wire fraud and money laundering; and they noted that the evidence would also establish probable cause of the defendants' participation in securities fraud, although that crime was not an authorized predicate offense under Title III. (*See, e.g.,* Gov't Opp'n to Rajaratnam Ex. 1–C at 3 & n.1; Gov't Opp'n to Chiesi Ex. 1–C at 3 & n.1.) In other

words, the government made quite clear that it wanted to use wiretaps to investigate an insider trading conspiracy, and that the investigation would likely uncover evidence of wire fraud and money laundering (offenses for which Title III specifically permits wiretaps) and securities fraud (an offense for which it does not). *Cf. Levine,* 690 F. Supp. at 1170 ("A factor pertinent to the determination of good faith may be whether the officials concealed from the judge issuing or extending the original warrant the fact that they foresaw a high likelihood that evidence of other crimes would be revealed. To hide that fact might give rise to an inference of bad faith.").[5] With all these facts in hand, several judges in this district found probable cause that Rajaratnam and Chiesi had committed or would commit the crimes of wire fraud and money laundering.[6] Accordingly, all

---

[5] 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. (*Cf.* Rajaratnam Br. at 63.) 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, *see United States v. Levine,* 690 F. Supp. 1165, 1171 (E.D.N.Y. 1988), 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 the wiretap to begin with.

[6] These findings are entitled to substantial deference. *See United States v. Wagner,* 989 F.2d 69, 72 (2d Cir. 1993) ("A reviewing court must accord substantial deference to the finding of an issuing judicial officer that probable cause exists.").

authorized the use of wiretaps in connection with the government's investigation.

Still, defendants say the government should not be allowed to use wiretap intercepts as evidence of securities fraud here. They argue that the interception of communications evidencing securities fraud could not have been incidental, because (1) it was the government's primary objective; (2) at a minimum it was anticipated; and (3) to so hold would undermine Congress's intent in enacting Title III. Each of these arguments is unavailing.

Defendants contend that the government's primary objective in using wiretaps was to drum up evidence of securities fraud, as shown by the wiretap applications' focus on insider trading as opposed to wire fraud. But defendants' argument unrealistically assumes a gulf between these two crimes. Securities fraud does contain an additional element, "fraud in connection with the purchase or sale of any security"; and wire fraud does require the "use of interstate wires." *United States v. Regensberg,* 604 F. Supp. 2d 625, 634 (S.D.N.Y. 2009). But unlikely is the insider trading scheme that uses no interstate wires. Sometimes the government even charges both kinds of fraud for the same core conduct, a practice that Congress, in the legislative history of the Insider Trading and Securities Fraud Enforcement Act of 1988, and the Supreme Court have both endorsed. *See* H.R. Rep. 100–910, at 29 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6074 (stating that the government can "litigate insider trading cases based on other provisions of the securities laws and of the general mail and wire fraud statutes"); *United States*

v. Carpenter, 484 U.S. 19, 28 (1987) (holding that conspiracy to trade on confidential information was within "the reach of the mail and wire fraud statutes, provided the other elements of the offenses are satisfied"). Here the government had evidence of insider trading with a wire. (*See* Gov't Opp'n to Rajaratnam Ex. 1–C ¶¶ 7, 10, 11, 18, 19.) Therefore it makes little sense to call securities fraud a primary objective and wire fraud a "fig leaf" (Rajaratnam Reply Br. at 40).

Of course, there is no denying that, in intercepting communications that would provide evidence of wire fraud, the government expected to get evidence of securities fraud, too. In that way this case is different from the usual one involving Section 2517(5), where the government gets permission to investigate one crime using a wiretap, and while doing so happens upon an entirely different crime. *Cf. United States v. Gotti,* 42 F. Supp. 2d 252, 269–70 (S.D.N.Y. 1999) (Parker, J.) (evidence of access device fraud was incidentally intercepted during the course of a lawfully executed order authorizing the interception of communications relating to money laundering); *United States v. Giordano,* 259 F. Supp. 2d 146, 153–155 (D. Conn. 2003) (evidence of sex offense with minor was incidentally intercepted during the lawfully authorized interception of communications relating to corruption and racketeering activities). Here, by contrast, the government wiretapped phones seeking evidence of conduct that would violate both the criminal statute for which wiretapping was authorized as well as another criminal law. Defendants say that this sort of anticipated interception cannot count as

incidental.

If the test were inadvertence, the defendants would be right. But that is not the test. "Incidental," not "inadvertent," is the word used in Title Ill's legislative history. And, although the Second Circuit has sometimes used the word "inadvertent" in dicta, more recent authority has implicitly rejected that gloss on the standard. *Compare Marion,* 535 F.2d at 701 ("Without a judge's determination of inadvertence, Title III authorization might rapidly degenerate into . . . the electronic equivalent of a general search warrant.") (internal quotation marks omitted), *and Masciarelli,* 558 F.2d at 1067 (when an officer "inadvertently comes upon evidence of another crime," he should not be required to "ignore" it), *with In re Grand Jury Subpoena Served on John Doe,* 889 F.2d 384, 388 (2d Cir. 1989) (finding that a wiretap, which was expected to reveal evidence of both the authorized crime and another crime, intercepted evidence of the second crime incidentally), *and United States v. Wager,* No. 00–Cr.–629, 2002 WL 31106351, at *2, *4 (S.D.N.Y. Sept. 20, 2002) (finding that evidence of securities fraud was intercepted incidentally, despite the fact that the government's original warrant application had noted that there was probable cause of securities fraud); *see also United States v. McKinnon,* 721 F.2d 19, 22–23 (1st Cir.1983) ("While an interception that is unanticipated is *a fortiori* incidental, the converse is not true: something does not have to be unanticipated to be incidental. Evidence of crimes other than those authorized in a wiretap warrant are intercepted 'incidentally' when they are the by-product of a bona fide investigation of crimes specified in a valid

warrant."); *cf. United States v. Gambino,* 734 F. Supp. 1084, 1094 n.14 (S.D.N.Y. 1990) (deciding not to reach the question whether the standard is "inadvertent" or "incidental"). In *In re Grand Jury Subpoena,* the government expected to, and did, intercept conversations relating to the "theft of federal, state and local taxes," although wiretapping was only authorized in connection with the state law crime of grand larceny for the theft of state taxes. 889 F.2d at 388. Notwithstanding those expectations, and notwithstanding that Section 2516 excludes federal tax crimes, the Second Circuit held that the federal crime evidence was intercepted incidentally because it was a by-product of the government's bona fide investigation of state law crimes. *Id.* Here, too, the interception of evidence of securities fraud was a by-product of the interception of evidence of wire fraud.

According to the defendants, allowing the government to use wiretapping in any insider trading case would subvert the intention of Congress, which has yet to add securities fraud to the list of predicate offenses in Section 2516. (*See* Rajaratnam Br. at 60.) But this Court does not hold that insider trading is always good grounds for a wiretap. It holds only that, 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. The government must still show, as six judges found that it did in this case, that it is investigating wire fraud in good faith. Defendants would have this Court bar the government from using wiretaps for wire fraud

investigations whenever the fraud concerns securities.[7] That is a carve-out Congress has not made and this Court is not permitted to make in its stead.[8]

Assuming that the government's wiretap applications established both probable cause and necessity-issues that the Court is about to address-

---

[7] Defendants deny that they are asking for an absolute bar. (July 27, 2010 Hr'g Tr. ("Tr.") at 48.) They say the government may still use a wiretap where it demonstrates a need to do so that is particularized to wire fraud, rather than to insider trading. This makes little sense. To be sure, the government does have an obligation to show why a wiretap is necessary in a particular investigation. But in a wire fraud investigation where the underlying fraud is insider trading, the government's showing of necessity will always be linked to insider trading. (It will be required to show why alternative investigative techniques would not suffice to ferret out the fraud in that case.) In practice the defendants' logic would limit the use of wiretaps to only those kinds of wire fraud, like bank or computer fraud, where the underlying fraud is itself specified in Section 2516. That is not what the statute says.

[8] It is true that, since adding wire fraud to Section 2516, Congress has added other kinds of fraud to the statute—access device fraud in 1986, bank fraud in 1990, aircraft parts fraud in 2000, computer fraud in 2001—without adding securities fraud. (*See* Rajaratnam Reply Br. at 37.) Congress inserted offenses like bank and computer fraud to Title III because it wanted to permit wiretapping to investigate those crimes even where they do not involve the use of a wire. As the government observed at oral argument, "[n]ot every bank . . . or computer fraud may involve wires. There are cases that don't." (Tr. 56.) Securities fraud may be committed without a wire, too, and in such cases, Title III precludes wiretapping. But that does not mean it precludes wiretapping in insider trading cases where a wire is involved.

the wiretap applications here were approved in accordance with Title III. Therefore, under Section 2517(5), the government can introduce evidence of insider trading it discovered on the wiretaps as long as the government applied to do so "as soon as practicable." 18 U.S.C. § 2517(5). On October 14, 2009, just before Rajaratnam's arrest, the government applied for and Judge Preska issued an order allowing the government to introduce wiretap evidence of securities fraud. (*See* Gov't Opp'n to Rajaratnam Ex. 9.)[9] Accordingly, the government can introduce wiretap evidence under Section 2517(5).

---

[9] The government may have had authorization well before that time. The Second Circuit has long held that "authorization under 18 U.S.C. § 2517(5) may be inferred when a judicial officer grants a continuation of the surveillance, even though the offense was not listed in the original order, so long as he was made aware of 'material facts constituting or clearly relating to [the] other offenses' in the application for the continuance." *United States v. Ardito,* 782 F.2d 358, 362 (2d Cir. 1986) (quoting *United States v. Masciarelli,* 558 F.2d 1064, 1067–1068 (2d Cir. 1977)). The government's applications to renew the Rajaratnam and Chiesi wiretaps clearly provided the issuing judges with notice that another offense, securities fraud, was implicated by the intercepts. Because courts "presume . . . that in renewing the tap the judge carefully scrutinized those supporting papers and determined that the statute's requirements had been satisfied," *United States v. Marion,* 535 F.2d 697, 703 (2d Cir. 1976), the renewal orders sufficed to provide Section 2517(5) approval. *See United States v. Tortorello,* 480 F.2d 764, 783 (2d Cir. 1973), *cert. denied,* 414 U.S. 866 (1974) ("It is enough [for Section 2517(5)] that notification of the interception of evidence not authorized by the original order be clearly provided in the renewal and amendment application papers.").

II. Probable Cause

A. Standard

Title III requires that law enforcement provide the authorizing court with a "full and complete statement of the facts and circumstances relied upon by the applicant" to establish probable cause that the target phone was and would continue to be used to commit the specified offense of wire fraud. 18 U.S.C. § 2518(1)(b). "The standard for probable cause applicable to § 2518 is 'the same as the standard for a regular search warrant.'" *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)).

"[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates,* 462 U.S. 213, 232 (1983). "While probable cause requires more than a 'mere suspicion' of wrongdoing, its focus is on 'probabilities,' not 'hard certainties.'" *Walczyk v. Rio,* 496 F.3d 139, 156 (2d Cir. 2007) (quoting *Gates,* 462 U.S. at 231) (internal citation omitted). "[P]robable cause does not demand any showing that a good-faith belief be 'correct or more likely true than false.' It requires only such facts as make wrongdoing or the discovery of evidence thereof probable." *Walczyk,* 496 F.3d at 157 (quoting *Texas v. Brown,* 460 U.S. 730, 742 (1983)) (internal citation omitted). "In determining whether probable cause for an eavesdropping warrant exists, the issuing officer need only make a practical, common sense decision whether, given the 'totality of the circumstances' set

forth in the affidavit requesting such warrant, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that evidence of a crime will be obtained through the use of electronic surveillance." *United States v. Funderbunk,* 492 F. Supp. 2d 223, 237 (W.D.N.Y. 2007) (quoting *Gates,* 462 U.S. at 238); *see also Diaz,* 176 F.3d at 110. Allegations in an affidavit "should be read in their entirety and in a common-sense manner with each fact gaining color from the others," rather than "in isolation" from one another. *Gotti,* 42 F. Supp. 2d at 262.

"[A]reviewing court must accord considerable deference to the probable cause determination of the issuing [judge]." *Walczyk,* 496 F.3d at 157; *see 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 . . . ."); *United States v. Miller,* 116 F.3d 641, 663 (2d Cir. 1997) ("In reviewing a ruling on a motion to suppress wiretap evidence, we accord deference to the district court . . . ."); *United States v. Torres,* 901 F.2d 205, 231 (2d Cir. 1990), *cert. denied,* 498 U .S. 906 (1990) ("The role of an appeals court in reviewing the issuance of a wiretap order . . . is not to make a de novo determination of sufficiency as if it were a district judge, but to decide if the facts set forth in the application were minimally adequate to support the determination that was made."). The reviewing court's task is "limited to determining whether that judicial officer had a 'substantial basis' for her determination." *Gotti,* 42 F. Supp. 2d at 262 (quoting *Gates,* 462 U.S. at 239). Nevertheless, little or no deference is due where the government's affidavit

misstated or omitted material information about probable cause. *See 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.").

Where a defendant makes a preliminary showing that the government's affidavit misstated or omitted material information, *Franks* instructs a district court to hold a hearing to determine if the misstatements or omissions were made intentionally or with reckless disregard, and if so, determine *de novo* whether, "after setting aside the falsehoods, what remains of the warrant affidavit is insufficient to support a finding of probable cause." *United States v. Coreas,* 419 F.3d 151, 155 (2d Cir. 2005).[10] "Omissions from an affidavit that are claimed to be material are governed by the same rules." *United States v. Ferguson,* 758 F.2d 843, 848 (2d Cir. 1985). But "[i]f an affidavit can be challenged because of material omissions, the literal *Franks* approach no

[10] The government argues that, "to the extent [the defendants'] challenges . . . don't involve alleged omissions and inaccuracies, the judicial determination warrants considerable deference." (Tr. at 58.) But it is hard to imagine how exactly this would work in practice. Reading the March 7, 2008 Kang Affidavit as a whole, Judge Lynch found probable cause. But how did he reach that conclusion? By relying exclusively on Khan's allegations? By deciding that the Goel tips added something to the case for probable cause? Short of asking Judge Lynch himself, it is not possible to know. Put simply, there are no determinate findings (besides the finding of probable cause itself) for this Court to defer to.

longer seems adequate because, by their nature, omissions cannot be deleted." *United States v. Ippolito,* 774 F.2d 1482, 1486 n.1 (9th Cir. 1985). "The ultimate inquiry is whether, after putting aside erroneous information and [correcting] material omissions, there remains a residue of independent and lawful information sufficient to support probable cause." *Canfield,* 212 F.3d at 718 (internal quotation marks omitted).

