# 11-4416-cr

IN THE

# United States Court of Appeals

**FOR THE SECOND CIRCUIT**

UNITED STATES OF AMERICA,

*Appellee,*

—against—

DANIELLE CHIESI,

*Defendant,*

RAJ RAJARATNAM,

*Defendant-Appellant.*

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

## BRIEF FOR DEFENDANT-APPELLANT

PATRICIA ANN MILLETT
TERENCE JOSEPH LYNAM
JAMES EAMONN SHERRY
HYLAND HUNT
AKIN GUMP STRAUSS HAUER
& FELD LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 887-4000

SAMIDH GUHA
AKIN GUMP STRAUSS HAUER
& FELD LLP
1 Bryant Park
New York, New York 10036
(212) 812-1000

*Attorneys for Defendant-Appellant*

## TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**CASES:**

**CONSTITUTION AND STATUTES:**

**RULES AND REGULATIONS:**



**OTHER AUTHORITY:**

## JURISDICTIONAL STATEMENT

The district court had jurisdiction under 18 U.S.C. § 3231. The court denied Appellant's motion to suppress, and entered the final judgment of conviction and sentence on October 25, 2011. Appellant timely filed a notice of appeal on October 13, 2011. *See* Fed. R. App. P. 4(b)(2). This Court has jurisdiction under 28 U.S.C. § 1291.

## ISSUES PRESENTED FOR REVIEW

1. Whether, when the government's false statements and misleading omissions so pervade a wiretap application that the authorizing judge cannot make the congressionally mandated findings on which issuance of a wiretap is expressly conditioned, statutory suppression under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2518(10)(a), and *United States v. Giordano*, 416 U.S. 505 (1974), is required.

2. Whether suppression under the Fourth Amendment is required when the government's false statements and misleading omissions so pervade a wiretap application that the authorizing judge cannot make the findings required by the Constitution for issuance of a wiretap in advance of the search and instead the search is upheld based on insufficient factual allegations that were never presented to the authorizing judge and that first appeared years later in a post-search *Franks* hearing.

3. Whether nine counts of conviction must be reversed because the court's instructions failed to require the jury to find the statutorily required causation element that the trade actually "used" or was made "on the basis of" material, nonpublic information.

## STATEMENT OF THE CASE

In March 2008, the FBI applied for and obtained authorization to wiretap Appellant's cell phone. The wiretap continued for nine months. On December 15, 2009, Appellant was indicted on charges of insider trading and conspiracy to commit insider trading. Appellant moved to suppress the wiretaps and, based on his showing of false statements and material omissions in the government's wiretap application, the district court ordered a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978). The district court (Holwell, J.) subsequently found that false and recklessly misleading statements and omissions pervaded the affidavit so extensively that it was impossible for the authorizing judge to have made the constitutionally and statutorily required determinations for issuance of the wiretap warrant. The court nevertheless denied suppression based on new factual allegations first presented by the government at the *Franks* hearing. A jury subsequently found Appellant guilty of five counts of conspiracy and nine counts of insider trading. He was sentenced on October 13, 2011, and, on October 25, 2011, the district court entered the final judgment of conviction and sentence.

## BACKGROUND

### A. Constitutional And Statutory Framework

**1.** The Fourth Amendment to the Constitution guarantees individuals the right "to be secure in their persons, houses, papers, and effects, against

unreasonable searches and seizures," and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV.

**a.** "[T]he very heart of the Fourth Amendment directive" is that "[p]rior review by a neutral and detached magistrate" is required before law enforcement may "inva[de] *** a citizen's private premises or conversation." *United States v. U.S. District Court*, 407 U.S. 297, 316, 318 (1972). "[P]ost-surveillance judicial review" will not suffice. *Id*. at 318. That requirement of "a prior judicial judgment," *id*. at 317, ensures "that the deliberate, impartial judgment of a judicial officer will be interposed between the citizen and the police," *Wong Sun v. United States*, 371 U.S. 471, 481-482 (1963).

The Warrant Clause obligates law enforcement to provide the authorizing judge sufficient information that he may "judge for himself the persuasiveness of the facts relied on by a complaining officer to show probable cause." *Giordenello v. United States*, 357 U.S. 480, 486 (1958). And the Clause "surely takes the affiant's good faith as its premise." *Franks*, 438 U.S. at 164. Accordingly, if a defendant establishes that the affiant, knowingly or with reckless disregard for the truth, included false statements or misleading omissions in the authorizing affidavit, then "the affidavit's false material [must be] set to one side." *Id*. at 156. If the

affidavit's "remaining content is insufficient to establish probable cause," then the fruits of the search must be suppressed. *Id.*

**b.** The Fourth Amendment "shields private speech from unreasonable surveillance," *U.S. District Court*, 407 U.S. at 313, and thus 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, 356 (1967). Because wiretaps inflict an extraordinary and prolonged intrusion on privacy, more than the ordinary standard of probable cause used to support "conventional warrants" is required. *Berger v. New York*, 388 U.S. 41, 60 (1967). For a wiretap to pass constitutional muster, the government must demonstrate both probable cause and "special facts" demonstrating "exigency" "under the most precise and discriminate circumstances," *id*. at 60, 63, that create a "genuine need" for government officials to secretly intercept private conversations, *Dalia v. United States*, 441 U.S. 238, 250 (1979). The judge authorizing the wiretap thus must independently determine not only that probable cause exists, but also that "no greater invasion of privacy was permitted than was necessary under the circumstances." *Berger*, 388 U.S. at 57.[1]

[1] The relevant constitutional and statutory provisions are appended to this brief.

**2.** Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2510-2522, to establish a "comprehensive scheme for the regulation of wiretapping and electronic surveillance" that would both implement the Fourth Amendment's "stringent" requirements and enforce congressional policy "strictly to limit the employment" of wiretapping. *Gelbard v. United States*, 408 U.S. 41, 46, 47 (1972). Congress broadly outlawed, with felony sanctions, all interceptions of wiretapped communications "[e]xcept as otherwise specifically provided in this chapter." 18 U.S.C. § 2511(1).

Congress confined wiretap authority to "certain major types of offenses and specific categories of crime." 18 U.S.C. § 2510 (note) (congressional findings); *see Gelbard*, 408 U.S. at 46. Congress's enumeration of the crimes for which the investigatory use of wiretaps is permitted, 18 U.S.C. § 2516, does not include securities fraud, 18 U.S.C. § 1348, 15 U.S.C. §§ 77q, 78j(b), or insider trading, 17 C.F.R. §§ 240.10b-5, 240.10b5-1.

"To safeguard the privacy of innocent persons," 18 U.S.C. § 2510 (note), Title III imposes "important preconditions to obtaining any intercept authority at all," *United States v. Giordano*, 416 U.S. 505, 515 (1974). Interception is "allowed only when authorized by a court of competent jurisdiction," 18 U.S.C. § 2510

(note), which is limited to an Article III or state court judge; a magistrate judge will not suffice, 18 U.S.C. § 2510(9).

Congress also "set[] forth with meticulous care" the information the government must provide to the judge to obtain a wiretap. *Dalia*, 441 U.S. at 249. Among other things, the government must provide a "full and complete statement of the facts and circumstances relied upon by the applicant" 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," 18 U.S.C. § 2518(1)(c). The authorizing judge may issue a wiretap warrant only if the judge determines "on the basis of the facts submitted by the applicant" that probable cause exists and that "normal investigative procedures *** have failed or reasonably appear to be unlikely to succeed[.]" 18 U.S.C. § 2518(3).

Rather than rely exclusively on "the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights" to enforce Title III's commands, *Giordano*, 416 U.S. at 524, Congress enacted a statutory suppression rule for "any" communication that was "obtained in violation of this chapter," 18 U.S.C. § 2518(10)(a); *see* 18 U.S.C. § 2515. Statutory suppression 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." *Giordano*, 416 U.S. at 527.

**3.** Section 10(b) of the Securities Exchange Act of 1934 makes it unlawful for any person "[t]o use or employ, in connection with the purchase or sale of any security * * * any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the [Securities and Exchange] Commission may prescribe." 15 U.S.C. § 78j(b). Congress "has not defined the criteria by which legal insider trading is separated from illegal trading" under that statute. *United States v. Chestman*, 947 F.2d 551, 572 (2d Cir. 1991) (en banc) (Winter, J., concurring in part and dissenting in part). Rather, those criteria are "based solely on administrative and judicial caselaw." *Id.* Caselaw defines the elements of insider trading as a trade made (1) on the basis of (2) material, (3) nonpublic information that was (4) disclosed by an insider (5) in breach of that insider's fiduciary duty, (6) for which the insider received a benefit, and (6) the trader knew that the insider violated a fiduciary duty by disclosing known material, nonpublic information. *See Dirks v. SEC*, 463 U.S. 646, 655-657 (1983); *SEC v. Warde*, 151 F.3d 42, 47 (2d Cir. 1998).