B. Rajaratnam's Claims

Rajaratnam contends that the government's application and supporting affidavit dated March 7, 2008,[11] (1) made false allegations regarding Roomy Khan's reliability and (2) mischaracterized other evidence referenced in the affidavits. As noted, he sought a *Franks* hearing to probe this issue.[12] The

---

[11] This is the crucial affidavit; if its deficiencies justify suppression, they justify suppression of all the wiretap intercepts, even those obtained on the strength of subsequent applications. *See United States v. Giordano,* 416 U.S. 505, 531–533 (1974) (Because "communications intercepted pursuant to the extension order were evidence derived from the communications invalidly intercepted pursuant to the initial order," they are "derivative evidence and must be suppressed"). The converse is also true: if the March 7, 2008 affidavit adequately supported Judge Lynch's decision to authorize a 30–day wiretap, any deficiencies in subsequent wiretap applications are of no consequence. The first 30 days of wiretapping Rajaratnam yielded enough evidence of criminal conduct to justify renewals of the wiretap.

[12] Rajaratnam's brief implies that even if a *Franks* hearing is not warranted, the Court should nevertheless suppress the wiretap intercepts under Section 2518(10)(a)(i) because the government failed to supply a "full and complete statement"

Court denied defendant's request for a hearing on the issue of probable cause in summary form in its order of August 15, 2010. The Court now sets forth its reasoning.

1. *Legal Standard*

Under *Franks,* a defendant may obtain an evidentiary hearing where (1) "the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit," and (2) "the allegedly false statement is necessary to the finding of probable cause." 438 U.S. at 155–56. To have misled knowingly or recklessly, the government must have done more than make an intentional decision not to include the information. Instead, the misleading statement or omission must have been "designed to mislead" or "made in reckless disregard of whether [it] would mislead." *United States v. Awadallah,* 349 F.3d 42, 68 (2d Cir. 2003) (quoting *United States v. Colkley,* 899 F.2d 297, 300–01 (4th Cir. 1990) (formatting normalized)).

---

explaining the basis for probable cause and the reasons why alternative investigative techniques would not be feasible. (*See* Rajaratnam Br. at 56; *see also* Tr. at 17 ("The full and complete statement standard in Title III is actually distinct from the constitutional standard in *Franks.*"); Tr. 116–17.) But that argument, for which the brief cites no authority, is inconsistent with the law of this circuit. *See United States v. Bianco,* 998 F.2d 1112, 1125–26 (2d Cir. 1993) (holding that the *Franks* standard governs the determination whether suppression is appropriate under Section 2518(10)(a)).

The meaning of recklessness is not "self-evident." *United States v. Mandell,* 710 F. Supp. 2d 368, 373 (S.D.N.Y. 2010). The Supreme Court in *Franks* did not define the term "reckless disregard" other than to state that "[a]llegations of negligence or innocent mistake are insufficient." *Franks,* 430 U.S. at 171. Nor has the Second Circuit conclusively defined "reckless disregard." *United States v. Perez,* 247 F. Supp. 2d 459, 473 (S.D.N.Y. 2003). Nevertheless, "most circuits that have considered the question have embraced a subjective test for recklessness." *United States v. Vilar,* No. 05–CR–621, 2007 WL 1075041, at *26 (S.D.N.Y. Apr. 4, 2007) (Karas, J.).

Under that test, as one court in this Circuit has phrased it, "the question is not what a reasonably prudent person would have appreciated given the attendant circumstances but rather whether the defendant in fact entertained serious doubts as to the truth of the subject statements." *United States v. Kunen,* 323 F. Supp. 2d 390, 395 (E.D.N.Y. 2004) (internal quotation marks omitted); *see also Vilar,* 2007 WL 1075041, at *26 ("[O]ne 'recklessly disregards' the truth when one makes allegations while entertaining serious doubts about the accuracy of those allegations."). Indeed, numerous lower courts in this Circuit have employed the "serious doubts" language. *See Mandell,* 710 F. Supp. 2d at 373; *Vilar,* 2007 WL 1075041, at *26; *United States v. Harper,* No. 05–CR–6068, 2006 WL 2873662, at *8 (W.D.N.Y. Oct. 6, 2006); *United States v. Goldenberg,* No. 05–CR–1034, 2006 WL 266564, at *4 (S.D.N.Y. Feb. 3, 2006); *Perez,* 247 F. Supp. 2d at 473, 479; *United States v. Markey,* 131 F. Supp. 2d 316, 324 (D.

Conn. 2001); *Kunen,* 323 F. Supp. 2d at 395. Other Courts of Appeals have used the same language. *See United States v. Butler,* 594 F.3d 955, 961 (8th Cir. 2010); *United States v. Lowe,* 516 F.3d 580, 584 (7th Cir. 2008); *Miller v. Prince George's County, Md.,* 475 F.3d 621, 627 (4th Cir. 2007); *United States v. Ranney,* 298 F.3d 74, 78 (1st Cir. 2002); *Wilson v. Russo,* 212 F.3d 781, 788 (3d Cir. 2000); *Hart v. O'Brien,* 127 F.3d 424, 449 (5th Cir. 1997), *abrogated in part on other grounds by Kalina v. Fletcher,* 522 U.S. 118 (1997); *Beard v. City of Northglenn, Colo .,* 24 F.3d 110, 116 (10th Cir.1994).

While the test for recklessness may be subjective, it is not wholly so and there are objective aspects to its application. Thus, "[t]here is a corollary to the 'serious doubt' standard: 'Because states of mind must be proved circumstantially, a fact finder may infer reckless disregard from circumstances evincing 'obvious reasons to doubt the veracity of the allegations.'" *Perez,* 247 F. Supp. 2d at 473 (quoting *United States v. Whitley,* 249 F.3d 614, 621 (7th Cir. 2001)); *see also United States v. Schmitz,* 181 F.3d 981, 986–87 (8th Cir. 1999); *Ranney,* 298 F.3d at 78; *Beard,* 24 at 116; *Vilar,* 2007 WL 1075041, at *27; *Markey,* 131 F. Supp. 2d at 324. Hence, as to any misstatements in the May 7, 2008 affidavit, Rajaratnam must prove either that "(1) the drafters of the affidavit made [a false statement] with knowledge that the statement was false, (2) they had a serious doubt as to the truth of the statement when they made it, *or* (3) they had obvious reason to doubt the veracity of the statement." *Perez,* 247 F. Supp. 2d at 474 (emphasis added).

As might be expected, the guideposts for determining recklessness are different when evaluating the alleged omission of material information. It makes little sense after all to speak of whether the affiant has 'serious doubt' about the veracity of statements not made. Rather the inquiry, at least in this circuit, is whether the "omitted information was clearly critical to assessing the legality of the search." *United States v. Reilly,* 76 F.3d 1271, 1280 (2d Cir. 1996) (internal quotation marks omitted). Accordingly, with respect to material omissions from the March 7, 2008 affidavit, Rajaratnam must prove that the drafters of the affidavit either intentionally omitted the information or that the omitted information was clearly critical to the affidavit, thereby raising an inference of recklessness.[13]

---

[13] There is some disagreement among the Courts of Appeals, and within this Court, as to whether recklessness can be established where a reasonable affiant would know that omitted information would be important to the reviewing court. That divide stems from the Third Circuit's statement that "omissions are made with reckless disregard if an officer withholds facts in his ken that '[a]ny reasonable person would know was the kind of thing the judge would wish to know.'" *Wilson,* 212 F.3d at 788 (quoting *United States v. Jacobs,* 986 F.2d 1231, 1235 (8th Cir. 1993)). Two decisions have cited this statement in holding that the standard for omissions is whether "any reasonable person would have known that this was the kind of information that the magistrate judge would have wanted to know." *Perez,* 247 F. Supp. 2d at 474 (Chin, J.); *United States v. Harding,* 273 F. Supp. 2d 411, 426 (S.D.N.Y. 2003) (Kaplan, J.) ("[T]he preliminary issue to be resolved is whether Harding has shown that Agent Castro knew or had reason to know the 'facts' he omitted from the search warrant affidavit. If these facts indeed

2. *Knowingly or Recklessly False Statements and Omissions*

In support of probable cause, the March 7, 2008 Kang Affidavit offered several pieces of evidence: (1) statements made by Roomy Khan, a cooperating witness, about exchanging inside information with Rajaratnam; (2) statements Rajaratnam made to Khan in telephone conversations she recorded at the FBI's request; and (3) summaries of conversations intercepted over wiretapped telephones belonging to Craig Drimal, who worked out of Galleon's offices, and Zvi Goffer, who worked as a trader for Galleon.

Describing the "Background of the Investigation," the affidavit said that, "[b]eginning in or about November 2007 [Agent Kang] and other FBI agents have had numerous discussions with a cooperating source ('CS–1')" we now know to be Khan. (Gov't Opp'n to Rajaratnam Ex. 1–C at 12.)

---

were 'in his ken,' the following question is whether they were the sort of facts a reasonable person would know a judge would want to know."). On the other hand, in Judge Karas's view, "a test that invokes the mythical 'reasonable person' speaks the language of negligence" which is insufficient for suppression under *Franks*. *Vilar,* 2007 WL 1075041, at *27. This Court agrees. Unlike negligence, reckless disregard connotes "[c]onscious indifference to the consequences of an act." Black's Law Dict. (9th ed.). The "serious doubt" standard for misstatements reflects that awareness, as does the corollary that with regard to omissions, recklessness "may be inferred when omitted information was clearly critical to assessing the legality of the search". *United States v. Reilly,* 76 F.3d 1271, 1280 (2d Cir. 1996) (internal quotation marks omitted).

According to Agent Kang, Khan "ha[d] been cooperating with the FBI since approximately November 2007." (*Id* . at 13 n.4.) Kang further stated that "since at least in or about 2005, [Khan] participated in an insider trading scheme;" that Khan "received the material, nonpublic information from a variety of sources, . . . including RAJARATNAM"; and that Khan "has not yet been charged with any crimes." (*Id.* at 13.) The affidavit notes that Khan has known Rajaratnam "since in or about the mid–1990s, when [s]he was working at Intel Corp," and that she subsequently "worked for Galleon from approximately mid–1998 through 1999." (*Id.* at 13 n.5.) It goes on to say that the two exchanged inside information beginning "in or about mid–2005" and continuing till "late 2007." (*Id.* at 13–14.)

This is what the affidavit left out: The FBI and U.S. Attorney's Office for the Northern District of California began investigating Khan in 1998 when she was working at Intel, in connection with allegations that she was sending inside information about her company to Rajaratnam's firm. (Rajaratnam Br. Ex. A.5 at 2–3.) In 2001 Khan was indicted and later that year pleaded guilty to felony wire fraud and was sentenced to probation.[14]

---

[14] Khan's 2001 criminal case, No. 01–20029 (N.D. Cal.), remained under seal in the Northern District of California, for reasons not explained, until late 2009. On October 16, 2009, the government unsealed the criminal complaint against Rajaratnam in this case, which had identified Khan as "CW." Khan's true identity was reported by the Wall Street Journal on October 22, 2009. Susan Pulliam, *Galleon Sinks, Informant Surfaces,* Wall St. J., Oct. 22, 2009. The same day, the *San Jose*

(Rajaratnam Br. Ex. A.3, A.4 ¶¶ 1–2; Ex. A.6 at 2, 4.) At Khan's sentencing in 2002, the government emphasized that Khan was cooperating with the government, that it had attempted to establish insider trading by Rajaratnam without success, and that its investigation was "continuing." (Rajaratnam Br. Ex. A.5 at 3, 7–8.)

The government thinks that none of this makes the Kang affidavit false. It says that Kang did not mean to imply that the investigation in this district, which began in 2007, was the 'only' time Khan and Rajaratnam were ever investigated for insider trading. And, according to the government, when Kang said that Khan had not yet been charged, he only meant that she had not been charged in connection with *this* investigation. The way the government parses Kang's grammar may be literally right. But the statements were nonetheless misleading, particularly when read with the literally false statement that Khan had been cooperating with the FBI only since November 2007. And Judge Lynch was invited to conclude that, so far as the government knew, Khan had a clean record when in fact she had previously been charged and convicted of very similar conduct, raising obvious questions as to

---

Mercury News reported that Khan had pled guilty to wire fraud in 2001 "for leaking proprietary information about Intel" while working there in 1998. Pete Carey, *Old Silicon Valley Case Linked to Hedge Fund Scandal,* San Jose Mercury News, Oct. 22, 2009. The *San Jose Mercury News* and Rajaratnam subsequently asked the California district court to unseal the entire case, and, on December 2, 2009, that court granted the unopposed motion.

her credibility.

The government cannot write these omissions off on the theory that Khan's criminal record was not important enough to include in the affidavit.[15] If that were true, why did the government deem it worthy to report that Khan "[ha[d] not yet been charged with any crimes"? (Kang Ex. 1 at 13.) Nor can the government plead ignorance. Agent Kang's own interview memoranda, produced to the defendants in discovery in this case, chart the extent of his knowledge: a December 17, 2007 memo refers to Khan's "past criminal record," and a November 28, 2007 memo refers to "some problems KHAN had in the past with the FBI." (*See* Rajaratnam Br. Ex. A. 17 at 2; Ex. A. 16 at 2.)[16]

---

[15] Indeed, at oral argument the government acknowledged that "in hindsight there is no question [the fact of the earlier investigation of Khan and Rajaratnam should have been included" (Tr. at 65) and that the government "wish[es] it would have been included" (*Id.* at 66). This is the type of candor that the Court expects from the government and, frankly, should have been exhibited to Judge Lynch.

[16] Rajaratnam cites additional omissions that supposedly bore on Khan's credibility, but these are not obvious examples of recklessness. For example, in interviews with the FBI Khan denied her involvement in the insider trading scheme before admitting to it. That fact adds little to an assessment of Khan's credibility. It is hardly surprising, or unusual, for an accused individual to deny having committed a crime before confessing to it. Rajaratnam also points to information that came to light after March 2008. In April 2008, Kang learned that, a few months earlier, Khan had deleted an email without telling the government, "because she was scared," and that she had also secretly registered a cell phone in her gardener's name,

Nor does the Kang affidavit's summary of telephone conversations between Khan and Rajaratnam win high marks for candor. (Gov't Opp'n to Rajaratnam Ex. 1–C at 15–17.) Describing one such conversation, on January 14, 2008, Kang's affidavit said that

> [d]uring this call, CS–1 asked RAJARATNAM what was "going on with the earnings this season," and whether he was "getting anything on Intel." RAJARATNAM proceeded to tell CS–1 that Intel would be up 9 to 10% and then guide down 8% and that margins would be good. RAJARATNAM then asked CS–1 "What are you hearing anything?" CS–1 responded "not really."

(*Id.* at 15–16.) That paraphrase omitted the fact that Rajaratnam had qualified his predictions with "I think." It also skipped a piece of the conversation in which Rajaratnam said that he thought margins the next quarter "will be below," and explained that he took this view "[b]ecause of [sic] the volumes are down, right?" (Rajaratnam Br. Ex. D.1 at 2–3.) In the government's paraphrased version of the conversation, Rajaratnam seems certain about the Intel numbers without giving any reason why; in the transcript, Rajaratnam equivocates ("I think") and

---

presumably to hide calls from the government. (*See* Rajaratnam Br. Ex. 20 at 5; Ex. 21 at 1.) These actions are of relevance to Khan's credibility, but the government did not discover them until after it had already gotten wiretap authorization from Judge Lynch in March 2008. (*See* Tr. 90–91; Gov't Opp'n to Rajaratnam at 39–41.)

explains at least why he thought margins would decline the following quarter ("volumes were down").

Kang's affidavit also paraphrased a January 17, 2008 call between Rajaratnam and Khan:

> During this call, CS–1 asked whether RAJARATNAM had heard anything on Xilinx. RAJARATNAM responded that he thought this quarter would be okay, but next quarter would not be so good . . . . RAJARATNAM then said he expected Xilinx to be "below the street." CS–1 asked whether he got "it" from someone at the company and RAJARATNAM said yes, somebody who knows.

(*Id.* at 16–17.) This paraphrase also subtly changed Rajaratnam's answer. In the audio recording, Khan asks whether Rajaratnam "got it from somebody at the company or—." Rajaratnam appears to answer, "Yeah I mean, somebody who knows his stuff." (Rajaratnam Br. Ex. D.2 at 4.)[17] That response is more equivocal than the government's paraphrase (a simple "yes, somebody who knows") lets on.[18] Such

---

[17] The government now claims "it is not at all clear from the recording" that this is what Rajaratnam said. (*See* Gov't Opp'n to Rajaratnam at 45.) But, having listened to the recording for itself, the Court believes the transcript is accurate. In any event, if the government truly believed that the recording was ambiguous, it should have said so to Judge Lynch, not quoted the most inculpatory version of Rajaratnam's words.

[18] Other misstatements about the content of Khan's recordings appear to be instances of simple carelessness on the government's part. Kang's affidavit claimed that, when

subtle shifts of meaning are not as compelling as direct misstatements and omissions, however, they evince a lack of frankness that should be found in all *ex parte* applications.

3. *Materiality to Judge Lynch's Decision*

The inaccuracies and inadequacies in the Kang affidavit give the Court pause. Particularly disturbing is the omission of highly-relevant information regarding Khan's prior criminal record for fraud which is "peculiarly probative of credibility."

Rajaratnam asked Khan what she was hearing on Google, she "did not respond." (Gov't Opp'n to Rajaratnam Ex. 1–C at 16.) Actually, Khan did respond. She said, "The market's been so shitty that I haven't been, it's only now that I've started to do the work." (Rajaratnam Br. Ex. D.l at 6.) This was not an omission designed to mislead. Indeed, had the government reproduced more of the conversation on Google, more evidence of probable cause might have emerged. When Rajaratnam again asked about Google, Khan said she had no information, and explained, "I told you that lady won't speak to me." Rajaratnam's response: "Idiot." (*See* Rajaratnam Br. Ex. D. 1 at 7.) "That lady" turns out to have been an investor relations person at Google. The most plausible exclamation is that the Google employee refused to provide inside information about her company. Kang's affidavit also said that Rajaratnam predicted Intel's revenues accurately ("up 9 to 10%). (Gov't Opp'n to Rajaratnam Ex. 1–C at n.8.) The affidavit mistakenly calculated the percentage jump in earnings by comparing earnings in fourth quarter 2007 to fourth quarter 2006, which yielded a percentage increase of 10.5%. What Rajaratnam was actually predicting was the percentage increase in Intel's earnings for the fourth quarter of 2007 as compared to the third quarter of that year (an increase of only six percent). (*See* Rajaratnam Br. at 29–30.)

United States v. Hayes, 553 F.2d 824, 827 (2d Cir. 1977). Still, a *Franks* hearing is required only if the government's misstatements were necessary to Judge Lynch's decision to authorize the wiretap. That is, after setting aside the government's misstatements and adding what it omitted from the affidavit, does the Court find that the affidavit set forth minimally adequate facts to establish probable cause? *See Coreas,* 419 F.3d at 155.

Rajaratnam contends that, with "Khan's lack of credibility and reliability accurately disclosed," her "general allegations" should be "discarded." (Rajaratnam Br. at 55.) This would go too far. True, "a criminal informer is less reliable than an innocent bystander with no apparent motive to falsify." *United States v. Gagnon,* 373 F.3d 230, 236 (2d Cir. 2004) (internal quotation marks omitted). But even a criminal informer can provide evidence of probable cause, particularly when other indicia of the evidence's explanation for Rajaratnam's reliability exist. *See United States v. Fermin,* 32 F.3d 674, 676–77 (2d Cir. 1994), *overruled on other grounds by Bailey v. United States,* 516 U.S. 137 (1995) (excusing the government's failure to accurately report a confidential informant's "criminal history and time as an informant" because the issuing judge would not "have completely discounted the evidence presented through" the informant, given the informant's "past reliability" and "corroborating evidence in the affidavit"); *United States v. Levasseur,* 816 F.2d 37, 43–44 (2d Cir. 1987) (holding that the government's failure to outline an informant's "full history of pre- and post-cooperation criminal activity, drug and alcohol abuse, and psychiatric problems" did not

require a *Franks* hearing, because other "independent and lawful information" sufficed to establish probable cause).[19]

Here, there were such indicia. For one thing, Khan was a known informant, not an anonymous tipper. That strengthens the case for believing her. *See Caldarola v. Calabrese,* 298 F.3d 156, 163 (2d Cir. 2002) (quoting *Florida v. J.L.,* 529 U.S. 266, 270 (2000)) ("[A]n anonymous tip is '[u]nlike a tip from a known informant whose reputation can be assessed and who can be held responsible if her allegations turn out to be fabricated.' "). And, in implicating Rajaratnam in crimes of insider trading, Khan made statements against her own penal interest. "Admissions of crime . . . carry their own indicia of credibility—sufficient at least to support a finding of probable cause to search. That the informant may be paid or promised a 'break' does not eliminate the residual risk and opprobrium of having admitted criminal conduct." *United States v. Harris,* 403 U.S. 573, 583–84 (1971) (plurality opinion).[20] Khan

---

[19] Rajaratnam's reply brief points out that none of the cases the government cites—*Fermin, Canfield,* and *Levasseur,* all cases in which the Second Circuit excused the government's failure to disclose an informant's prior criminal conviction—involved a prior conviction for fraud. (Rajaratnam Reply Br. at 7 (citing *United States v. Hayes,* 553 F.2d 824, 827 (2d Cir. 1977), for the proposition that a prior fraud conviction is "peculiarly probative of credibility").) That is true, but it does not mean that Khan's credibility stood at zero.

[20] To be sure, even admissions against penal interest are "suspect insofar as they inculpate other persons." *Lilly v. Virginia,* 527 U.S. 116, 138–39 (1999); *see United States v. Bakhtiar,* 994 F.2d 970, 978 (2d Cir. 1993) (statements "made in

admitted, among other things, that she had provided Rajaratnam with inside information about Google. That statement exposed her to greater criminal penalties-by the government's calculation, the profits from trading on this information exceeded $6 million. (*See* Gov't Opp'n to Rajaratnam Ex. 1–C, ¶ 18 n.9.)

In addition to all this, the government was able to corroborate some of Khan's statements. *See Canfield,* 212 F.3d at 719–20 (quoting *United States v. Wagner,* 989 F.2d 69, 73 (2d Cir. 1993) ("[I]f an informant's declaration is corroborated in material respects, the entire account may be credited, including parts without corroboration."). Khan told the FBI that Rajaratnam had previously provided her with earnings information on Broadcom; in a call she recorded at the FBI's request, Rajaratnam told her he knew someone "very good" at Broadcom who could give him "the numbers" (Gov't Opp'n to Rajaratnam Ex. 1–C at 17). Similarly, Rajaratnam's statement on a recorded call that he needed to call "a couple guys" at Xilinx to get information from them squares with Khan's statement to the FBI that Rajaratnam had previously bragged about receiving inside information on Xilinx. (*Id.* at 16.) Trading records also provide limited corroboration of certain of Khan's

---

an attempt to minimize [one's] own culpability, to shift blame to [another], or to curry favor with authorities . . . do not bear the same indicia of reliability as the usual statement exposing a declarant to unpleasant consequences, such as criminal liability"). But that does not mean such admissions are *no* evidence of veracity—especially where, as here, the admissions are not made in an attempt to reduce the individual's share of the blame.

statements. For example, Khan claimed to have provided Rajaratnam with inside information about Polycom in January 2006 and Google in the summer of 2007; trading records show that Rajaratnam's funds executed profitable trades in those two securities during the relevant time periods. (*See* Gov't Opp'n to Rajaratnam Ex. 1–C n.6, n.9.) Finally, toll records indicate that Rajaratnam repeatedly talked to an Intel insider, Rajiv Goel, in the run-up to earnings announcements in March 2006, April 2007, and February 2008. (*See id.* at 38.)

Given the evidence of corroboration, Khan's allegations of Rajaratnam's criminal conduct provide at least some support for probable cause. But there is more. Rajaratnam's recorded telephone conversations with Khan independently show that he intended to get information about stocks from company insiders. In advance of Xilinx's earnings announcement for the fourth quarter of 2007, Rajaratnam said he thought that "Xilinx this quarter" had "turned out well"; when Khan asked "what do you think they'll do," Rajaratnam said that he needed to "call a couple of guys there at Xilinx." (Rajaratnam Br. Ex. D. 1 at 4.) In a conversation with Khan about Broadcom, Rajaratnam told Kang that that "he knew somebody very good there who could give him the numbers but that he had to check." (*Id.* Ex. D.2 at 6.) The specificity of Rajaratnam's comment about Broadcom—he would get "the numbers"—is especially telling. Rajaratnam's alternate explanation for these remarks—that he meant he had to check with company insiders about publicly available information—is hardly more plausible than the

government's explanation. That Rajaratnam has an innocent explanation at all, moreover, does not make the remarks irrelevant to probable cause. *See Gagnon,* 373 F.3d at 236 ("[P]robable cause does not demand the certainty we associate with formal trials," and "the fact that an innocent explanation may be consistent with the facts as alleged . . . does not negate probable cause."). Here, Rajaratnam's answers created at least a fair probability that insider trading was afoot.

The March 7, 2008 Kang Affidavit also contained summaries of and quotations from intercepts of Craig Drimal's and Zvi Goffer's phones. Drimal worked out of Galleon's offices; Goffer was a trader there. (Gov't Opp'n to Rajaratnam Ex. 1-C ¶¶ 20-30.) These intercepts appear to indicate that Goffer and Drimal knowingly obtained inside information and passed it on to others, including Rajaratnam. In September 2007, Drimal gave a government cooperator (not Khan) the stock symbols of four companies that were acquisition targets; he warned the cooperator to "be careful in trading the securities of one of the companies on the list, because there were no public rumors that the company was an acquisition target." (*Id.* at 19-20). Drimal later said to the cooperator in recorded conversations that he did not want to talk about the four stocks on the telephone, that is was "like shooting fish in a barrel," and that he was nervous about having too much success (presumably because it would raise eyebrows). (*Id.* at 20.) Drimal told the cooperator that he had provided the same four stocks to Rajaratnam (*Id.* at 19). Perhaps Rajaratnam accepted the tips innocently, without knowing they

were non-public. But assuming Drimal was right that one or more of these tips was completely unexpected to the public, there is at least a fair inference that Rajaratnam, a sophisticated investor, knew that.

The government also intercepted calls between Goffer and Drimal, and between Goffer and another source of information. In one recorded call, Goffer mentioned to the source that he had given Galleon a couple of "big calls" (which the affidavit interpreted to mean tips), including a "call" on Bear Stearns, which "went up 13 dollars." (*Id.* at 34.) According to the affidavit, Goffer then said that Rajaratnam had one or two hundred thousand shares, and that if Goffer had had as much conviction in the tipper as Rajaratnam had, he would have made a lot of money. (*Id.*)

This evidence, taken alone, is far from conclusive of Rajaratnam's culpability. But to suffice for probable cause, it need not have been. *See United States v. Martin,* 426 F.3d 68, 76 (2d Cir. 2005) (calling it a "defect" to "conflate [ ] evidence of probable cause to sustain a warrant with proof of a prima facie case," because "probable cause does not require a prima facie showing" of the crime); *United States v. Bellomo,* 954 F. Supp. 630, 638 (S.D.N.Y. 1997) (Kaplan, J.) ("While the intercepted conversations, considered separately, may not be dispositive of guilt on the particular issues, that is not the relevant standard."). Adding it all up, and correcting the affidavit to account for the government's misstatements and omissions, the Court believes that there were enough facts for Judge

Lynch to have found probable cause.