**B. Factual And Procedural Background**

**1.** Raj Rajaratnam was the founder and managing general partner of Galleon Management, a hedge fund investment partnership. At its largest, Galleon

employed dozens of professional portfolio managers, stock analysts, and traders, many with advanced professional degrees in technology and engineering, who assembled and analyzed publicly available information about the companies in which Galleon invested billions of dollars of client funds. JA376-389, 391-92.

On March 7, 2008, the government submitted the sworn, *ex parte* application and supporting affidavit of FBI Special Agent B.J. Kang to Judge Gerard Lynch seeking a warrant to wiretap Appellant's cellular telephone under Title III. SA3. On the basis of that affidavit, Judge Lynch approved the wiretap. *Id.* Based on that warrant and renewal applications that relied on information discovered through the wiretaps, the FBI spent nine months secretly recording over 2,200 private conversations between Appellant and at least 130 of his colleagues, employees, friends, and family. SA3-4, 64.

**2.** Subsequent to his indictment, Appellant moved to suppress the wiretaps and all evidence derived therefrom under both Title III and the Fourth Amendment. JA17-18. The district court found that Appellant made a "substantial preliminary showing" that the government's wiretap application "recklessly or knowingly misleadingly omitted several key facts *** material to Judge Lynch's determination that a wiretap was justified in this case," and accordingly ordered a hearing under *Franks v. Delaware*, *supra*. JA145.

After the *Franks* hearing, the court found that the government had repeatedly violated its duty of "candor" to the court, had recklessly disregarded the truth of its allegations of necessity and probable cause, and had included false and misleading statements throughout its affidavit. SA20-25 & n.15, 36-43.

**a.** With respect to necessity, the court found that the authorizing affidavit "glaring[ly] *** failed to disclose to Judge Lynch that the SEC had for several years been conducting an extensive [conventional] 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 unlike to be successful," even though that SEC investigation was being conducted in close coordination with the U.S. Attorney's Office and FBI and was the "heart and soul" of the criminal investigation. SA36, 42-43. The court further found that the "prosecutor and FBI were relying—almost entirely" on being "spoon-fed" by the SEC "to construct their own case." SA36, 48.

The district court found itself "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 [Appellant] 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." SA36. In particular, the court found that the government:

- Affidavit ¶40: "[B]landly assure[d] Judge Lynch that interviewing Rajaratnam and other targets is an 'investigative route' that is 'too risky at the present time.'" SA41; JA108-10.

  Court Finding of Recklessly Disregarded Truth: With the consent of and in coordination with the "criminal authorities," the SEC "had interviewed or deposed under oath over twenty Galleon employees, including two interviews and a day-long deposition of Rajaratnam." SA41.

- Affidavit ¶38: Asserted that the use of grand jury subpoenas "does not appear to be a promising method of investigation" because, *inter alia*, "[w]itnesses who could provide additional relevant evidence have not been identified[.]" JA107-08.

  Court Finding of Recklessly Disregarded Truth: The entire paragraph's content "blinks reality," SA42 & n.23, because, by the time the government submitted its application, "the SEC [had] interviewed numerous Galleon employees, including Rajaratnam himself, and had identified at least twelve other potential interviewees based on trading records, phone records, and IMs [Instant Messages]." SA52. The prosecution and FBI not only had the benefit of those interviews and depositions, but also met with the SEC before Appellant's deposition to "talk strategy." SA39.

- Affidavit ¶43: Asserted 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.'" SA41; JA111.

  Court Finding of Recklessly Disregarded Truth: "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," SA41-42, and the documents provided to the

criminal authorities "were so extensive that the government had not had the time to review all of them," a fact also withheld from Judge Lynch, SA42.

- Affidavit ¶39: Claimed that subpoenas for trading records "'would jeopardize the investigation'" because "'clearing firms *** sometimes alert traders to the requests.'" SA42; JA108.

  Court Finding of Recklessly Disregarded Truth: "[T]he SEC had already issued over two hundred subpoenas for, *inter alia*, trading records, and *** the grand jury had issued such subpoenas as well, all apparently without jeopardizing its investigation." SA42.[2]

- Affidavit ¶38: Proffered a "boilerplate assertion that 'the issuance of grand jury subpoenas likely would not lead to the discovery of critical information.'" SA42 & n.23, JA107-08.

  Court Finding of Recklessly Disregarded Truth: "Grand jury subpoenas and SEC subpoenas had already led to a mountain of incriminating circumstantial evidence as the impressively detailed chronologies prepared by [the SEC] fully attest." SA42 & n.23. In addition, the affidavit recklessly failed to disclose that the criminal authorities had also used "grand jury subpoenas to obtain documents from third parties." SA50 & n.24.

Based on those facts, the district court found that the government had made a "nearly *** full and complete *omission* of what investigative procedures in fact had been tried," SA40, had falsely withheld the very "nuts and bolts" of its conventional investigation, SA42, had said no evidence could safely be obtained through conventional techniques when a "mountain" of evidence had been and was

continuing to be obtained that way, SA42 & n.23, failed to advise Judge Lynch that criminal authorities had not yet reviewed the records, interviews, or depositions available to them, SA42, and failed to inform Judge Lynch that 12 new witnesses for potential interview had been identified, SA52. The court also found that the SEC's investigation was the "sum and substance," "heart and soul," and "the most important part" of the FBI's investigation, as the FBI "largely devoted [its] time to analyzing the information [it] w[as] receiving from the SEC," doing little on its own except "supplement[ing]" the SEC's information with some of those grand jury subpoenas that it had told Judge Lynch it could not issue. SA39-40, SA42-43. In addition, the court found it to be "likely true *** that the government could have developed more evidence by conventional means and proceeded to indictment of at least some alleged co-conspirators," and thus "[i]t is clear that conventional techniques have at least proven adequate in the past" for insider trading cases, and the FBI "attempting to interview or seek the cooperation of other witnesses was a conventional technique that would, in fact, be likely to succeed." SA51, SA53.

The court further found that the reckless falsity of almost all of the affidavit's allegations of necessity and the information "that must be presented to a

---

[2] The government continued to issue such record requests even after informing the district court that the use of such subpoenas would "jeopardize" its investigation. JA126-141.

court if it is to fulfill its function of determining [necessity]," SA42, "deprived Judge Lynch of the opportunity to assess what a conventional investigation of Rajaratnam could achieve," and made it "impossible" for him to make "a reasoned evaluation of the necessity of employing wiretaps," SA40-43.

Despite the "troubling," and "[p]articularly disturbing" questions raised by the government's misconduct, SA2, SA25, and their direct impact on the ability of Judge Lynch to make the findings required for issuance of a warrant, SA40, the district court denied suppression. The court concluded that the government's representations "now" based on facts that "emerged from the [*Franks*] hearing" established necessity. SA41, 53. Specifically, the court made factual findings that: (1) Appellant "had been careful to exchange nearly all of his inside information by telephone" and was "careful not leave a paper trail," SA49, SA52; (2) the *Franks* record "did not preclude a showing that a wiretap was necessary to confirm those sources and fully uncover Rajaratnam's network of sources," SA49-50; (3) "the SEC, and by inference the criminal authorities, had 'hit a wall' of sorts" with respect to witness interviews because "none of the people the SEC interviewed admitted any insider trading" and were "stonewalling," SA52-53; (4) although Roomy Khan had been "flipped," she was a "special case," and there was no evidence to "suggest[] that attempting to flip other witnesses was a risk-free strategy that rendered a wiretap unnecessary," SA54; and (5) reviewing the four

million records successfully obtained by conventional methods would not have been "cost-effective," SA52.

None of those facts were contained in the application submitted to the authorizing judge.

**b.** The court also found that "important information" bearing on probable cause was "omitted and misstated" in the warrant application. SA2. Specifically, the court found that the government's representations about its "key" cooperating witness were "false," SA2, 22, in that the government:

- Affidavit ¶15: Asserted that cooperating witness Roomy Khan "has not yet been charged with any crimes." SA21; JA77.

  Court Finding of Recklessly Disregarded Truth: Khan had a prior felony fraud conviction "peculiarly probative of [her] credibility" known to the government at the time of its application. SA22, 25.

- Affidavit ¶15 n.4: Contained the "literally false" statement that Khan "has been cooperating with the FBI since approximately November 2007." SA22; JA77 n.4.

  Court Finding of Non-Falsified Truth: Khan had previously attempted to cooperate in an earlier unsuccessful investigation of Appellant for insider trading in the late 1990s. SA21-22.

The Court further found that the government had "paraphrased" two consensually recorded telephone conversations between Khan and Appellant in a manner that "evince[d] a lack of frankness" and failed to "win high marks for candor." SA23-25. Specifically, the court found that the government:

- Affidavit ¶18: Asserted that Khan asked Appellant whether he was "getting anything on Intel," and that Appellant "proceeded to tell [Khan] that Intel would be up 9 to 10% and then guide down 8% and that margins would be good." SA23-24; JA79-80.

  Court Finding of Recklessly Disregarded Truth: The government "omitted the fact that Rajaratnam had qualified his predictions with 'I think,'" and "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 'because the volumes are down,'" and the government thereby made "Rajaratnam seem[] certain about the Intel numbers without giving any reason why," when in reality "Rajaratnam equivocate[d] and explain[ed] at least why he though margins would decline[.]" SA23-24.

- Affidavit ¶19: Asserted that Appellant "said he expected Xilinx to be 'below the street,'" prompting Khan to ask "whether he got 'it' from someone at the company and Rajaratnam said yes, somebody who knows." SA24; JA80-81.

  Court Finding of Recklessly Disregarded Truth: Khan actually asked whether Appellant "got it from somebody at the company or ---," to which Appellant answered "Yeah, I mean, somebody who knows his stuff," which was "more equivocal than the government's paraphrase," which simply "quoted the most inculpatory version of Rajaratnam's words." SA24 & n. 17.

The court ruled that those "literally false" misstatements and misleading omissions, while made with reckless disregard for the truth, were not "material" to Judge Lynch's finding of probable cause because a "corrected" affidavit would have contained "a residue of independent and lawful information sufficient to support probable cause," SA16, citing (1) a "toll" analysis showing that Appellant traded Intel stock in close proximity to telephone calls with an Intel employee, and

(2) three summaries of conversations recorded or intercepted in which other individuals discuss providing stock information to Appellant or Galleon. SA29-30.

**3.** At trial, the government introduced 45 wiretap recordings into evidence, as well as extensive documentary and testimonial evidence derived from the wiretaps. During its summation, the government repeatedly stressed to the jury that the wiretaps were the "core evidence in this case" for "all the crimes" charged. JA393-97.

The defense introduced extensive evidence reflecting Galleon's contemporaneous research and analysis by its own professional analysts into the very stocks and trading decisions at issue, as well as voluminous public information and analysis obtained from the more than 100 sell-side firms and other entities that Galleon dealt with daily, which supported Appellant's trading strategies. *See*, *e.g.*, Trial Tr. at 3910-4049; 4070-4266; 4273-4373; 4686-4751; 4763-4910. In charging the jury with respect to the causal element of whether Appellant's trades were "on the basis of" inside information rather than the other information in Appellant's possession, the court instructed the jury that insider trading could be found if the inside information was "a factor, however small" in his trading activity. JA433.

After almost three weeks of deliberation, the jury returned a verdict of guilty on five counts of conspiracy and nine counts of substantive securities fraud. JA44.

Appellant was subsequently sentenced to a term of 132 months' imprisonment, a $10 million fine, and ordered to forfeit $53.8 million. SA69-74.

## SUMMARY OF ARGUMENT

1. Because the constitutional mandate that search warrants rest on *prior* and independent judicial review is so ingrained in the law, neither this Court nor the Supreme Court has ever upheld a search warrant on the basis of facts that were *not* included in the original affidavit and were *never* provided to the authorizing judge. The long pattern of falsities, misleading misrepresentations, and material omissions that the government thrust on Judge Lynch *under oath* and *ex parte* here ill deserves to be the first such case; and Title III and the Constitution both flatly forbid it.

The district court, in fact, specifically found that the affidavit's false content made it "impossible" (SA43) for the authorizing judge to make the necessity finding required by both the Constitution and Title III as an indispensable prerequisite to a wiretap warrant. And rightly so: stripping out the false statements and factually eliminating the misleading distortions of the existing allegations, as *Franks* requires, destroys the affidavit's necessity and probable cause showings. The court had no license to salvage the warrant by then accepting the slew of brand new factual allegations first presented by the government during the *Franks* hearing years after the wiretap authorization issued. None of those facts were

*misleadingly* omitted; they are nothing more than the government's backpedaling do-over of its warrant application having been caught red handed misleading the court.

Choices have consequences, especially when made under oath. The government chose the factual basis on which it wanted to obtain this warrant in an *ex parte* proceeding in which the court depended on its candor and forthrightness. The government's self-chosen reckless disregard of the truth and of the critical role of independent judicial review breached that trust and desolated the warrant's basis. The government does not get to try a whole new story now. The Fourth Amendment is *not* indifferent to whether the basis for a wiretap warrant is established before or after the search. Neither is Title III. On this record, both mandate suppression.

2. Although Congress made "use" of a fraudulent device a required element of securities fraud, the court instructed the jury that it could convict Appellant on eight counts of insider trading if the inside information was "a factor, however small" in his trading decisions. That instruction, which nearly dissolves any causal connection between the information and the trades, was consistent with prior Second Circuit precedent. The Supreme Court's intervening decision in *CSX Transp., Inc. v. McBride*, 131 S. Ct. 2630, 2644 n.14 (2011), however, specifically addressed the type of statutory language required to support a "however small"

instruction in even a civil case, let alone a criminal case, and contrasted that civil statute with securities fraud, for which the Supreme Court requires proximate causation. Based on *McBride*, this Court should reconsider its erroneous precedent and, applying the rule of lenity, join its sister circuits in holding that proximate causation is required in that the government must prove that the trade actually was made "on the basis of" the inside information.

## ARGUMENT

### I. TITLE III AND THE CONSTITUTION MANDATE SUPPRESSION

Unlike any other type of search, a wiretap puts the government secretly into the home, car, office, and most intimate conversations of not only the target but also scores of individuals against whom the government has no reasonable suspicion, searching nonstop 24 hours a day for months on end.[3] For that reason, the Supreme Court has placed a "heavier responsibility" on the courts to supervise "the fairness of procedures" for obtaining such a warrant. *Berger v. New York*, 388 U.S. 41, 56 (1967). Because wiretap authorizations are an *ex parte* proceeding, however, the court's ability to stand "between the citizen and the police," *Wong Sun v. United States*, 371 U.S. 471, 481-482 (1963), depends critically on candor, honesty, and a forthright respect for the judicial role on the part of the prosecutors

[3] The wiretap in this case eavesdropped on 2,200 conversations involving more than 130 individuals. *See* SA64.

and agents who unilaterally decide what information is shared with the authorizing court.

The government broke that trust in this case. As the district court found, the government submitted a sworn affidavit to the authorizing judge that, from top to bottom, was pervaded with falsity and misleading omissions so comprehensive that it was "impossible" (SA43) for the authorizing judge to make the findings necessary to sustain the warrant and to discharge his statutory and constitutional duties of independent review. In an attempt to deny suppression and salvage the wiretap, the district court threw out the affidavit's allegations and allowed the government to substitute in their place entirely new factual allegations that first emerged in the *Franks* hearing two and a half years after the search and that bear no resemblance to the affidavit actually submitted.

That holding defies binding precedent from the Supreme Court and this Court mandating both statutory and constitutional suppression. Because this Court's duty is to construe Title III in a way that avoids raising a substantial question about the constitutionality of its wiretap authorization process, however, this Court can reverse on the statutory basis alone. *See Skilling v. United States*, 130 S. Ct. 2896, 2929-2930 (2010) (courts must "avoid constitutional difficulties by [adopting a limiting interpretation of a statute] if such a construction is fairly possible"); *United States v. Weingarten*, 632 F.3d 60, 70-71 (2d Cir. 2011).

### A. Standard Of Review

The proper interpretation of a federal statute is reviewed de novo. *Fiero v. Financial Indus. Regulatory Auth.*, 660 F.3d 569, 573 (2d Cir. 2011). Questions of constitutional law are also reviewed de novo, including whether, under *Franks*, the remaining "untainted portions [of the affidavit] suffice to support" the requisite probable cause or necessity finding. *United States v. Canfield*, 212 F.3d 713, 717 (2d Cir. 2000). The district court's factual findings, including its determination that agents made false statements deliberately or in reckless disregard for the truth, are reviewed only for clear error. *United States v. Awadallah*, 349 F.3d 42, 65 (2d Cir. 2003). The issuing judge's determination of probable cause or necessity "is not due any deference because he did not have an opportunity to assess the affidavit without the inaccuracies." *Canfield*, 212 F.3d at 717.

### B. Binding Precedent Mandates Statutory Suppression

Congress authorized wiretaps only "upon compliance with stringent conditions" that implement the congressional "policy *** strictly to limit the employment of those techniques." *Gelbard v. United States*, 408 U.S. 41, 46-47 (1972). Among those "stringent conditions," *id.* at 46, are the requirements that the government's application provide a "full and complete statement" of the necessity of a wiretap in light of other investigative procedures that have been tried and failed or are likely to fail, and a "full and complete statement of the facts and

circumstances" establishing probable cause. 18 U.S.C. § 2518(1)(b)-(c). Title III's plain text further demands that the judge's approval of a wiretap be made "on the basis of the facts submitted by the applicant," *id.* § 2518(3), prior to the warrant's issuance.