C. Chiesi's Claims

The case for probable cause against Chiesi relied exclusively on communications intercepted pursuant to the Rajaratnam wiretap. Accordingly, were the Rajaratnam wiretap evidence suppressed, suppression of the Chiesi wiretaps would likewise be warranted. *See Giordano,* 416 U.S. at 533 (suppressing "derivative evidence" of a suppressed wiretap). The government has acknowledged as much. (*See* Tr. at 142 ("[T]he government concedes that if the Rajaratnam wiretap falls, then the Chiesi one does also on probable cause.").) But that argument is moot in light of the Court's decision to deny Rajaratnam's motion for suppression.

Chiesi argues separately that, even if the Rajaratnam wiretap intercepts survive suppression, they do not establish probable cause of her participation in an insider trading conspiracy. Because Chiesi does not suggest that the government misstated facts in its application for authorization to wiretap Chiesi's phones, the usual standard of "deference to the probable cause determination of the issuing [judge]" applies. *Walczyk,* 496 F.3d at 157. So long as the "facts set forth in the application were minimally adequate to support the determination that was made," *Conception,* 579 F .3d at 217, suppression is not warranted. *See also Awadallah,* 349 F.3d at 64 ("Ordinarily, a search or seizure pursuant to a warrant is presumed valid.").

The government first applied for authorization

to wiretap Chiesi's phones on August 13, 2008. The application contained ample support for Judge Sullivan's order authorizing the wiretaps. The affidavit attached to the August 13 application (the "August 13, 2008 Kang Affidavit") described the interception of several calls between Rajaratnam and Chiesi. It cited numerous plausible examples of inside information Chiesi apparently gave to Rajaratnam concerning AMD, Akamai, IBM, and Microchip. (*See* Gov't Opp'n to Chiesi Ex 1-C at 23-30.)

Consider the following evidence: in a pair of conversations between Rajaratnam and Chiesi on June 6, 2008, the two discussed AMD's upcoming quarterly earnings announcement. During the first call, Chiesi said she had asked AMD's chairman whether AMD was "making the quarter," and he had replied, "it's close." (*Id.* at 24). Chiesi also told Rajaratnam that the AMD chairman was "trying to put a deal together . . . [b]ut he said they're not close." (*Id.* at 24-25). In the second call, Chiesi told Rajaratnam that AMD's "quarter is suspect," and he responded that she should "[s]hort" AMD stock, "then go long before the deal . . . ." (*Id.* at 26.) Chiesi said she would "be very nimble about it." (*Id.*). This is sufficient evidence of probable cause, despite Chiesi's description of the information conveyed as "polite ether" (Chiesi Br. at 26) and a matter of public knowledge (*id.* at 26-27). Chiesi rightly observes that the public new an AMD deal might happen, but the information given to Rajaratnam is more specific than that: it concerns the *timing* of the deal, which itself may be material.

Other calls provided additional support for probable cause. In several calls between July 24 and July 30, 2008, Chiesi and Rajaratnam discussed information about Akamai. Chiesi said she had "just got a call from my guy" who said that the company was going to "guide down"; that "people internally" believed the stock would go "down to 25"; that they needed to be "radio silent"; and that she was telling Rajaratnam this because they "share everything." (Gov't Opp'n to Chiesi Ex. 1-C at 28.) Later, Chiesi told Rajaratnam that if "the stock gets killed," her source would be "afraid," and that "[i]if he loses his job, I'll get blamed for it." (*Id.* at 29). A reasonable inference is that the two were dealing in inside information—why else would a company insider be worried about losing his job if found out? Chiesi points out that, about this time, rumors were flying of a potential downturn at Akamai. But Chiesi gave Rajaratnam specific numbers, not vague speculation about the stock's direction. Chiesi also told Rajaratnam that she had learned from Microchip's CEO that the company was going to "start buying back stock on Monday." (*Id.* at 27.) Although Microchip had previously announced that it was buying back stock (*see* Chiesi Br. At 27-28), it had not announced the timing of that buyback. Regardless of whether these facts establish Chiesi's culpability, they are certainly minimally adequate to support Judge Sullivan's finding of probable cause.

III. Necessity

Both defendants argue that the government's wiretap applications failed to 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 be too dangerous," 18 U.S.C. § 2518(1)(c), as Title III requires. Congress required that showing to ensure that "wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." *United States v. Kahn,* 415 U.S. 143, 153 n.12 (1974). What Title III "envisions is that the showing [of the wiretap's necessity] be tested in a practical and commonsense fashion." *Concepcion,* 579 F.3d at 219 (quoting S. Rep. No. 90–1097, at 12).

Like a court reviewing an affidavit containing misstatements or omissions as to probable cause, a court reviewing an affidavit for necessity must "decide if the facts set forth in the application were minimally adequate to support the determination that was made." *Torres,* 910 F.2d at 231. In that determination, "generalized and conclusory statements that other investigative procedures would prove unsuccessful" do not suffice. *United States v. Lilla,* 699 F.2d 99, 104 (2d Cir. 1983). At the same time, however, Title III "only requires that the agents inform the authorizing judicial officer of the nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods." *Concepcion,* 579 F.3d at 218; *see also United States v. Scala,* 388 F. Supp. 2d 396, 404 (S.D.N.Y. 2005) ("[A]reasoned explanation, grounded in the facts of the case, and which squares with common sense, is all that is required . . . .")

(internal quotation marks omitted).[21] The government is not "required to exhaust all conceivable investigative techniques before resorting to electronic surveillance." *Concepcion,* 579 F.3d at 218; *see also Fury,* 554 F.2d at 530 ("At the outset we note that the purpose of these 'other investigative

---

[21] In her briefs and at oral argument through counsel, Chiesi claims that the standard is exhaustion of ordinary investigative techniques. (*See* Chiesi Br. at 13; Chiesi Reply Br. at 6–7; Tr. at 137–139.) Chiesi quotes language from an opinion of the Tenth Circuit that phrases the requirement in terms of exhaustion. *See United States v. Castillo–Garcia,* 117 F.3d 1179, 1188 (10th Cir. 1997), *overruled on other grounds by United States v. Ramirez–Encarnacion,* 291 F.3d 1210 (10th Cir. 2002) ("[W]e require the government to prove *exhaustion*—either by attempt or explanation of why the method would not work—of all 'reasonable' investigatory methods.") (emphasis added). However, even that statement refers to exhaustion "either by attempt *or explanation",* and the Tenth Circuit has elsewhere described its decisions in this area as "repeatedly h[o]ld[ing] that law enforcement officials are not required 'to exhaust all other conceivable investigative procedures before resorting to wiretapping .'" *United States v. Edwards,* 69 F.3d 419, 429 (10th Cir. 1995) (quoting *United States v. Apodaca,* 820 F.2d 348, 350 (10th Cir.), *cert. denied,* 484 U.S. 903 (1987)). That is the law in this Circuit. *See United States v. Torres,* 901 F.2d 205, 231 (2d Cir. 1990) (The "purpose of the statutory requirements is not to preclude resort to electronic surveillance until after all other possible means of investigation have been exhausted by investigative agents . . . ."); *United States v. Young,* 822 F.2d 1234, 1237 (2d Cir. 1987) ("[T]here is no requirement that any particular investigative procedures be exhausted before a wiretap may be authorized") (internal quotation marks omitted); *see also United States v. Valdez,* 90–793(JFK), 1991 WL 41590, *2 (S.D.N.Y. Mar. 19, 1991), *aff'd,* 952 F.2d 394 (2d Cir. 1991) ("The law is clear in this circuit that the requirements of section 2518 were not intended to turn electronic surveillance into a tool of last resort.").

techniques' requirements is not to foreclose electronic surveillance until every other imaginable method of investigation has been unsuccessfully attempted, but simply to inform the issuing judge of the difficulties involved in the use of conventional techniques.") (internal quotation marks omitted). "Rather, the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried. . . ." *Giordano,* 416 U.S. at 515. Put another way, "an affidavit offered in support of a wiretap warrant must provide some basis for concluding that less intrusive investigative procedures are not feasible." *Lilla,* 699 F.2d at 103.

A. Rajaratnam's Claims

In his motion, Rajaratnam argued that suppression was warranted because the March 7, 2008 affidavit failed to disclose, *inter alia,* (1) the nature and extent of the lengthy SEC investigation that preceded the wiretap request, and a prior FBI investigation of Rajaratnam's connection to insider trading; (2) the voluminous evidence the SEC was able to collect using conventional techniques; and (3) the prosecutor's total access to and use of that evidence prior to the submission of its wiretap application to Judge Lynch. (*See* Rajaratnam Br. at 65–73.) In an opinion issued last month, the Court found that Rajaratnam had "at least established good grounds for holding a *Franks* hearing regarding the veracity of the March 7, 2008 affidavit and the issue *vel non* of whether the necessity requirement has been satisfied." *United States v. Rajaratnam,* No. 09–CR–1184, 2010 WL 3219333, at *2 (S.D.N.Y. Aug.

12, 2010). A four-day hearing was held from October 4 through October 7, 2010. At that hearing, Rajaratnam presented four witnesses: Lindi Beaudreault, former counsel to Rajaratnam and Galleon; Andrew Michaelson, formerly an attorney at the Division of Enforcement at the Securities and Exchange Commission ("SEC"); Special Agent Kang; and Lauren Goldberg, a former Assistant United States Attorney who led the investigation by the USAO and drafted the March 7, 2008 affidavit. The Court's findings based upon the hearing record are set forth below.

1. Misstatements and Omissions

The *Franks* hearing established that the criminal authorities in this case made a glaring omission. They failed to disclose to Judge Lynch that the SEC had for several years been conducting an extensive investigation into the very same activity the wiretap was intended to expose using many of the same techniques the affidavit casually affirmed had been or were unlikely to be successful. A judge hearing an *ex parte* application relies entirely on the government's representation that it has disclosed all material facts. But how could Judge Lynch assess whether conventional investigative techniques had failed or were likely to fail without even knowing that they were presently being used in an ongoing SEC investigation upon which the prosecutor and FBI were relying—almost entirely—to construct their own case? Of course, there is nothing wrong in their piggybacking the SEC investigation provided they were not improperly directing it. But the Court is at a loss to understand how the government could have

ever believed that Judge Lynch could determine whether a wiretap was necessary to this investigation without knowing about the most important part of that investigation—the millions of documents, witness interviews, and the actual deposition of Rajaratnam himself, all of which it was receiving on a real time basis and all of which was being acquired through the use of conventional investigative techniques. It is all well and good to now argue that these tools proved inadequate—and the Court ultimately accepts that contention—but it would have been far better for Judge Lynch to have been in a position to make that decision for himself.

The USAO and FBI first learned about the on-going investigation in March 2007, when the SEC referred an investigation of insider trading by Rajaratnam and his brother Rengan Rajaratnam, a principal at Sedna Capital Management, LLC. (Kang Ex. 3; *Franks* Tr. at 95.) The SEC had opened its investigation, which was formally captioned an investigation of Sedna, on September 21, 2006. (Michaelson Ex. 1–A.)[22] On March 26, 2007, the

[22] Since November 5, 2003 the SEC had also been conducting a technically separate but somewhat related investigation into insider trading at Galleon. (Beaudreault Ex. 4.) The SEC had served Galleon with numerous subpoenas and requests for a variety of documents, including trading and telephone records, and a complete record of Galleon emails and instant messages (IMs) from November 2003 through June 2005. (Beaudreault Ex. 5; *Franks* Tr. at 29–35.) Galleon produced documents in response to these requests and subpoenas, which included the standard Form 1662 warning that information provided to the SEC could be used in a criminal proceeding. (*Franks* Tr. at 30, 33.)

USAO and FBI requested access to the SEC's investigative file (Michaelson Ex. 12) and three days later, the USAO and the FBI held the first of what would be numerous meetings with the SEC to discuss the course of its investigation. (*See* Kang Ex. 3.) Over the next year leading up to the March 7, 2008 wiretap application, the SEC "ke[pt] the criminal authorities up to speed" (*Franks* Hr'g Tr. at 132–133) and met and spoke with them regularly to discuss the investigation. (*See id.* at 128, 732; Kang Exs. 3, 6, 7, 10, 11, 13, 14, 15, 17, 18, 20, 21, 23, 24, 25.) The SEC also provided the criminal authorities with documents of particular note as well as chronologies outlining circumstantial cases of insider trading and identifying likely sources of inside information regarding several different companies. (Kang Exs. 4, 21, 22; Michaelson Exs. 59 84, 94, 95, 96, 97, 98, 100, 101, 106, 120.) Accordingly, the USAO and FBI either knew about or had access to "the best of what the SEC could produce." (*Franks* Tr. at 827–28.)

That was quite a bit to say the least. In early 2007, the SEC Office of Compliance Inspections and Examinations (OCIE) began an on-site examination of Galleon. (*Franks* Tr. at 112, 367; Michaelson Ex. 10.) As part of that investigation, OCIE made nearly two dozen requests for numerous classes of documents, including trading records, telephone records, and a complete record of e-mails and IMs sent and received by Rajaratnam and others in 2006. (*Franks* Tr. at 35–36, 112–120.) OCIE also interviewed eighteen Galleon employees and twice interviewed Rajaratnam himself, once in February and once in March of 2007, regarding insider trading. (*See id.* at 62–69.)

As part of the SEC investigation, Rajaratnam was deposed on June 7, 2007. (*See* Michaelson Ex. 45.) He was asked numerous questions regarding insider trading at Galleon, trading in various technology stocks, IMs exchanged with Roomy Khan, and his connections to executives at several publicly traded companies. Rajaratnam denied that he ever traded on, had any sources of, or even received any inside information. (*Franks* Tr. 347–54; Michaelson Exs. 45 at 77, 84, 184.) The SEC also deposed five other individuals associated with Sedna and/or Galleon, none of whom admitted to insider trading. (Michaelson Exs. 46–50; *Franks* Tr. 190–93, 346–47.)