Congress meant exactly what it said, and to enforce its commands, Title III provides that, 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," statutory suppression is mandated. *United States v. Giordano*, 416 U.S. 505, 527 (1974); *see* 18 U.S.C. §§ 2515, 2518(10)(a). That congressionally commanded, "nonconstitutional" suppression remedy is broader than the Fourth Amendment's mandate, *United States v. Amanuel*, 615 F.3d 117, 125 (2d Cir. 2010), and thus is "not limited to constitutional violations," *Giordano*, 416 U.S. at 527; *id.* at 524 (Title III suppression is distinct from "the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights.").

Both separately and cumulatively, the government's comprehensive abandonment of its duty to establish truthfully, fully, and completely the necessity of and probable cause for this wiretap "on the basis of the facts submitted" to the authorizing judge, 18 U.S.C. § 2518(3), necessitates statutory suppression.

### *1. The "Full and Complete Statement" Requirements and Prior-Authorization Mandate are Critical Limitations on Wiretaps*

The statutorily mandated "full and complete statement[s]" of necessity and probable cause, as well as prior authorization by an Article III judge based on the content of the application, are critical means by which Congress "limit[ed] the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device," and thus their violation warrants suppression, *Giordano*, 416 U.S. at 527.

The Supreme Court has specifically identified the duty of "the applicant [to] state" and the authorizing court to "find that normal investigative procedures" are not viable as "important preconditions to obtaining any intercept authority at all." *Id.* at 515. Congress, in fact, wanted to be "doubly sure" that wiretaps were employed only when necessary, *United States v. Lilla*, 699 F.2d 99, 102 (2d Cir. 1983) (quoting *Giordano*, 416 U.S. at 515), and "not resorted to in situations where traditional investigative techniques would suffice to expose the crime," *United States v. Concepcion*, 579 F.3d 214, 218 (2d Cir. 2009).

The "full and complete statement" of probable cause likewise is part of the "specific and detailed procedures" that Title III prescribes in order "to ensure careful judicial scrutiny" of wiretap applications. *United States v. Gigante*, 538 F.2d 502, 503 (2d Cir. 1976); *see United States v. Huss*, 482 F.2d 38, 52 (2d Cir. 1973) (Title III's "rigorous, carefully drawn standards" enforce the Nation's

"historic" "protection of privacy" and "the spirit of liberty which has distinguished this nation from its birth.").

Further, the Supreme Court's holding in *Giordano* that the absence of the "prior, informed judgment" of Justice Department officials requires suppression because it is a "critical precondition to any judicial order," necessarily renders the absence of the "prior" and truthfully "informed judgment" of the "Federal judge" issuing that "judicial order" an equivalent ground for suppression. 416 U.S. at 515, 516; *see United States v. Marion*, 535 F.2d 697, 704 (2d Cir. 1976) (absence of statutorily required judicial approval mandated reversal of conviction). Indeed, the fact that Congress confined federal wiretap authorizations to Article III judges—debarring the commonplace role of magistrate judges in authorizing search warrants—underscores the importance that Congress attached to fully informed and independent judicial review in the wiretap authorization process.

It would stand *Giordano* and ordinary logic on their head to hold that, while internal pre-approval by the wrong person in the Justice Department alone requires statutory suppression, the government's "nearly *** full and complete omission" of a truthful necessity showing—that rendered it "impossible" for the authorizing judge to make Title III's required findings—combined with the stark distortions, false statements, and material omissions about probable cause, SA22, 40, 43, do not equally warrant suppression. Surely the prior and *truthfully informed*

independent authorization of a judge was at least as important to Congress in limiting the use of wiretaps as the Executive Branch's internal review process.

### *2. The Government's Disregard of those Statutory Preconditions Mandates Suppression*

The government's wiretap application was a virtually wholesale abandonment of its duty to provide a truthful, "full and complete statement" of both necessity and probable cause. With respect to necessity, the Kang affidavit intentionally omitted the "elephant in the room,"—the conventional investigation long underway and the extensive evidence it had successfully developed—which was "the most important part," the "sum and substance," "the nuts and bolts," and the "heart and soul" of the FBI's own investigation. SA2, SA36, SA40-43.[4]

That rendered almost all of the necessity allegations, including the most important conventional techniques like subpoenas, witness interviews, and review of records, outright false. SA41, 42. The government's allegation that it could not continue to use its confidential informant (Roomy Khan) was also belied by their undisputed continued use of her after the wiretap issued. JA118-25. With those

[4] In district court, the government attempted to distance itself from the SEC investigation for purposes of its necessity *disclosure* in the wiretap application, while simultaneously wrapping itself tightly in the SEC's investigation as the basis for its post-search, factually reinvented purported necessity *showing* that the FBI *cum* SEC had sufficiently exhausted conventional techniques. The government cannot have it both ways.

false allegations deleted, all that remained of the necessity showing was the government's "slapdash" physical surveillance, SA50 n.24, an allegation regarding toll records, and five cursory sentences about arrests and undercover agents, *see* JA102-12. Those few non-false allegations rendered the government's "boilerplate representation that 'alternative investigative techniques have been tried or appear unlikely to succeed if tried' *** just that—boilerplate." SA41.

That "intentional" disregard of Title III's necessity requirement, by itself, mandates suppression under *Giordano*.[5] To hold otherwise, is to write the prior judicial determination of necessity out of the statute. But this Court need not stop there because the government's violation of Title III did not stop there either. It also "misstated important information," served up a "literally false statement" about the credibility of the "key" informant, and intentionally distorted the content of consensual calls in the probable cause allegations, SA2, SA22, which equally deprived Judge Lynch of a full and complete *truthful* statement of the facts establishing probable cause.

In no case to Appellant's knowledge has a wiretap been sustained when the federal government engaged in such cascading recklessly false statements and

[5] A misrepresentation or omission "is intentional when the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth." *Awadallah*, 349 F.3d at 64.

misleading omissions in a single affidavit. The government's misconduct literally threw Congress's necessity requirement out the window, substituting a nearly "full and complete *omission*" instead. SA40. The necessity allegations were so unhinged from reality —swearing under oath that they do not know where records are when they had 4,000,000 at their fingertips unreviewed; swearing that they could not issue subpoenas that they had and were continuing to issue; swearing under oath that they could not interview or question individuals when they had 22 such interviews at hand and a full-day deposition of Appellant they had not even bothered to read "cover to cover," JA174A—"deprived Judge Lynch of the opportunity," SA40, to make "doubly sure" as Congress intended that the wiretap was genuinely needed, *Lilla*, 699 F.2d at 102.

The government likewise brushed off Congress's mandate to provide a "full and complete statement" of the facts and circumstances establishing probable cause, substituting in its place repeated misleading factual distortions and flatly untrue assertions about the criminal history and credibility of its key witness. By the end, the district court could say only that a "residue" of the affidavit scraped together the *constitutionally* required probable cause showing. SA16. That, however, will not suffice for Title III. Congress commanded a "full and complete statement," not a "residue"; the two are textually polar opposites. This Court must presume that when Congress said "full and complete," it meant just that and not the

bottom-scraping leftovers that the government selectively picks and chooses in retrospect from the ash heap of a materially false and misleading application. *Carr v. United States*, 130 S. Ct. 2229, 2241-2242 (2010) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."); *United States v. Martinez-Santos*, 184 F.3d 196, 204 (2d Cir. 1999).[6]

Indeed, in *Giordano*, the Supreme Court held that the government could not sustain the use of certain wiretaps by showing that the "remaining evidence submitted in the extension application was sufficient to support the extension order." 416 U.S. at 533. Whether constitutionally required or not, the Supreme Court explained, Title III commanded a more comprehensive disclosure, and the government's failure to comply required statutory suppression. *Id*. That Supreme Court holding governs here.

[6] On occasion, this Court has applied the "residue" standard to probable cause challenges under Title III, none of which involved the systemic and multi-layered violations of Title III that occurred here. *See United States v. Fermin*, 32 F.3d 674, 676-677 (2d Cir. 1994); *United States v. Ferguson*, 758 F.2d 843, 849 (2d Cir. 1985). The depth of the government's departure here is unique, and makes it impossible to apply such residue analysis consistently with statutory text or congressional purpose.

### *3. Title III Does Not Permit Post Hoc Factual Justification*

The district court tried to salvage the wiretaps by finding entirely new facts during the *Franks* hearing that it concluded could have established necessity had they been known at the time of the application, had they been truthfully conveyed by the government, and had they been persuasive to the authorizing judge. SA45-54. But that approach simply layered on *yet another* departure from yet another central Title III command: the requirement that the warrant authorization be made "on the basis of the facts submitted by the applicant" *before* the warrant issues. 18 U.S.C. § 2518(3).

That requirement of *prior* judicial authorization, which is rooted deeply in constitutional tradition, "directly and substantially implement[s] the congressional intention to limit the use of intercept procedures," and thus itself triggers Title III suppression. *Giordano*, 416 U.S. at 527. If *Giordano* means anything, it means that Title III is not ambivalent about whether the required statutory showing for a wiretap warrant is made beforehand or after the fact. Only prior review and only "on the basis of the facts submitted by the applicant," 18 U.S.C. § 2518(3) will suffice. Title III's "standards are to be construed strictly, because Congress knew that it was creating an investigative mechanism which potentially threatened the constitutional right to privacy, and it carefully wrote into the law the protective procedures for the issuance of warrants which the Supreme Court had declared in"

*Katz, supra*, and *Berger, supra*, to be "'constitutional precondition(s) of *** electronic surveillance.'" *United States v. Capra*, 501 F.2d 267, 276-277 (2d Cir. 1974).

Holding the government to the affidavit it submitted to the authorizing judge is the only viable mechanism for enforcing honesty and forthrightness in such important *ex parte* applications, so that courts can independently exercise the "full[y] and complete[ly]" informed judicial review that Congress so plainly intended, *see* 18 U.S.C. § 2518(1)(b)-(c). "[B]ypassing a neutral predetermination of the scope of a [wiretap] search," the Supreme Court has stressed, would "leave[] individuals secure from" privacy "violations only in the discretion of the police." *Katz*, 389 U.S. at 358, 359.

To be sure, Title III's "full and complete statement" requirements undoubtedly permit the inadvertent misstatement of facts that have no material bearing on necessity or probable cause. But at a bare minimum, Title III's requirements of "full and complete statement[s]" mandate truthfulness in allegations and the forthright inclusion of those facts and circumstances needed to make the affidavit's affirmative representations not misleading. Otherwise, the system of *ex parte* applications for wiretap authorizations simply cannot function, because courts cannot provide genuinely independent review of the statutory and

constitutional prerequisites to the search without that foundational level of governmental candor.

The district court invoked *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), *abrogated on other grounds by Groh v. Ramirez*, 540 U.S. 551 (2004), (holding government cannot rely on materials that were not originally incorporated within a warrant to repair its defects). But *Bianco* addressed not the ability to obtain a wiretap order in the first instance, but the parameters of an otherwise authorized wiretap's use (*i.e.*, whether a "roving intercept" order was justified). *Id.* at 1125. Extension of the *Franks* protections beyond the initial authorization into the terms of a warrant thus "enhance[d] the protection" provided, *id.* at 1226, so that the "*Franks* standard [wa]s consistent with the purposes of" the Title III exclusionary rule, *id*.

Not so here. While *Franks* equally requires suppression, *see* Section I.C, *infra*, any court-made rule that would sanction the unprecedentedly comprehensive, multi-leveled, and consequential abandonment of core Title III requirements that occurred in this case would "go[] against the grain of the[] [congressional] purposes," *Bianco*, 998 F.2d at 1126, and thus would not be proper statutory construction of the Title III suppression rule. Such a reading would also impermissibly construe the wiretap statute to create, rather than to avoid, a substantial question about the constitutionality of the wiretap process, and would

collapse the Title III and Fourth Amendment suppression remedies, which is forbidden by *Giordano* and *Amanuel*.

Instead, the only question for purposes of Title III suppression is whether the "nearly full and complete *omission*" of the necessity showing and the critical falsity and misstatements in the probable cause showing together were at least equally significant departures from congressional limitations as the omission of the specific internal Justice Department signatory that required suppression in *Giordano*. That question answers itself.

### C. The Fourth Amendment Mandates Suppression

The Fourth Amendment's answer to the government's multi-faceted abandonment of its constitutional duty to make a *truthful* showing of necessity and probable cause is suppression under *Franks v. Delaware*, 438 U.S. 154 (1978). The government's "reckless disregard for the truth" met *Franks*' and this Court's intentionality requirement. *Id*. at 155; *Awadallah*, 349 F.3d at 64. And the district court further found that the stream of falsehoods and misleading omissions was so comprehensive and so material to the affidavit that it made it "impossible" for the authorizing judge to make "a reasoned evaluation of the necessity of employing wiretaps," SA43.

The district court nevertheless held that suppression was not required because it found necessity based on entirely new factual allegations made by the

government at "the [*Franks*] hearing," SA53—facts that appear nowhere within the affidavit on which the warrant rested. That runs headlong into two bedrock constitutional principles: (1) "[A]ntecedent justification *** is central to the Fourth Amendment" and a "constitutional precondition" of electronic surveillance, *Katz*, 389 U.S. at 359; "post-surveillance judicial review" cannot suffice, *United States v. U.S. District Court*, 407 U.S. 297, 318 (1972); and (2) to enforce the constitutional command of *prior*, independent, and informed judicial review, the Fourth Amendment requires that, when affidavits are proven to be false and materially misleading, the search can only be sustained if the "remaining content" of the original affidavit, *Franks*, 438 U.S. at 156, establishes probable cause and necessity.

### *1. Prior Judicial Review Is Constitutionally Indispensable*

"Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights," and sits at the "very heart of the Fourth Amendment directive." *U.S. District Court*, 407 U.S. at 318, 316. "The bulwark of Fourth Amendment protection" thus is the constitutional command that "the magistrate *** must determine independently whether there is probable cause" "*before*" law enforcement may "embark[] upon a search." *Franks*, 438 U.S. at 164, 165 (emphasis added). It is, after all, "not asking too much that officers be

required to comply with th[at] basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded." *Berger*, 388 U.S. at 63

Wiretapping is an "extraordinary investigative device," *Giordano*, 416 U.S. at 527, by which the government covertly enters the home and perpetually searches, without notice, all conversations of both the target and the scores of innocent individuals on the calls for months on end. For that reason, both this Court and the Supreme Court have long recognized that the Constitution requires a "prior judicial judgment" not only of probable cause, *U.S. District Court*, 407 U.S. at 317, but also of the necessity of resort to a wiretap. *See United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986) (The "minimum constitutional standards governing the use of aural electronic surveillance" include the requirement that a court "must certify that there is no less intrusive means for obtaining the needed evidence."); *see also Dalia v. United States*, 441 U.S. 238, 250 (1979) (showing of "genuine need" required); *Berger*, 388 U.S. at 57, 60 (because of wiretapping's "inherent dangers," "special facts" "showing *** exigency" needed, and court must ensure that "no greater invasion of privacy was permitted than was necessary under the circumstances").[7]

[7] *Cf. Winston v. Lee*, 470 U.S. 753, 765-766 (1985) (State must demonstrate "compelling need" for surgical search).

The Constitution's "obvious assumption," moreover, is that the constitutionally mandated showing "will be a *truthful* showing" by the government. *Franks*, 438 U.S. at 164-165. Indeed, "[b]ecause it is the magistrate who must determine independently whether there is probable cause," it is "an unthinkable imposition" upon both the judge's "authority" and the Constitution's command of prior judicial authorization when "a warrant affidavit is revealed after the fact to contain a deliberately or reckless false statement," *id*. at 165, let alone the litany of recklessly false statements about the "heart and soul" of its investigation served up by the government here, SA43.

### *2. Only the "Remaining Content" of the Original Affidavit Can Sustain this Search*

The rule under *Franks* is settled. The wiretap warrant may be upheld if, and only if, after "the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content *in the warrant affidavit* to support" probable cause or necessity. *Franks*, 438 U.S. at 171-172 (emphasis added); *see Canfield*, 212 F.3d at 718 ("The ultimate inquiry is whether, after putting aside erroneous information and material omissions, there remains a residue of independent and lawful information sufficient to support" the warrant). The court thus "gauge[s] materiality by a process of subtraction." *Awadallah*, 349 F.3d at 65.

The district court's determination that there was a "nearly *** full and complete *omission*" of the necessity showing, which "deprived Judge Lynch of the

opportunity to assess" necessity—and, indeed, rendered it "impossible" to make the required finding—conclusively answers that materiality inquiry. SA40, 43.

And rightly so. Subtracting out the "several specific statements" rendered false or "misleading" by the government's "glaring omission," SA41, 36, leaves only the most skeletal and largely boilerplate allegations of necessity. The allegations that a grand jury could not be used because witnesses have not been identified (in fact, scores had been interviewed and 12 new ones had just been identified), that witnesses would not testify voluntarily (22 had, including Appellant), that subpoenas would not lead to critical information (a "mountain" of evidence had resulted), and that subpoenas would tipoff the subjects (regular use of subpoenas and demands had been employed without such consequence) must all be deleted. SA39, 41-42. So too must the court jettison the allegations about the inability to obtain trading records from securities clearing firms (which the government had successfully done and *continued* to do throughout the wiretap), SA42, JA126-41; the complete inability to continue using CS-1 (whom the government did continue to use, JA118-25); and the inutility of search warrants to obtain records and professed ignorance of the records' locations (more than 4 million records, including instant messages, found), SA41-42.