Following the Rajaratnam deposition, the SEC served Galleon with additional subpoenas for various documents, including trading records, investor lists, and Rajaratnam's contact lists, hard drive, bank records, and calendar. Galleon produced four million pages of documents in response to the subpoenas, including several hundred thousand e-mails and almost fifty thousand pages of FMs. (*Franks* Tr. 38–40.) These documents suggested that Rajaratnam was exchanging inside information by telephone. (*See Franks* Tr. 398–408, 702; Gov't Exs. 17, 24, 32.) As part of its investigation, the SEC also served 221 subpoenas on banks, clearing houses, telephone companies, and issuers of publicly traded securities prior to March 7, 2008. (Michaelson Exs. 52–56; *Franks* Tr. at 195–97.)

The USAO and FBI knew about all of this. They knew about the OCIE investigation, including that Galleon had produced documents and that the OCIE had interviewed Galleon employees, including

Rajaratnam. (*Franks* Tr. at 508–12, 731.) They knew that Rajaratnam had been deposed and they received a transcript of that deposition as well as of the five others the SEC had taken. (Michaelson Exs. 45, 51, 72; *Franks* Tr. at 190–92, 507, 739–41). In fact, they knew in advance that the SEC was going to depose Rajaratnam and, according to documents introduced at the hearing, met with the SEC in part to "talk [ ] strategy" regarding that deposition. (Michaelson Ex. 26–A; Tr. 139–45; 733–39.) They knew that the SEC had issued over two hundred subpoenas from Galleon and third parties, that the SEC had received millions of documents in response, and that they had full access to those documents. (*Franks* Tr. 729–31.) They knew from the SEC's chronologies that the SEC was building circumstantial cases of insider trading and identified several possible sources of inside information, including Khan and Rajiv Goel. (*See, e.g.* Michaelson Exs. 93–99; *Franks* Tr. at 732.) And they knew from the same chronologies that the SEC had identified twelve individuals as potential interviewees (Michaelson Ex. 84 at 2; *Franks* Tr. at 256–58, 703–4) and hoped to review some additional records. (Michaelson Ex. 120.)

The USAO and FBI also knew that the SEC investigation was the most important part of their own. Indeed, Agent Kang testified that the SEC knew more about the investigation than he did. (*Franks* Hr'g Tr. at 614.) When asked by the Court to describe what the federal criminal authorities did other than rely on the SEC, the government prosecutor testified that the USAO and FBI had largely devoted their time to analyzing the

information they were receiving from the SEC, "assimilating their own analyses of what all this information meant . . . ." (*Franks* Hr'g Tr. at 828–29.) Though the criminal authorities "independently obtained some of [their] own records, phone records, trading records, bank records", the prosecutor testified that "[w]hatever [they] obtained through grand jury subpoenas would *supplement* what the SEC had provided." (*See id.* (emphasis added.)) The criminal authorities did not themselves review the SEC's investigative file but instead relied on the SEC to provide the most important documents. (*Franks* Tr. at 124, 614, 685.) And they decided to approach and interview Roomy Khan (and her broker) in large part based on information provided by the SEC. (*See Franks* Tr. at 813.)

The USAO and the FBI also knew that all of this evidence was being developed through conventional investigative techniques. But this was not disclosed to Judge Lynch. Title III requires "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c). By failing to disclose the substance and course of the SEC investigation, the government made what was nearly a full and complete *omission* of what investigative procedures in fact had been tried. That omission deprived Judge Lynch of the opportunity to assess what a conventional investigation of Rajaratnam could achieve by examining what the SEC's contemporaneous, conventional investigation of the same conduct was, in fact, achieving.

The government strenuously argues that it did not "hide" the existence of the SEC investigation from Judge Lynch. But this misses the point. If anything, passing references to having "reviewed trading records and other information provided by the SEC" (Kang Ex. 1 at 15) obscures the fact that, on the record before the Court, the prosecutor's investigation was, in sum and substance, the SEC investigation, and its results up until March 2008 were the product of entirely conventional investigative techniques not disclosed to Judge Lynch. In light of the fact that the Kang Affidavit all but ignored the SEC investigation—the elephant in the room—the boilerplate representation that "alternative investigative techniques have been tried or appear unlikely to succeed if tried" (Kang Ex. 1 at 38) remains just that—boilerplate.

As might be expected, this broad omission also rendered several specific statements in the affidavit misleading. For example, the affidavit blandly assures Judge Lynch that interviewing Rajaratnam and other targets is an "investigative route" that is "too risky at the present time." (*Id.* at 44–45.) Yet during that same time period, the SEC, after asking the criminal authorities if they had any objection (*Franks* Tr. at 133, 142), had interviewed or deposed under oath over twenty Galleon employees, including two interviews and a day-long deposition of Rajaratnam. The results of these interrogations were promptly provided to the prosecutor and, in the case of Rajaratnam, the prosecutor met with the SEC beforehand to discuss "strategy." (Michaelson Ex. 26–A; Tr. 139–45; 733–39.) The government now contends that the interview results were useless and

disclosure of a criminal as opposed to an SEC investigation would have been harmful. Perhaps so, but that is the very decision a reviewing court, not the government, should be making.

Cut of the same cloth is the representation that the conventional use of search warrants "is not appropriate at this stage of the investigation, as the locations where . . . records related to the scheme have not been fully identified, if at all." (Kang Ex. 1 at 47.) At that stage in the investigation—unknown to Judge Lynch—the government had, in fact, accumulated or had access to four million Galleon documents obtained through either SEC or grand jury subpoenas and had built a compelling circumstantial case of insider trading in several securities. (*See* Kang Exs. 4, 21, 22; Michaelson Exs. 59 84, 94, 95, 96, 97, 98, 100, 101, 106, 120.) Moreover, the files were so extensive that the government had not had the time to review them all and was relying on the SEC to do so. (*Franks* Tr. at 124, 614, 685.) This is precisely the nuts and bolts of an investigation that must be presented to a court if it is to fulfill its function of determining whether conventional investigative techniques are likely to prove inadequate.[23]

---

[23] For much the same reason, the boilerplate assertion that "the issuance of grand jury subpoena likely would not lead to the discovery of critical information," (Kang Ex. 1 at 43) blinks reality. Grand jury subpoenas and SEC subpoenas had already led to a mountain of incriminating circumstantial evidence as the impressively detailed chronologies prepared by Mr. Michaelson fully attest. The government contends that the

Though less compelling, the Court is also troubled by the Kang affidavit's reference to the acquisition and review of trading records as an investigative technique. While acknowledging that it had reviewed "certain" trading records, the affidavit goes on to state that requesting more records "would jeopardize the investigation" because "clearing firms . . . sometimes alert traders to the requests." (Kang Ex. 1 at 44.) Fair enough, but it would have been informative to have also disclosed that the SEC had already issued over two hundred subpoenas for, *inter alia,* trading records, and that the grand jury had issued such subpoenas as well, all apparently without jeopardizing its investigation. The Court, of course, is not charged with fly-specking the government's affidavit and does not seek to do so. But stepping back to look at the forest, the government in this case did not merely omit some discrete piece of information possibly relevant to a reviewing court's analysis of necessity; it failed to disclose the heart and soul of its investigation, without which a reasoned evaluation of the necessity of employing wiretaps was impossible.

2. Suppression Analysis

Of course, the government's omission is the beginning rather than the end of the Court's suppression inquiry, for a misleading affidavit alone

---

reference to the inefficacy of grand jury subpoena was only meant to refer to witness subpoenas. But of course that is the problem with falling back on boilerplate; unless brought alive by disclosure of the course of the particular investigation at hand, boilerplate serves little purpose.

is not grounds for suppression. While the *Franks* analysis discussed above is typically employed to evaluate misstatements and omissions relating to probable cause, the Second Circuit has extended the *Franks* analysis to other Title III requirements for obtaining a warrant. *See United States v. Bianco,* 998 F.2d 1112, 1125–26 (2d Cir. 1993) (applying *Franks* to 18 U.S.C. § 2518(11)(a)(ii), which requires that the government explain why "specification of the place of interception is not practical"). And district courts in this Circuit have done so with respect to the issue of necessity in particular. *See United States v. King,* 991 F. Supp. 77, 88–90 (E.D.N.Y. 1998); *United States v. Sanchez–Flores,* No. 94–CR–864, 1995 WL 765562, at *5 (S.D.N.Y. Dec. 29, 1995). *Cf. 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); *Ippolito,* 774 F.2d at 1485 ("although *Franks* dealt specifically with probable cause, its reasoning applies [to Title Ill's necessity requirement] as well"). Thus, to warrant suppression on the issue of necessity, Rajaratnam must establish (1) that the omissions from the Kang Affidavit regarding the necessity of using wiretaps were the product of the government's "deliberate falsehood" or "reckless disregard for the truth", and (2) that, after inserting omitted information and setting aside misstatements, the affidavit fails to establish necessity. *See Coreas,* 419 F.3d at 155. Rajaratnam has made the former showing but not the latter.

a. Reckless Disregard

Having heard the testimony of the government witnesses at the *Franks* hearing, the Court

comfortably concludes that no one acted with the deliberate intent to mislead Judge Lynch. Recklessness, however, is another matter. As discussed in the probable cause analysis, recklessness may be inferred when omitted information was "clearly critical" to assessing the legality of employing a wiretap. *Reilly,* 76 F.3d at 1280. Here the issue is whether the omission of information regarding the nature and scope of the SEC investigation upon which the government's own investigation was based would have been critical to Judge Lynch in assessing whether conventional investigative techniques would (or had) failed and, therefore, a wiretap was necessary. The Court, putting itself in the shoes of the original reviewing court, has already answered that question in the affirmative.

The government demurs, arguing that it could not have acted recklessly in failing to disclose a "more detailed description of the SEC investigation" because it "did not view that investigation as an investigative technique under control of the Criminal Authorities." (Gov't Post Hr'g Opp'n at 22, 26). The Court finds this argument unpersuasive for several reasons. As an initial matter, the government's description of the underlying issue as simply whether a "more detailed" description of the SEC investigation was warranted reflects the very fundamental flaw in the original Kang affidavit. The issue is not the accuracy of passing references to having received discrete pieces of information from the SEC. The issue is whether the government should have informed the reviewing court of the array of conventional investigative techniques

contemporaneously being employed by the SEC to unearth significant evidence of insider trading, all of which was at the core of the government's own criminal investigation. Furthermore, the government's contention that disclosure was somehow inappropriate because it did not and could not "control" the SEC investigation is formalism carried to its extreme. And, of course, it does not address the proper inquiry under the first prong of the *Franks* analysis: whether it was "clearly critical" to the reviewing court's analysis of the necessity issue to be informed that conventional investigative techniques were then being employed by the SEC and relied upon by the government, all at the time that the government was providing boilerplate assurances that alternative investigation techniques "appear unlikely to succeed."

b. *Materiality*

i. Legal Standard

A showing that the government acted recklessly is only half of Rajaratnam's burden. Rajaratnam also bears the burden of proving that the misstatements and omissions were material. Indeed, under *Franks,* "[t]he ultimate inquiry on a motion to suppress is . . . not whether the affidavit contains false allegations or material omissions, but whether after putting such aside, there remains a residue of independent and lawful information sufficient" to support the affidavit. *Ferguson,* 758 F.2d at 848. In making that determination, "a court should disregard the allegedly false statements and determine whether the remaining portions of the affidavit would

support" the affidavit. *United States v. Trzaska,* 111 F.3d 1019, 1027–28 (2d Cir. 1997); *see also Canfield,* 212 F.3d at 718. And omissions should also be corrected. *See Ferguson,* 758 F.2d at 848. A court, therefore, "should . . . delete false or misleading statements and insert the omitted truths revealed at the suppression hearing." *Ippolito,* 774 F.2d at 1486 n.1.

One further issue deserves mention. The Supreme Court has stated that "an otherwise insufficient affidavit cannot be rehabilitated by testimony concerning information possessed by the affiant when he sought the warrant but not disclosed to the issuing magistrate." *Whiteley v. Warden, Wyo. State Penitentiary,* 401 U.S. 560, 565 n.8 (1971). Citing that statement, Rajaratnam repeatedly argues that the Court should not consider many of the government's arguments as to the sufficiency of a corrected affidavit because those arguments are "post-hoc rationalizations" that the government did not make in the initial application. (*See, e.g.,* Rajaratnam Post Hr'g Reply Br. at 13.) Rajaratnam's argument that this would give the government "a free second bite at the application apple" (Rajaratnam Post Hr'g Reply Br. at 5) is appealing, but overly simple.

As an initial matter, *Whiteley* is not exactly "controlling Supreme Court" precedent." (Rajaratnam Post Hr'g Reply Br. at 21.) That case involved a challenge to the sufficiency of a warrant application, not a *Franks* proceeding regarding the truth of an application. *See Whiteley,* 401 U.S. at 564. Since a *Franks* proceeding requires deleting

falsehoods and correcting omissions, the entire premise of the *Franks* approach is that the court must consider information that did not appear in the original affidavit. In that case, arguments about what that affidavit would have meant necessarily involve inferences that were not explicitly made in the original affidavit. Indeed, the Eighth Circuit has held *Whiteley* inapplicable to *Franks* for precisely that reason. *See United States v. Finley,* 612 F.3d 998, 1003 n.7 (8th Cir. 2010).

What is more, Rajaratnam's argument that "the remaining content is simply the *factually* corrected affidavit" and does not "include a supplementary *advocacy* piece" (Rajaratnam Post Hr'g Reply Br. at 5 (emphasis in original), elides the fact that, because the Court does not literally rewrite the affidavit, the exact content of the "remaining content" is amorphous. Rajaratnam's distinction comes close to tying the government's hands in arguing the materiality point. *Cf. United States v. Williams,* 737 F.2d 594, 604 (7th Cir.1984) (reasoning in *Franks* proceeding related to probable cause that "if the challenger is permitted to marshal all exculpatory facts, fairness dictates that the government be allowed to support the affidavit with additional inculpatory information known to the affiant at the time the affidavit was made"). More importantly, it also is inconsistent with the purpose of both Title III and the Fourth Amendment, for, as Rajaratnam himself notes, "[t]he point of the Fourth Amendment . . . is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence" but that it "require[s] that those inferences be drawn by a neutral magistrate . .

. ." *Johnson v. United States,* 333 U.S. 10, 13–14(1948). Therefore, the Court will draw its inferences from the totality of facts presented in the government's wiretap application as well as those omitted therefrom.

ii. Application

The March 7, 2008 affidavit, as corrected, would have informed the issuing judge that Rajaratnam had been under investigation for insider trading since 1998 when the U.S. Attorney's office in San Francisco began investigating Roomy Khan; that Khan cooperated in the investigation of Rajaratnam as part of a plea agreement; that the SEC began investigating Rajaratnam and Galleon in 2002; that the SEC had interviewed eighteen Galleon employees and deposed Rajaratnam and others under oath; that the SEC had issued over two hundred subpoenas and obtained millions of pages of documents, including telephone records, trading records, e-mails, and IMs; that all the evidence was shared with the government through regular meetings during the course of the investigations; and that the evidence thus gathered enabled both the SEC and the government to develop substantial circumstantial evidence of insider trading by Rajaratnam and numerous associates in the securities of several companies. Finally, the evidence gathered led directly to the FBI's interviews of Roomy Khan during which she "flipped" and provided the government with direct evidence of insider trading by Rajaratnam.

Given the advances made in both

investigations through the application of conventional investigative techniques, it is surely incorrect to say that these investigative procedures had "failed" in an abstract sense. But Rajaratnam's characterization that "the government's conventional investigation had yielded a veritable mountain of evidence" oversimplifies the case. (Rajaratnam Post Hr'g Reply Br. at 19.) On the other hand, the government repeatedly understates what it found in that "mountain" of evidence, careful analysis of which, after all, enabled the criminal authorities and the SEC to identify multiple sources of inside information and flip Khan, thereby developing additional leads. The government's suggestion that these were only 'weak or non-existent' circumstantial cases" (Gov't Post Hr'g Opp'n at 38) cannot be squared with the minute-by-minute analyses of IMs, toll records, and trading records prepared by the SEC and spoon-fed to the government.

However, "failure" in the Title III sense is not an abstract proposition. "Just because the government had achieved some success in collecting evidence through [a confidential source] does not demonstrate the success of 'normal investigative procedures' under Title III." *Gambino,* 734 F. Supp. at 1103. As the government rightly points out, if that were so, a wiretap would never be approved because a showing of probable cause would negate necessity and a showing of necessity would negate probable cause. *Cf. United States v. McLee,* 436 F.3d 751, 763 (7th Cir.2006) ("[T]he fact that the government may have been able to indict him in the absence of evidence obtained through the use of a wiretap does not preclude a finding of necessity.").

Many of the same documents that were used to compile the SEC chronologies strongly suggested that Rajaratnam had been careful to exchange nearly all of his inside information by telephone. (*See Franks* Tr. 398–408, 702; Gov't Exs. 17, 24, 32.) "[W]iretapping is particularly appropriate when the telephone is routinely relied on to conduct the criminal enterprise under investigation." *United States v. Steinberg,* 525 F.2d 1126, 1130 (2d Cir. 1975); *see also Lilla,* 699 F.2d at 105 n.6 ("If the crimes in question were planned and consummated only by means of telephone . . . the argument that wiretapping was the only option might seem more persuasive.") Rajaratnam argues that "the government cannot satisfy the statutory requirement of necessity simply by defining the goals of its investigation so expansively that no investigative technique, including wire surveillance, could ever satisfy them." (Rajaratnam Post Hr'g Br. at 45.) True, but the fact that the SEC's investigation had identified certain sources did not preclude a showing that a wiretap was necessary to confirm those sources and fully uncover Rajaratnam's network of sources.[24] *See United States v. Hinton,* 543 F.2d

[24] A corrected affidavit would also have disclosed that the criminal authorities had made use of grand jury subpoenas to obtain documents from third parties. However, Rajaratnam introduced no evidence that any of these records produced anything of value. The original affidavit also represented that the government had tried to conduct physical surveillance but had failed because Rajaratnam and his confederates worked in large office buildings and traveled frequently. (*See* Kang Ex. 1 at 39–42.) Other than the government's slapdash efforts to perform surveillance and thereby touch all the bases in its

1002, 1011 (2d Cir. 1976) (rejecting suppression where "even though state or federal officers may have garnered sufficient information without the use of wiretaps to support an indictment . . . . there was every reason to believe that additional co-conspirators were involved who could not be successfully investigated without wiretapping"); *United States v. Blount,* 30 F. Supp. 2d 308, 312 (D. Conn. 1997) (rejecting suppression where investigation "reflected the need for additional information to tie conclusively into the conspiracy not only those targeted by and named in the application, but others then unidentified" because "[t]hose added purposes buttressed the government's claim that though successful to a degree, the methods used had not entirely succeeded").[25]

Rajaratnam responds that if the government believed it needed more evidence "there was absolutely nothing to prevent the USAO, FBI, and SEC from continuing to use these same techniques to develop additional evidence going forward based on

---

wiretap application, nothing adduced at the *Franks* hearing cast doubt on the accuracy of the representation itself.

[25] *Cf. United States v. West,* 589 F.3d 936, 939 (8th Cir.2009) ("If law enforcement officers are able to establish that conventional investigatory techniques have not been successful in exposing the full extent of the conspiracy and the identity of each coconspirator, the necessity requirement is satisfied."); *United States v. McLee,* 436 F.3d 751, 763 (7th Cir.2006) ("The government's demonstrated need for a wiretap as a means of identifying all coconspirators and the roles they occupied in the structure of the conspiracy is sufficient for a finding of 'necessity' under the statute.").

the leads already developed." (Rajaratnam Post Hr'g Reply Br. at 15.) Not so says the government. Despite the development of circumstantial evidence that led to flipping Roomy Khan in early 2008, the criminal authorities say they had "hit a bit of a wall" by March 2008. (*Franks* Tr. at 814.) Not surprisingly, both parties' positions are overstated. It is likely true, as Rajaratnam contends, that the government could have developed more evidence by conventional means and proceeded to indictment of at least some alleged co-conspirators. Indeed, the government asserts that this is the very first time that wiretaps have been used in an insider trading investigation. (Michaelson Ex. 2 at 4.) It is clear that conventional techniques have at least proven adequate in the past. But whether they were or would be adequate in the present cases requires a more particular inquiry.

Could or should the government have done more with conventional techniques to test whether a wiretap was "necessary"? It is hard to make that argument with regard to document subpoenas, search warrants, and other forms of documentary investigation. Over four million documents from targets and third parties had already been gathered. Analysis of the documentary evidence was fairly sophisticated and while this revealed much circumstantial evidence of insider trading it also confirmed what one would expect: insider trading is typically conducted verbally. Thus it seems reasonably unlikely that additional documents would have produced qualitatively different evidence.

Rajaratnam argues that the criminal

authorities "had not finished doing their own homework by actually completing their review of the documentary evidence that [the SEC] had obtained." (Rajaratnam Post Hr'g Reply Br. at 15.) Given that Rajaratnam so strenuously argues that the SEC and the criminal authorities were effectively one and the same, his argument that the USAO and FBI needed to rework the analysis provided by the SEC is unconvincing. Particularly where the documents suggest that defendants were careful not leave a paper trail, there is little reason to believe that Judge Lynch would have required the criminal authorities to repeat the SEC's effort. *See Steinberg,* 525 F.2d at 1131. While it is theoretically possible that the criminal authorities could have found a needle in the haystack, that search hardly would have been "cost-effective", *Ippolito,* 774 F.2d at 1486, and the government is not "required to exhaust all conceivable investigative techniques before resorting to electronic surveillance." *Concepcion,* 579 F.3d at 218. Moreover, at least one court in this Circuit has rejected a *Franks* challenge premised in part on the ground that criminal authorities relied on other agencies' reports about their own files. *See United States v. Pappas,* 298 F. Supp. 2d 250, 265 (D. Conn. 2004) (rejecting *Franks* challenge where FBI agent "fail[ed] to disclose in his affidavit the fact that he did not physically review the Arizona DEA's and FBI's files" in part because "the inclusion of this information in the affidavit would not have precluded a finding that the Government satisfied the necessity requirement").

The criminal authorities also had other options. They could have introduced undercover

agents, but Rajaratnam points to no reason why Judge Lynch should have doubted "the difficulty of introducing a [n undercover agent] into this close-knit scheme." (Kang Ex. 1 at 47.) Whether additional witness interviews were "reasonably unlikely to succeed" presents a much closer question. As an initial matter, a properly drafted affidavit would have (and should have) disclosed that the SEC interviewed numerous Galleon employees, including Rajaratnam himself, and had identified at least twelve other potential interviewees based on trading records, phone records, and IMs. However, none of the people the SEC interviewed admitted any insider trading and the most useful piece of information they provided was that Rajaratnam was friends with Rajiv Goel. In this respect, at least, it appears that the SEC, and by inference the criminal authorities, had "hit a wall" of sorts. Where an investigation develops strong circumstantial evidence of wrongdoing but then is confronted by "stonewalling" by witnesses, the case for wiretapping is surely strengthened.

The FBI, however, seemed to have more success than the SEC. When the FBI interviewed Roomy Khan, she agreed to cooperate, identified sources of information, and recorded phone calls with Rajaratnam. (Michaelson Exs. 109, 110; Goldberg Ex. 17; *Franks* Tr. at 753.) And none of this compromised the covert nature of the criminal investigation. It is therefore natural to ask why the FBI could not have tried to flip any of the twelve other potential interviewees that the SEC had identified, including Rajiv Goel. And if the government is correct that witnesses take a criminal investigation more seriously than one conducted by

the SEC (*Franks* Tr. at 639–40, 654–55, 799–801), it may be inferred that attempting to interview or seek the cooperation of other witnesses was a conventional technique that would, in fact, be likely to succeed.

Two reasons emerged from the hearing, however, as to why it made sense to approach Khan but not others. First, it was suggested that Khan "was the only one that [the criminal authorities] had what [they] felt to be convincing enough evidence that made an approach a reasonable risk to take." (*Franks* Tr. at 813.) Khan's prior conviction coupled with damaging IMs, call logs and trading records made this a fair judgment. Second, and indisputably, Khan's agreement to cooperate against Rajaratnam in 2002 made her "a good candidate for cooperation" in the present case. (*Franks* Tr. at 812–13.) So there was a good reason to start with Khan, and given her unique posture, her cooperation does not necessarily imply that other targets could also be flipped.

Rajaratnam dismisses the risks that a failed approach to other targets could compromise the criminal investigation since the existence of the SEC investigation would have likely been known by other targets. But the Court sees this as a closer question of judgment. The Court is aware that "[d]istrict courts must remain vigilant in ensuring that . . . reasoning [ ] based more on efficiency and simplicity than necessity [ ] will not justify a wiretap." *Concepcion,* 579 F.3d at 220. However, Title III only requires a showing that traditional techniques are *"reasonably* unlikely to succeed"; "a reasoned explanation, grounded in the facts of the case, and which squares with common sense, is all that is

required . . ." *Scala,* 388 F. Supp. 2d at 404 (internal quotation marks omitted); *see also Conception,* 579 F.3d at 218; *Fury,* 554 F.2d at 530. Rajaratnam, who bears the burden of proof, *Franks,* 438 U.S. at 155–56, has not introduced any evidence other than the success of the Khan approach that suggests that attempting to flip other witnesses was a risk-free strategy that rendered a wiretap unnecessary. And the government's contention that Roomy Khan was a special case is not unreasonable. In that circumstance, suppression based on speculation that alternative strategies might have been effective seems inappropriate. *See United States v. Shipp,* 578 F. Supp. 980, 989 (S.D.N.Y. 1984) (Weinfeld, J) ("Monday morning quarterbacking as to what investigative techniques the agents should have employed in addition to what they did employ is utterly unrealistic, if not naive."), *aff'd sub nom. United States v. Wilkinson,* 754 F.2d 1427 (2d Cir. 1985).

Finally, Rajaratnam argues that "[t]he government has conspicuously failed to cite any case, from any jurisdiction, ever, that found a wiretap to be necessary under the circumstances that a corrected affidavit would disclose in this case." (Rajaratnam Post Hr'g Reply Br. at 16.) As an initial matter, that argument seems to saddle the government with Rajaratnam's own burden of proof. *See Franks,* 438 U.S. at 155–56. And Rajaratnam himself fails to cite any case where a court found a wiretap unnecessary in the circumstances that a corrected affidavit would

have disclosed here.[26] Rajaratnam cites *United States v. Aileman,* 986 F. Supp. 1228 (N.D. Cal. 1997), but suppression in that case was based in part on the fact that the criminal authorities "made little meaningful effort, before [they] applied for the wiretap, to draw on the resources or the expertise of the Customs Service, the IRS, the INS, the FBI, or the Canadian office of the DEA" or a related investigation conducted by Canadian authorities. *Id.* at 1301, 1314. The entire premise of Rajaratnam's *Franks* challenge is that the criminal authorities here did exactly the opposite with respect to the SEC.

---

[26] The dearth of decisions ordering suppression is hardly surprising, since, with the exception of *United States v. Lilla,* 699 F.2d 99 (2d Cir. 1983), and *United States v. Concepcion,* No. 07–CR–1095, 2008 WL 2663028 (S.D.N.Y. July 1, 2008), *rev'd* 579 F .3d 214 (2d Cir. 2009), the Court is not aware of any case in this Circuit where a court found a wiretap unnecessary in any circumstance. *Conception* was reversed by the Second Circuit, *see* 579 F.3d 214, and *Lilla* is distinguishable because, unlike the corrected affidavit here, which would have described an extensive investigation to determine the identity of Rajaratnam's sources, the affidavit in that case "merely asserted that 'no other investigative method exists to determine the identity' of individuals who might have been involved" with the drug dealer from whom the officers had already purchased drugs and, to all appearances, could easily approach again. *See id.* at 104. Rajaratnam argues that "[t]he fact that the Second Circuit considered *Concepcion* to be 'exceptionally close,' even though *none* of these conventional techniques were available to the criminal investigators in that case, simply shows how far short of the statutory demonstration of necessity a corrected affidavit would fall in this case." (Rajaratnam Post Hr'g Reply Br. at 16 (emphasis in original).) That argument is misplaced because the allegedly available techniques in that case—confidential informants and physical surveillance—were likely unavailable here.