When "these allegations are excised," *United States v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005), all that is left is the description of the government's "slapdash"

physical surveillance, SA50 & n.24, a boilerplate allegation about toll records that must be discarded, JA107; *Lilla*, 699 F.2d at 104, and the inability to use arrests or undercover agents. JA111-12. That does not even come close to establishing necessity, let alone truthfully "inform[ing] the authorizing judicial officer of the nature and progress of the investigation," and truthfully explaining the purported "difficulties inherent in the use of normal law enforcement methods." *Concepcion*, 579 F.3d at 218; *see United States v. Blackmon*, 273 F.3d 1204, 1209-1210 (9th Cir. 2001) (suppressing fruits of wiretap because affidavit, purged of statements rendered misleading by omissions, no longer "explain[ed] the specific circumstances rendering normal investigative techniques ineffective in this case").

Nor does it "enlighten [the court] as to why this [insider trading] case presented problems different from any other [insider trading] case," *Lilla*, 699 F.2d at 104, in which conventional investigative techniques have been successfully used for decades, SA51. That showing is particularly critical because Congress carefully enumerated the crimes for which wiretaps were authorized, and in so doing, omitted securities fraud from that list. 18 U.S.C. § 2516. Nor is there any precedent for concluding that Congress intended to authorize wiretaps for a crime like insider trading, in which the critical elements have all been devised by agency regulations and judicial common law, rather than legislative direction.

Thus, because "the affidavit's remaining content is insufficient to establish [necessity], the search warrant must be voided." *Franks*, 438 U.S. at 156.

### *3. Facts First Alleged and Found at the* Franks *Hearing Cannot Sustain the Warrant*

Because the court had already determined that the false and misleading content of the affidavit precluded the constitutionally required prior judicial determination of necessity, SA43, the district court denied suppression only by erroneously casting aside this Court's "process of subtraction" rule for *Franks* cases, *Awadallah*, 349 F.3d at 65, and instead making different factual findings that were entirely unanchored in the warrant application and, instead, were based on the government's brand-new, post hoc, and never-before-alleged necessity arguments first aired before any judge in the *Franks* hearing.

That is fundamental constitutional error. *Franks* and circuit precedent mandate that the grounds for sustaining the search be within the four corners of the "warrant affidavit." 438 U.S. at 172; *see United States v. Ferguson*, 758 F.2d 843, 849 (2d Cir. 1985) (wiretap based on a false affidavit can only be sustained on the "residue of independent and lawful information" provided to the authorizing judge). But virtually all of the facts on which the district court relied in sustaining the wiretap appeared nowhere in the government's affidavit submitted to Judge Lynch:

- New Facts Relied On: In the interviews of "numerous Galleon employees, including Rajaratnam himself, *** none of the people the SEC interviewed admitted any insider trading." SA52-53. The conventional investigation was "confronted by 'stonewalling' by witnesses." *Id*.

  *Contrast* Affidavit ¶40: Discloses no witness interviews whatsoever; flatly denies the ability to even conduct them, much less asserts that witnesses have been "stonewalling," SA53, and asserts that "[i]nterviewing *** Rajaratnam *** is an investigative route that, in the judgment of the law enforcement agencies involved, is too risky." JA108-10.

- New Facts Relied On: "Many of the *** 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." SA49. "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." SA51.

  *Contrast* Affidavit ¶¶39, 43: "[I]t would jeopardize the investigation to request more detailed records from clearing firms"; "the locations where the TARGET SUBJECTS currently maintain records related to the scheme have not been fully identified, if at all"; does not disclose the SEC chronologies, the instant messages, or the four million other records on which the SEC chronologies were based; discloses no judgment that the (unmentioned) documents confirmed use of the telephone. JA108, 111.

- New Facts Relied On: "[T]he 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." SA49-50.

  *Contrast* Affidavit ¶¶39-40: Asserts inability to identify, not to confirm sources, because "[t]rading records *** cannot identify the sources of any material, nonpublic information," and witness interviews would make it "difficult, if not impossible, to identify the sources of the Inside Information"; does not disclose that the SEC investigation had identified

certain sources; makes no allegation that a wiretap was necessary to confirm those (unmentioned) sources. JA108-10.

- New Facts Relied On: Completing the government's review of the four million records successfully obtained by conventional methods would not have been "'cost-effective.'" SA52.

  *Contrast* Affidavit ¶¶39, 43: Asserts that "it would jeopardize the investigation to request more detailed records from clearing firms"; asserts that the locations of relevant records have not been identified; discloses only the review of "certain trading records," not the four million documents including far more than trading records; makes no allegation that further review of the unmentioned documents would not be cost-effective. JA108, 111.

- New Facts Relied On: The FBI had success in interviewing and flipping Roomy Khan, without "compromis[ing] the covert nature of the criminal investigation." SA53. But "reasons emerged *from the hearing* *** as to why it made sense to approach Khan but not" any of the "twelve other potential interviewees that the SEC had identified." *Id.* (emphasis added).

  - Khan was the only one that criminal authorities thought they had enough evidence on to risk an approach, due to her "prior conviction coupled with damaging [instant messages], call logs and trading records." SA53.

    *Contrast* Affidavit ¶¶15 n.4, 40, 43: Asserts that "CS-1 *** has not yet been charged with any crimes"; does not disclose the millions of instant messages and other records gathered by the SEC; does not disclose the twelve potential interviewees identified. JA76-77, 108-11.

  - "Khan's agreement to cooperate against Rajaratnam in 2002 made her a good candidate for cooperation in the present case." SA53.

    *Contrast* Affidavit ¶15 n.4: Asserts that "CS-1 has been cooperating with the FBI since approximately November 2007"; discloses no judgment that her unmentioned conviction and

> cooperation in 2002 made her a good candidate to "flip." SA 48, JA76-77.

In making those findings based on new factual evidence developed at the *Franks* hearing two-and-a-half years after the search, the district court noted that "it would have been far better for Judge Lynch to have been in a position to make that decision for himself." SA36. That is quite a constitutional understatement. It is not only "far better" for the warrant application to have permitted the authorizing judge to make those necessary fact findings, *id.*; that is the central command of the Fourth Amendment. Judge Lynch, of course, could not find facts never alleged to him.

The Supreme Court has already forbidden precisely what the district court held. In *U.S. District Court*, the government undertook wiretap surveillance without obtaining the constitutionally required warrant. 407 U.S. at 316-318. When the wiretapping was challenged, the Supreme Court rejected the argument that the absence of a properly approved warrant could be forgiven because the government *could have* made the necessary showing prior to the warrant's issuance: "It may well be that, in the instant case, the Government's surveillance of [the defendant's] conversations was a reasonable one *which readily would have gained prior judicial approval*." *Id*. at 317 (emphasis added). "But *** [t]he Fourth Amendment contemplates a prior judicial judgment." *Id*. "[P]ost-surveillance judicial review" will not suffice. *Id*. at 318.

This Court's law is the same. "[R]elated facts which were also known at the time of the application *** lie outside the scope of a proper *Franks* inquiry because the relevant question is whether the *remaining portions* of the affidavit give rise to probable cause." *Awadallah*, 349 F.3d at 70 n.22. That is why neither the district court nor the government were able to cite a single case from this Court or the Supreme Court upholding a search warrant—in the *Franks* context or otherwise—based on facts that were alleged for the first time in a post-search judicial hearing.

Other circuits agree. "[W]hat will sustain the warrant must already be within it." *Baldwin v. Placer Cnty.*, 418 F.3d 966, 971 (9th Cir. 2005) (*Franks* case). Accordingly, "[a]llowing the government to bolster the magistrate's probable cause determination through post-hoc filings does not satisfy the Fourth Amendment concerns addressed in *Franks*." *United States v. Harris*, 464 F.3d 733, 739 (7th Cir. 2006).

Consequently, because the remaining content of the affidavit, shorn of falsity and misleading misstatements, could not establish necessity, the Fourth Amendment mandates suppression.

#### *4. Compounding the False Statements with Materially Misleading Omissions Does Not Make the Government Better Off*

In a *Franks* case, false statements are virtually always married together with the materially misleading omission of the actual truth. This case was no exception:

the government compounded the falsity of its affidavit with "broad" and "glaring" misleading omissions of the extensive conventional techniques it was employing and the successes it had obtained. SA36, 41. The law is settled that, under *Franks*, those false statements must be erased, and the search rises or falls based on the "remaining content" of the original affidavit; the government may not inject new facts. *Franks*, 438 U.S. at 156; *Awadallah*, 349 F.3d at 70 n.22.