Instead, *United States v. Zolp,* 659 F. Supp. 692, (D.N.J. 1987) seems the most apposite decision. In that case, which involved a securities fraud scheme regarding a company called Laser Arms, the government's wiretap applications claimed that:

> participants in securities fraud schemes conduct much of the unlawful side of their business over the telephone; such participants are aware the paper documentation involved in their business is subject to being subpoenaed and they thus often prepare such documentation so as to conceal wrongdoing; the confidential informant's knowledge of, and anticipated testimony on, the conspiracy would be insufficient to bring about convictions of all participants in the conspiracy; surveillance and searches of the premises would be insufficient to reveal the full extent of the conspiracy; and, because many of the suspects were aware of the pending SEC investigation into Laser Arms, they were particularly cautious about infiltration and "normal" governmental surveillance.

Id. at 710. Like Rajaratnam here, Zolp argued (a) that the "affidavits failed to set forth details of [a] SEC civil proceeding against Laser Arms and thus failed to advise the judge to whom the initial wiretap application was directed that normal investigative surveillance techniques had already proven effective in the investigation" and (b) that "the judges to whom the applications were made might not have authorized the wiretaps had they been made aware of

the success which 'normal' investigative techniques had already achieved." *Id.* But the court found this argument "unpersuasive" where "the judges to whom the wiretap applications were made were aware that non-wiretap techniques had produced information against Laser Arms at least sufficient to suspend trading in Laser Arms stock" but "the affidavit [wa]s explicit that 'normal' techniques were unlikely 'to determine the complete scope of the RICO conspiracy and related predicate offenses in which [the targets] [we]re involved, and to identify the other participants and the roles played by such other participants.'" *Id.* at 710–11. Just so, with the affidavit, as corrected, here.

C. Chiesi's Claims

Chiesi also argues that the government failed to demonstrate necessity in its initial August 13, 2008 wiretap application. She makes two arguments. First, she accuses the government of misstating information in the August 13, 2008 Kang Affidavit. (Chiesi Br. at 10, 16 n.9 & n.10.) Second, she says that the government did virtually no investigation of her before requesting wiretap authorization—in other words, that there were not minimally adequate facts to justify Judge Sullivan's order authorizing wiretaps of her phones. (Chiesi Br. at 10–11, 14–20.) Both arguments are unavailing.[27]

[27] Chiesi also incorporates all of Rajaratnam's arguments regarding necessity, "because those allegations are nearly identical to and form the basis of the necessity allegations with respect to the necessity of the wiretaps over the Chiesi Phones."

1. *False or Misleading Statements or Omissions in the August 13 Kang Affidavit*

Chiesi argues that the August 13, 2008 Kang Affidavit made various false statements. Unlike Rajaratnam, Chiesi does not request a *Franks* hearing to probe the government's conduct in preparing its first application, on August 13, 2008, for authorization to wiretap her phones. Instead, she appears to argue that suppression is warranted based on the allegations made in her brief. However, there is "a presumption of validity with respect to the affidavit supporting the search warrant," *Franks,* 438 U.S. at 171, and Chiesi's allegations do not come close to showing that the affidavit was false or misleading or that the government drafted it with "reckless disregard", never mind that its "remaining content is insufficient." *Id.* at 156.[28]

Chiesi points to the affidavit's comment that

(Chiesi Br. at 15 n.7.) Were that true, Chiesi would have the same right to a *Franks* hearing that the Court granted Rajaratnam. It is not true, however, because there is no indication that the SEC investigation extended to Chiesi and her sources. The omission of that investigation is the most glaring problem that Rajaratnam identifies in the government's March 7, 2008 affidavit. But it has little relevance to Chiesi.

[28] *Franks* itself states that this standard applies "at that hearing," *Franks v. Delaware,* 438 U.S. 154, 156 (1978), but given that the *Franks* standard is designed to ensure that a "challenger's attack must be more than conclusory," *id.* at 171, it would make no sense that a defendant who chose to challenge an affidavit without a hearing could win suppression by satisfying a lower standard.

wiretaps would help to reveal, among other things, the "identities of the TARGET SUBJECTS, their accomplices, aiders and abettors, co-conspirators and participants in their illegal activities." (Gov't Opp'n to Chiesi Ex. 1-C at 8.) According to Chiesi, this was false because the government already knew that Moffat, De Ruiz, and Taylor were Chiesi's sources. (Chiesi Br. at 15 n.8.) Even granting this, all the government knew was that Chiesi had at least three sources—not that she had *only* three.

Chiesi also cites the affidavit's claims that various investigative techniques would not work (Gov't Opp'n to Chiesi Ex. 1-C at 34-41), claims she calls unsupportable," "self-contradictory," and "untrue." (Chiesi Br. at 16 n.9 & n.10, 17.) Chiesi, for example, believes that it was misleading for the government to say that requesting more detailed records from clearing firms about the trading activity of Chiesi's hedge fund, New Castle, could jeopardize the investigation. (Gov't Opp'n to Chiesi Ex. 1-C at 37.) She argues that the government had reviewed Galleon records during the previous few years, and it could have done the same for New Castle records. (Chiesi Br. At 16 n.10.) But Chiesi offers no evidence that the SEC was investigating Chiesi at the time, or that she or New Castle had any other reason to suspect they were targets of a federal criminal investigations. The government could reasonably have worried that requesting records would have tipped Chiesi's fund. In the same way, the government could reasonably have worried that witness interviews could compromise the investigation.

Finally, Chiesi accuses the government's affidavit of internal inconsistencies in describing why witness interviews and confidential informants would be inadequate substitutes for wiretapping. In one place, the affidavit claimed that witness interviews of Chiesi or other target subjects would be too risky and could jeopardize the investigation. (Gov't Opp'n to Chiesi Ex. 1-C at 37-38.) In another, it mentioned two confidential informants and noted that it had approached three other individuals, each of whom "has provided information to the government in connection with the investigation," but none of whom "communicates directly with CHIESI or any other TARGET SUBJECT." (*Id.* at 39-40.) There is no internal inconsistency here. The affidavit's section on witness interviews related only to interviewing Chiesi and other target subjects; the section on confidential informants did not. (*See id.* at 40.)

For all these reasons the Court finds no evidence that the government knowingly or recklessly misled Judge Sullivan. The Court therefore finds no reason to disregard the "presumption of validity with respect to the affidavit supporting the search warrant." *Franks,* 438 U.S. at 171.

2. *Minimally Adequate Facts in the Affidavit to Justify Wiretap Authorization*

Chiesi nevertheless attacks the sufficiency *vel non* of the August 13, 2008 Kang Affidavit's necessity section on the ground that it too closely resembled the necessity section in the March 7, 2008 Kang

Affidavit in support of wiretap authorization for Rajaratnam's phone. The Second Circuit has held that "generalized and conclusory statements that other investigative techniques would prove unsuccessful" are inadequate to satisfy the necessity requirement. *Lilla,* 699 F.2d at 104. True enough, but Judge Sullivan has made a considered determination that the August 13, 2008 Kang Affidavit adequately supported a finding that wiretaps were necessary to the government's investigation of Chiesi. And, absent any misstatements, that determination is entitled to "considerable deference," *Concepcion,* 579 F.3d at 217 & n.1, with the reviewing court's task limited to ensuring that the application was "minimally adequate to support the determination that was made," *Miller,* 116 F.3d at 663.

The August 13, 2008 Kang Affidavit was particularized enough to Chiesi to pass muster under this standard of review. It described, for example, law enforcement officers' attempts to surveil Chiesi. (Gov't Opp'n to Chiesi Ex. 1-C at 34-35.) The government also explained why physical surveillance of Chiesi's residence was not likely to be successful: (1) it was not yet sure where or when Chiesi might be meeting with sources or co-conspirators; and (2) physical surveillance was "expected to be of limited utility," because the government anticipated that the primary means by which Chiesi and other targets subjects were engaging in the crime was via telephone. (*See* Gov't Opp'n to Chiesi Ex. 1-C at 35-36.) The fact that the Rajaratnam warrant affidavit closely parallels the Chiesi one is similarly unproblematic. Where boilerplate accurately depicts

the facts on the ground, Title III requirements are satisfied. *See United States v. Herrera,* No. 02–CR–0477, 2002 WL 31133029, at *2 (S.D.N.Y. Sept. 23, 2002) (Kaplan, J.) (upholding use of "boilerplate" language, noting that it "should come as no surprise that the facts supporting the conclusion that the alternative methods would be unavailing often are similar from one narcotics operation to another").

Chiesi also argues that the August 13, 2008 Kang Affidavit is insufficient on its face because the government failed to first try a number of conventional techniques, such as reviewing New Castle's trading records, approaching potential witnesses, trying to flip targets, trying to identify confidential informants, inserting an undercover agent, and applying for a conventional search warrant. (Chiesi Br. 16-17.)[29] But "[a]gents are not required to resort to measures that will clearly be unproductive." *Terry,* 702 F.2d at 310. Even assuming that the use of alternative techniques would have achieved some measure of success, the government was entitled to use a wiretap if necessary

[29] Chiesi thinks that too little time passed between the government's finding out about her and its request for wiretap authorization—two months—for it to have conducted a meaningful investigation. But "[t]here is no rule on the amount of time investigators must try and fail, using other methods, before turning to a wiretap application." *United States v. Cartagena,* 593 F.3d 104, 110 (1st Cir. 2010) (brackets in original) (internal quotation marks omitted).

to achieve other investigatory objectives.[30] *See Gambino,* 734 F. Supp. at 1103; *United States v. Cartagena,* 593 F.3d 104, 110 (1st Cir. 2010) ("Even if traditional investigative procedures produce some results, the *partial* success of the investigation does not mean that there is nothing more to be done.") (emphasis in original) (internal quotation marks and alterations omitted). In this case, the government provided a "reasoned explanation" that "square[d] with common sense," *Scala,* 388 F. Supp. 2d at 404, as to why only a wiretap would achieve all of its investigatory goals. That "is all that is required." *Shipp,* 578 F. Supp. at 989.

In sum, the government fulfilled its statutory responsibility to "inform the authorizing judicial officer of the nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods." *Torres,* 901 F.2d at 231. At the least, minimally adequate facts existed to justify Judge Sullivan's decision authorizing the wiretaps of Chiesi's phones.

IV. Minimization

Rajaratnam and Chiesi both challenge a number of intercepts because they say the government failed to minimize properly. Title III

[30] Chiesi also contends that other insider trading investigations have succeeded without using Title III, and this one could have too. But on that logic Title III would never justify wiretapping for types of investigations that sometimes succeed without wiretaps. That is not the law.

requires that eavesdropping "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." 18 U.S.C. § 2518(5). Every wiretap order must contain a provision mandating minimization in accordance with Title III. *See id.* Here, the judges who authorized wiretapping of both defendants' telephones included such a provision in their orders of authorization. Therefore the question is "whether the [g]overnment obeyed the provision in carrying out the wiretaps." *United States v. Salas,* 07–CR–0557, 2008 WL 4840872, at *6 (S.D.N.Y. Nov. 5, 2008) (Koeltl, J).

The minimization 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." *Scott v. United States,* 436 U.S. 128, 140 (1978). It "only requires a reasonable effort to minimize the interception of irrelevant calls." *United States v. McGuinness,* 764 F. Supp. 888, 900 (S.D.N.Y. 1991) (citing *United States v. Manfredi,* 488 F.2d 588 (2d Cir. 1973), *cert. denied,* 417 U.S. 936 (1974)).

Compliance is measured by the reasonableness of the monitoring agents under the circumstances. *See Scott,* 436 U.S. at 139; *Salas,* 2008 WL 4840872, at *6. Reasonableness is gauged "in the context of the entire wiretap, as opposed to a chat-by-chat analysis." *McGuinness,* 764 F. Supp. at 901. "[T]he mere fact that every conversation is monitored does not necessarily render the surveillance violative of the minimization requirement of the statute . . . .

[N]o electronic surveillance can be so conducted that innocent conversation can be totally eliminated." *United States v. Bynum,* 485 F.2d 490, 500 (2d Cir. 1973), *vacated on other grounds,* 417 U.S. 903 (1974). Even "where the percentage of nonpertinent calls is relatively high," their interception may still be reasonable in some cases. *Scott,* 436 U.S. at 140. And "when the investigation is focusing on what is thought to be a widespread conspiracy more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise." *Id.* Moreover, the "minimization requirement does not extend to calls lasting two minutes or less." *Salas,* 2008 WL 4840872, at *6 (citing *Bynum,* 485 F.2d at 500); *see United States v. Capra,* 501 F.2d 267, 275–76 (2d Cir. 1974).

The government has the burden to show that it properly minimized intercepts. *See United States v. Rizzo,* 491 F.2d 215, 217 n.7 (2d Cir. 1974). Once a prima facie showing is made, the burden shifts to the defendant to show that, despite a good faith compliance with the minimization requirements, "a substantial number of non-pertinent conversations have been intercepted unreasonably." *United States v. Menendez,* No. 04–219, 2005 WL 1384027, at *3 (S.D.N.Y. June 8, 2005) (citing cases); *United States v. Ianniello,* 621 F. Supp. 1455, 1470 (S.D.N.Y. 1985) (Weinfeld, J.).

A. Rajaratnam's Claims

In support of his claim that the government failed to comply with the minimization requirement, Rajaratnam cites 150 calls that were non-pertinent

but were still recorded. (*See* Rajaratnam Br. at 74.) Of the 150 non-pertinent conversations mentioned, Rajaratnam only actually summarizes 69. (*See* Rajaratnam Br. Ex. E.1.) By the Court's count, 54 of those 69 calls lasted less than two minutes. (*See id*.) Accordingly, they were not subject to the minimization requirement. *See Salas*, 2008 WL 4840872, at *6. The remaining 15 calls represent .68 percent of the total calls (2,200) the FBI intercepted. The government says that even these calls were minimized frequently. (*See* Gov't Opp'n to Rajaratnam at 69.) In these circumstances the government's conduct in monitoring the Rajaratnam wiretap was objectively reasonable. *See Salas,* 2008 WL 4840872, at *7 (failing to minimize 11 calls out of 1,541 "was not objectively unreasonable"); *Bynum,* 485 F.2d at 500 ("[N]o electronic surveillance can be so conducted that innocent conversation can be totally eliminated.").

In addition, the government has represented to the Court that it took "extensive measures" to "increase the likelihood of its compliance." (Gov't Opp'n to Rajaratnam at 69.) In particular, it maintained monitoring logs; submitted progress reports to the issuing court; briefed monitoring officers on the minimization requirements; and posted written memos at the wire facilities explaining the standards for minimization and the procedures to be followed for compliance. (*Id*.) As other courts have held, such measures "are helpful in establishing compliance with the minimization requirement." *Menendez,* 2005 WL 1384027, at *3-4; *see United States v. Pichardo,* No. 97-CR-02323, 1999 WL 649020, at *6 (S.D.N.Y. Aug. 25, 1999) (internal

citations omitted).

Considering the "nature and scope of the criminal enterprise under investigation," *Pichardo,* 1999 WL 649020, at *6, the small number of interceptions to which Rajaratnam raises any objection at all, and the government's precautions to ensure compliance with the minimization requirement, Court finds that the government acted objectively reasonably under the circumstances. No suppression is required.

B. Chiesi's Claims

Chiesi claims that 155 calls lasting more than two minutes, or 13.9% of the 1, 116 intercepted called lasting longer than two minutes, pertained solely to personal issues. She contends that the government made virtually no effort to minimize these recordings. (Chiesi Br. at 32.) The Court disagrees. In reality, the government spot-checked frequently and minimized more than 50 percent of the duration of these 155 calls. (*See* Gov't Opp'n to Chiesi Ex. 9.)

Chiesi, moreover, does not dispute that 29 of the challenged calls "involved a communication between Chiesi and an individual with whom Chiesi frequently engaged in pertinent, criminal conversations." (Gov't Opp'n to Chiesi at 38.) Some of the 29 calls themselves involved pertinent information. Chiesi calls this "incorrect" because the calls "contained significant personal content" as well. (Chiesi Reply Br. At 18.) That the calls contained both personal and pertinent content, however, does not make them non-pertinent altogether. Nor does it

mean that the calls should have been terminated for veering into the speakers' personal lives. As Judge Koeltl noted in *Salas,* "[s]ome allowance must . . . be made for the fact that conversations can shift topics, and it would be unreasonable for surveilling agents to minimize each call that did not begin as incriminating." *Salas,* 2008 WL 4840872, at *7; *see Ianniello,* 621 F. Supp. at 1471 ("It is common, of course, for conversations to treat more than one subject, and entirely possible for such dialogues to be comprised of discussion of innocent matters, interspersed with topics of a criminal nature. The statutory requirement of minimization does not mean that only communications exclusively devoted to criminal subjects may be intercepted."). Even so, the 29 called were minimized; the government recorded 72 percent of the total duration of those calls.

The remaining 126 calls were spot-checked and minimized; ultimately the government monitored and recorded about 40 percent of their duration. (Gov't Opp'n to Chiesi at 39.) Only seven of these calls were not minimized at all. (*See id*. at 40; Ex. 9, Calls M-25, M-32, M-45, M-100, M-119, M-135, M-140.) In two of them, Chiesi discussed AMD, a company about which inside information was allegedly exchanged. (Gov't Opp'n to Chiesi Ex. 9, Calls M-45, M-140.) Three other calls barely passed the two-minute mark. (*Id*., Calls M-25, M-32, M-119.)

Beyond this, the government has represented to the Court that it took extensive measures to comply with the minimization requirement. As it did for the Rajaratnam wiretap, the government maintained monitoring logs; submitted progress

reports to the issuing court; briefed monitoring officers on the minimization requirements; and posted memoranda at the wire facilities explaining the standards for minimization and the procedures to be followed for compliance. (Gov't Opp'n to Chiesi at 40.) These measures provide more evidence of the government's substantial compliance with the minimization requirement. *See Pichardo,* 1999 WL 649020, at *6.

The government's efforts here were at least as good as those upheld in *Salas*. There, the government had intercepted 50 calls lasting more than two minutes, 11 of which were non-pertinent calls that were not minimized at all. 2008 WL 4840872, at *7. Here, the government intercepted 1,116 calls lasting more than two minutes, of which Chiesi challenges 155. Even assuming that all of Chiesi's contentions are right, the Court finds the government's conduct objectively reasonable under the circumstances.

CONCLUSION

For the foregoing reasons, Rajaratnam's and Chiesi's motions [86, 90] to suppress are denied.[31]

---

[31] By letter dated May 12, 2010, Chiesi also moved to suppress evidence that the government had obtained pursuant to wiretaps of phones used by C.B. Lee and Ali Far. That motion is denied. First, as Chiesi implicitly acknowledges, evidence obtained from the Rajaratnam and Chiesi wiretaps supports probable cause for wiretapping Lee's and Far's phones. (*See* May 12, 2010 Letter at 2.) Second, Chiesi has not established that the government's October 14, 2008, application to wiretap Lee's

SO ORDERED.

Dated: New York, New York
November 24, 2010

/s/ Richard J. Holwell
Richard J. Holwell
United States District Judge

---

and Far's phones was deficient in describing why wiretaps were necessary. Chiesi says that the government only attempted physical surveillance of Lee once, and that its October 14 affidavit closely resembled the August 13, 2008 affidavit. This argument fails for exactly the reasons articulated above in the section rejecting Chiesi's motion to suppress based on the government's failure to establish necessity.

UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 18th day of November, two thousand thirteen,

---

United States of America,

Appellee,

ORDER

v.

Docket No: 11-4416

Raj Rajaratnam,

Defendant - Appellant.

Appellant Raj Rajaratnam filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. The panel that determined the appeal has considered the request for panel rehearing, and the active members of the Court have considered the request for rehearing *en banc*.

IT IS HEREBY ORDERED that the petition is denied.

FOR THE COURT:
Catherine O'Hagan Wolfe, Clerk

/s/ Catherine O'Hagan Wolfe

Constitution of the United States, Amendment IV

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

United States Code

Title 15. Commerce and Trade

Chapter 2B. Securities Exchanges

§ 78j. Manipulative and deceptive devices

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange--

(a)(1) To effect a short sale, or to use or employ any stop-loss order in connection with the purchase or sale, of any security other than a government security, in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

(2) Paragraph (1) of this subsection shall not apply to security futures products.

(b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement (as defined in section 206B of the Gramm-Leach-Bliley Act), any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

(c)(1) To effect, accept, or facilitate a transaction involving the loan or borrowing of securities in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

(2) Nothing in paragraph (1) may be construed to limit the authority of the appropriate Federal banking agency (as defined in section 1813(q) of Title 12), the National Credit Union Administration, or any other Federal department or agency having a responsibility under Federal law to prescribe rules or regulations restricting transactions involving the loan or borrowing of securities in order to protect the safety and soundness of a financial institution or to protect the financial system from systemic risk.

Rules promulgated under subsection (b) of this section that prohibit fraud, manipulation, or insider trading (but not rules imposing or specifying reporting or recordkeeping requirements, procedures, or standards as prophylactic measures against fraud, manipulation, or insider trading), and judicial precedents decided under subsection (b) of this section and rules promulgated thereunder that prohibit fraud, manipulation, or insider trading, shall apply to security-based swap agreements (as defined in section 206B of the Gramm-Leach-Bliley Act) to the same extent as they apply to securities. Judicial precedents decided under section 77q(a) of this title and sections 78i, 78o, 78p, 78t, and 78u-1 of this title, and judicial precedents decided under applicable rules promulgated under such sections, shall apply to security-based swap agreements (as defined in

section 206B of the Gramm-Leach-Bliley Act) to the same extent as they apply to securities.

United States Code

Title 18. Crimes and Criminal Procedure

Part I. Crimes

Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications

§ 2510. Definitions

As used in this chapter--

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

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

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto

Rico, and any territory or possession of the United States;

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

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

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

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

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

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

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

(9) "Judge of competent jurisdiction" means--

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

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

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

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

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic,

photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

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

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

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

(13) "user" means any person or entity who--

(A) uses an electronic communication service; and

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

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

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

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

(A) scrambled or encrypted;

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

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

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

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

(17) "electronic storage" means--

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

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

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

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

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

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

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

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

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

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

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

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

(21) “computer trespasser”--

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

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

* * *

§ 2510 note (Congressional Findings)

Section 801 of Pub. L. 90-351 provided that: "On the basis of its own investigations and of published studies, the Congress makes the following findings:

"(a) Wire communications are normally conducted through the use of facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings, and by persons whose activities affect interstate commerce.

The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

"(b) In order 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, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

"(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such 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.

"(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused."

United States Code

Title 18. Crimes and Criminal Procedure

Part I. Crimes

Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications

§ 2515. Prohibition of use as evidence of intercepted wire or oral communications

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

United States Code

Title 18. Crimes and Criminal Procedure

Part I. Crimes

Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications

§ 2516. Authorization for interception of wire, oral, or electronic communications

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

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of

the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons) chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

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

(c) any offense which is punishable under the following sections of this title: section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit

applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the

United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), section a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport

issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

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

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

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

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

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

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

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

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

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

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

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

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

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

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

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

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

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, 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, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

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

United States Code Annotated

Title 18. Crimes and Criminal Procedure

Part I. Crimes

Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications

§ 2518. Procedure for interception of wire, oral, or electronic communications

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

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

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

offense and whose communications are to be intercepted;

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

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

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

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

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

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

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

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

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

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

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

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

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

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

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

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

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose

communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any

event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

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

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

(a) an emergency situation exists that involves--

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

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

(iii) conspiratorial activities characteristic of organized crime,

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

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

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized

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

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

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

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

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

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

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing,

or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

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

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

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

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

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

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

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

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

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

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

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

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

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

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

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

(iv) the order authorizing or approving the interception is limited to interception only for such

time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

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

Code of Federal Regulations

Title 17. Commodity and Securities Exchanges

Chapter II. Securities and Exchange Commission

Part 240. General Rules and Regulations, Securities Exchange Act of 1934

Subpart A. Rules and Regulations Under the Securities Exchange Act of 1934

Manipulative and Deceptive Devices and Contrivances

§ 240.10b–5 Employment of manipulative and deceptive devices.

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

(a) To employ any device, scheme, or artifice to defraud,

(b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or

(c) To engage in any act, practice, or course of business which operates or would operate as a fraud

or deceit upon any person, in connection with the purchase or sale of any security.

Code of Federal Regulations

Title 17. Commodity and Securities Exchanges

Chapter II. Securities and Exchange Commission

Part 240. General Rules and Regulations, Securities Exchange Act of 1934

Subpart A. Rules and Regulations Under the Securities Exchange Act of 1934

Manipulative and Deceptive Devices and Contrivances

§ 240.10b5–1 Trading "on the basis of" material nonpublic information in insider trading cases.

Preliminary Note to § 240.10b5–1: This provision defines when a purchase or sale constitutes trading "on the basis of" material nonpublic information in insider trading cases brought under Section 10(b) of the Act and Rule 10b–5 thereunder. The law of insider trading is otherwise defined by judicial opinions construing Rule 10b–5, and Rule 10b5–1 does not modify the scope of insider trading law in any other respect.

(a) General. The "manipulative and deceptive devices" prohibited by Section 10(b) of the Act (15 U.S.C. 78j) and § 240.10b–5 thereunder include, among other things, the purchase or sale of a security of any issuer, on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly,

indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information.

(b) Definition of "on the basis of." Subject to the affirmative defenses in paragraph (c) of this section, a purchase or sale of a security of an issuer is "on the basis of" material nonpublic information about that security or issuer if the person making the purchase or sale was aware of the material nonpublic information when the person made the purchase or sale.

(c) Affirmative defenses.

(1)(i) Subject to paragraph (c)(1)(ii) of this section, a person's purchase or sale is not "on the basis of" material nonpublic information if the person making the purchase or sale demonstrates that:

(A) Before becoming aware of the information, the person had:

(1) Entered into a binding contract to purchase or sell the security,

(2) Instructed another person to purchase or sell the security for the instructing person's account, or

(3) Adopted a written plan for trading securities;

(B) The contract, instruction, or plan described in paragraph (c)(1)(i)(A) of this Section:

(1) Specified the amount of securities to be purchased or sold and the price at which and the date on which the securities were to be purchased or sold;

(2) Included a written formula or algorithm, or computer program, for determining the amount of securities to be purchased or sold and the price at which and the date on which the securities were to be purchased or sold; or

(3) Did not permit the person to exercise any subsequent influence over how, when, or whether to effect purchases or sales; provided, in addition, that any other person who, pursuant to the contract, instruction, or plan, did exercise such influence must not have been aware of the material nonpublic information when doing so; and

(C) The purchase or sale that occurred was pursuant to the contract, instruction, or plan. A purchase or sale is not "pursuant to a contract, instruction, or plan" if, among other things, the person who entered into the contract, instruction, or plan altered or deviated from the contract, instruction, or plan to purchase or sell securities (whether by changing the amount, price, or timing of the purchase or sale), or entered into or altered a corresponding or hedging transaction or position with respect to those securities.

(ii) Paragraph (c)(1)(i) of this section is applicable only when the contract, instruction, or plan to purchase or sell securities was given or entered into in good faith and not as part of a plan or scheme to evade the prohibitions of this section.

(iii) This paragraph (c)(1)(iii) defines certain terms as used in paragraph (c) of this Section.

(A) Amount. "Amount" means either a specified number of shares or other securities or a specified dollar value of securities.

(B) Price. "Price" means the market price on a particular date or a limit price, or a particular dollar price.

(C) Date. "Date" means, in the case of a market order, the specific day of the year on which the order is to be executed (or as soon thereafter as is practicable under ordinary principles of best execution). "Date" means, in the case of a limit order, a day of the year on which the limit order is in force.

(2) A person other than a natural person also may demonstrate that a purchase or sale of securities is not "on the basis of" material nonpublic information if the person demonstrates that:

(i) The individual making the investment decision on behalf of the person to purchase or sell the securities was not aware of the information; and

(ii) The person had implemented reasonable policies and procedures, taking into consideration the nature of the person's business, to ensure that individuals making investment decisions would not violate the laws prohibiting trading on the basis of material nonpublic information. These policies and procedures may include those that restrict any purchase, sale, and causing any purchase or sale of any security as to which the person has material

nonpublic information, or those that prevent such individuals from becoming aware of such information.