That rule does not change—the government cannot possibly be better off—because it doubly misbehaved and compounded its false representations with a long series of material omissions. Yet that is exactly what the district court held by sustaining the wiretap based on entirely new facts and information that were never provided to the authorizing judge and were entirely divorced from the affidavit submitted to Judge Lynch. The court reasoned that "the entire premise of the *Franks* approach is that the court must consider information that did not appear in the original affidavit." SA46. That mixes apples and oranges.

The government may introduce new evidence at a *Franks* hearing for the narrow, limited purpose of proving the government agent's (non-reckless or non-deliberate) state of mind. *See United States v. Finley*, 612 F.3d 998, 1003 n.7 (8th Cir. 2010) ("[E]valuating an affiant's state of mind requires us to view all of the evidence."). Likewise, proving that the affidavit's factual content was true is necessarily permitted.

But that is very different from the question presented here. Once those predicate facts (the requisite intentionality and the false or misleading character of the allegations) have been established, then the Fourth Amendment's command of informed *prior* judicial authorization forecloses the post hoc resuscitation of a warrant based on facts never presented to the authorizing judge. Indeed, that fundamental principle runs throughout the Fourth Amendment. When the government fails altogether to obtain a constitutionally required warrant, those searches are "unlawful notwithstanding facts unquestionably showing probable cause" that might be demonstrated at a suppression hearing. *Katz,* 389 U.S. at 357; *see U.S. District Court*, 407 U.S. at 317.

And *Franks* makes crystal clear that a warrant based on government falsehoods gets no second bite at the apple. *See Franks*, 438 U.S. at 156 (If "the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided."); *Awadallah*, 349 F.3d at 70 n.22 ("[R]elated facts lie outside the scope of a proper *Franks* inquiry.").

Likewise, the mistaken omission of information from an 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).

But if the *inadvertent* omission of needed facts cannot be cured by post hoc factual allegations, *Whiteley, supra*, then there is no legal or logical basis at all for affording the government's *deliberate or recklessly misleading* omissions more solicitude and better treatment. And there are multiple reasons for not doing so.

***First***, the district court's conclusion that its after-the-fact ability to "draw its inferences" is an adequate substitute for having those inferences "'drawn by a neutral magistrate'" before the search occurs, SA47 (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)), misapprehends the central "point of the Fourth Amendment," *Johnson*, 333 U.S. at 13. Quite simply, the Fourth Amendment is *not* indifferent to whether the government justifies such exceptionally intrusive searches in advance or after having been caught materially misleading the authorizing judge. Rather, interposing "prior judicial judgment" before "invasion of a citizen's private premises or conversation" sits at "the very heart of the Fourth Amendment directive." *U.S. District Court*, 407 U.S. at 316, 317.

***Second***, rewarding governmental misconduct would destroy the incentive for candor that is so vital to the proper functioning of the *ex parte* warrant authorization process. *See Franks*, 438 U.S. at 169 (the *ex parte* "hearing before the magistrate not always will suffice to discourage lawless or reckless misconduct"). The whole reason that *Franks* confines the government's defense to the "remaining content" of the *original* application is to avoid "denud[ing]" the

requirement of antecedent, independent judicial review "of all real meaning." *Id*. at 156, 168. But under the district court's rule, law enforcement would be "able to use deliberately falsified allegations to demonstrate probable cause, and, having misled the magistrate," would be "able to remain confident that the ploy was worthwhile," *id*. at 168, and entirely cost free. The government could rest assured knowing that, in the rare case where its falsehood is discovered, the government can later substitute in the record at "the [*Franks*] hearing" (SA53) for the original affidavit. All harm, no foul.

***Third***, post-search judicial review is constitutionally inadministrable. Upholding a warrant based on newly asserted facts and evidence not only bypasses the fundamental rule that information known but not conveyed to the authorizing judge is irrelevant. It also creates a substantial risk that the evaluation of a search will be influenced by the state of facts and 20/20 hindsight at the time review is undertaken, rather than confined to the state of facts known to the government at the time of the search, as the Constitution requires. *See Henry v. United States*, 361 U.S. 98, 103 (1959) ("It is *** necessary to determine whether at or before that time [of a search,] [the officers] had reasonable cause to believe that a crime had been committed."). Indeed, the Supreme Court has made clear that "[p]ost-surveillance judicial review," *U.S. District Court*, 407 U.S. at 318, is impermissible precisely because, in "bypass[ing] the safeguards provided by an objective

predetermination of probable cause, the procedure "substitutes instead the far less reliable procedure of an after-the-event justification for the arrest or search[.]" *Beck v. Ohio*, 379 U.S. 89, 96 (1964).

That is particularly true for necessity, because the relevant facts involved in assessing the progress of an investigation are rarely recorded in any non-privileged evidentiary form and, as a matter of human nature, can easily and even unconsciously be distorted by a retrospective desire to protect an arrest or conviction. In this case, for example, the district court simply assumed, without finding, that the government's factual allegations about the proven inadequacy of conventional techniques had actually been made by the government prior to the wiretap application's submission, rather than helped along by indictment-saving hindsight. *Cf. Bumper v. North Carolina*, 391 U.S. 543, 548 n.10 (1968) ("Any idea that a search can be justified by what it turns up was long ago rejected in our constitutional jurisprudence.").

### *5. A Proper Fourth Amendment and Title III Analysis Requires Suppression*

Instead of casting prior judicial review aside, the district court should have followed this Court's lead in *Awadallah*. The Court ruled that the *Franks* review process concerns itself exclusively with omissions that "are *designed to mislead*, or that are made in *reckless disregard of whether they would mislead*." 349 F.3d at 68. Accordingly, in assessing the materiality of omissions, this Court "excis[ed]

the information obtained in violation of the Fourth Amendment and emend[ed] *** four misleading statements." 349 F.3d at 69. Critically, in emending the misleading statements, the Court added in only the omitted exculpatory information that was needed to make the government's affirmative statements no longer misleading. *See id.* at 66, 69. At the same time, this Court refused the government's request to open the factual door further and entertain "related facts" that were not part of the original affidavit and that did not misleadingly distort the affidavit's content by their omission. *Id.* at 70 n.22.

The Seventh Circuit agrees. In language that flatly contradicts the district court's approach here, the court of appeals held that the district court's "consideration of new information omitted from the warrant affidavit should [be] limited to facts that did not support a finding of probable cause." *Harris*, 464 F.3d at 739. "Allowing the government to bolster the magistrate's probable cause determination through post-hoc filings does not satisfy the Fourth Amendment concerns addressed in *Franks*." *Id*.

As the Seventh Circuit recognized, an omission of information is only "misleading" if its absence would make the case for a warrant artificially appear stronger than it really is. By contrast, no court would sensibly conclude it was "misled" just because the government could have made its case even stronger. The rule against misleading is a rule against hiding the ball.

Accordingly, because the Constitution and Title III command that the probable cause and necessity analyses be confined to the allegations of the original affidavit, under *Franks* and *Adwallah*, courts are confined to "subtract[ing]" the false statements and "emending" only those facts needed to render the affidavit's remaining affirmative statements non-misleading, 349 F.3d at 65, 69. That is the only way to allow an assessment of probable cause and necessity that is untainted by governmental misconduct, while holding the government to the case it chose to bring to court, preventing misconduct being rewarded with a second bite at the apple, and preserving the integrity and centrality of prior independent judicial review.

***6. Neither Probable Cause Nor Necessity Was Established***

**a.** The 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 Appellant were the heart of its probable cause allegations.

***First***, the district court concluded that it would have been reasonable to credit Khan's allegations notwithstanding the government's "[p]articularly disturbing *** omission of highly relevant information" bearing on her credibility. SA25. But that overlooks that Khan was a convicted-felon informer, and therefore categorically "less reliable than an innocent bystander with no apparent motive to

falsify." *United States v. Gagnon*, 373 F.3d 230, 236 (2d Cir. 2004). Still worse, the government knew—but did not tell Judge Lynch—that, the last time Khan had been investigated for securities fraud, she worked a deal for herself by (unsuccessfully) trying to implicate Appellant. The district court's conclusion that Khan's status "as a known informant, not an anonymous tipper *** strengthen[ed] the case for believing her," SA26, thus got it exactly wrong, because Khan was not merely a "known informant." She was a known, unsuccessful informant with a prior felony fraud conviction "peculiarly probative" of her credibility, SA25, who was herself under investigation yet again for very serious felony charges, SA53.[8]

***Second***, the district court reasoned that it would be inappropriate to discount her allegations entirely because they were "corroborated." SA27. But that corroboration was the product of two phone calls for which the government reworded the conversations "and subtly changed [Appellant's] answer" in a way that did not win "high marks for candor." SA23, 24. For example, on the January 17 call, the affidavit reported that Khan had inquired whether Appellant got information on Xilinx "from someone at the company and RAJARATNAM said yes, somebody who knows." JA80-81. But what Appellant actually said was that

[8] By the third application, the government had given up altogether trying to pretend that Roomy Khan should be believed, and just quietly excised the word "reliable" from its affidavit. *See* Def. Mot. to Suppress (DCT Docket No. 86) at 26 n.12 & Ex.A.33. Khan was not called to testify at trial.

he had received the information from "someone who knows his stuff." SA24. And on the January 14 call, the government had falsely rephrased Appellant's discussion of Intel in order to make it sound more inculpatory. SA23-24.

In short, the court found that the government's editing of those conversations had selectively deleted precisely those words and phrases that mark the line between legitimate research and analysis and illegal insider trading. Maybe with the government's candor-challenged "paraphrase" of the two phone calls included, the statements that Appellant knew someone at Broadcom and needed to call individuals at Xilinx could sustain probable cause. But without either of those falsely inculpatory summaries, and without the inculpatory glue of Khan's claim of a conscious criminal conspiracy with Appellant, the affidavit's remaining allegations reflect nothing more than a professional investment manager and stock analyst engaged in the legitimate, legal, and "commonplace" business of "'ferret[ing] out and analyz[ing] information,'" including by "meeting with and questioning corporate officers and others who are insiders." *Dirks*, 463 U.S. at 658-59.

That leap from evidence of innocent behavior to an inference of illegal conduct based on nothing more than a credibility-impaired confidential witness is insufficient to support probable cause. *See United States v. Falso*, 544 F.3d 110, 121 (2d Cir. 2008). Quite the opposite, the fact that the government felt the need to

selectively and self-servingly alter the true content of Appellant's statements in order to make them sound incriminating simply confesses their own lack of faith in the truthful evidence.

***Third***, the district court found support for Judge Lynch's probable cause determination in wiretap intercepts obtained over telephones belonging to Craig Drimal and Zvi Goffer. As the court put it, those intercepts "appear[ed] to indicate that Goffer and Drimal knowingly obtained inside information and passed it on to others, including Rajaratnam." SA29. But, as the Court itself acknowledged, Drimal and Goffer worked in Galleon's offices, and there was nothing in the government's application or in the wiretap intercepts themselves to indicate that Appellant *knew* this information was coming from insiders, if indeed it was. *Id*.[9]

**b.** The court's effort to make a silk purse out of the sow's-ear of post hoc necessity allegations fares no better. If necessity means anything under Title III and the Constitution, it means the government must do more than simply assert that a wiretap is more efficient than (i) actually reading the target's deposition "cover to cover"; (ii) taking the time "themselves [to] review the SEC's investigative file" and the "mountain" of documentary evidence and witness interviews at hand, which investigators had not done; (iii) undertaking independent

[9] Appellant was never charged with illegal trading or conspiracy in any of the securities discussed in those intercepted conversations.

investigatory efforts beyond being "spoon-fed" by the SEC; and (iv) continuing the use of subpoenas that the government itself considered so fruitful it kept issuing them throughout the wiretap period. JA174A, SA40, SA42 n.23, SA48.[10] Indeed, the district court found it "likely true *** that the government could have developed more evidence by conventional means"; that those efforts would have resulted in the "indictment of at least some alleged co-conspirators"; and that "attempting to interview or seek the cooperation of other witnesses was a conventional technique that would, in fact, be likely to succeed." SA51, 53. Furthermore, "[i]t is clear that conventional techniques have at least proven adequate in the past," SA51, and none of the government's explanations showed how this insider trading case "present[s] problems different from any other" insider trading case, *Lilla*, 699 F.2d at 104.

Tellingly, this Court has considered necessity an "exceptionally close" question when the government had available at most "two limited avenues of investigation other than the wiretap" and the government had (barely) explained why those methods failed. *Concepcion*, 579 F.3d at 219. The government had far

[10] Certainly the government could not have determined *at that time* that materials it had not bothered to examine with care could not support further conventional, roll-up-the-sleeves investigative effort by the FBI, especially given that at that point the criminal authorities had undertaken only the most minimal independent investigative effort. SA39-40.

more here, and relying on the efficiency of resorting to a wiretap when other options remained available was straightforward legal error under *Concepcion*. Even if "it would be in some sense more efficient to wiretap," Title III represents "a congressional judgment that the cost of such efficiency in terms of privacy interests is too high." *Lilla*, 699 F.2d at 105 n.7. The court's findings thus signal not necessity, but precisely the type of judicial judgment call that the Constitution and Title III insist be made *before* a warrant issues to avoid strained post hoc justifications.

***7. Suppression Requires Reversal***

Finally, suppression based on the invalidity of the original wiretap would require reversal of Appellant's conviction on all counts. The initial affidavit's legality was "crucial" because, "if its deficiencies justify suppression, they justify suppression of all the wiretap intercepts." SA16 & n.11. The government has never argued otherwise. Nor could it. All of the subsequent wiretap applications repeated the false and misleading information of the original affidavit and supplemented it only with the content of the wiretap recordings. Accordingly, all of the wiretap information would be the illegitimate fruits of the original flawed application.

Additionally, the government has acknowledged that the wiretaps were the "core evidence in its case" for "all the crimes" charged, JA394, 397, both as direct evidence and as the source of extensive documentary and witness testimony.

## II. THE PREJUDICIALLY ERRONEOUS JURY INSTRUCTION REQUIRES REVERSAL OF COUNTS 6-14

### A. Standard Of Review

This Court reviews the district court's jury instructions de novo. *United States v. Masotto*, 73 F.3d 1233, 1238 (2d Cir. 1996). "A jury instruction is erroneous if it misleads the jury as to the correct legal standard or does not adequately inform the jury on the law," and it "requires a new trial unless the error is harmless." *Id*. An instruction that would permit the jury to convict without finding an essential element of the charged offense must be reversed unless a properly instructed jury "would have necessarily returned a verdict of guilty." *United States v. Ferguson*, --- F.3d ----, 2011 WL 6351862, at *10 (2d Cir. Dec. 19, 2011).

### B. The "Factor However Small" Instruction Eliminated The Statutory Causation Element

Congress has criminally proscribed the "use" or "employ[ment]" of a "manipulative or deceptive device" "in connection with the purchase or sale" of a registered security. 15 U.S.C. § 78j(b). Because the "manipulative or deceptive device" alleged in this case was insider trading, 17 C.F.R. § 240.10b-5, the

government had to prove that Appellant traded "*on the basis of* material, nonpublic information" to establish the prohibited use or employment of inside information. *United States v. O'Hagan*, 521 U.S. 642, 650, 651-652 (1997) (emphasis added).

The jury instruction omitted that critical causal element. Over Appellant's objection, JA389B, the court instructed the jury that it could find the "use" element if "the material nonpublic information given to the defendant was *a factor, however small*, in the defendant's decision to purchase or sell stock." JA432-33.

Appellant acknowledges that the "factor however small" instruction was similar to Second Circuit precedent. *See, e.g., United States v. Royer*, 549 F.3d 886, 899 n.12 (2d Cir. 2008) ("in some way informed"); *United States v. Teicher*, 987 F.2d 112, 119-121 (2d Cir. 1993) ("knowing possession") (dicta). Intervening Supreme Court precedent, however, warrants a reversal of course.

Last year, in *CSX Transportation, Inc. v. McBride*, 131 S. Ct. 2630 (2011), the Supreme Court narrowly upheld a jury instruction in a civil case that imposed liability under the Federal Employers' Liability Act (FELA) as long as "[the Defendant's] negligence played a part – *no matter how small* – in bringing about the [plaintiff's] injury." *Id.* at 2636 (emphasis added). The Court explained, however, that such an unusually diluted causation standard was permitted because the statutory text imposed liability for injuries "'resulting in whole or part from [the defendant's] negligence,'" *id.* at 2634 (quoting 45 U.S.C. § 51), and thus the

statutory causation element was "as broad as could be framed," *id*. at 2636. In so holding, the Court specifically distinguished the "securities fraud statutes," explaining that "traditional notions of proximate causation" apply in securities fraud cases because the statutory text does "no[t] assign liability in language akin to FELA's[.]" *Id*. at 2644 n.14.

Because that distinction between FELA's text and the text of, *inter alia*, the securities fraud statute where proximate causation controls was "necessary to [the Court's] conclusion," *Capital Currency Exch., N.V. v. National Westminster Bank PLC*, 155 F.3d 603, 608 (2d Cir. 1998), it constitutes the type of intervening Supreme Court precedent that "casts doubt on our controlling precedent" and permits departure from it, *Wojchowski v. Daines*, 498 F.3d 99, 105 (2d Cir. 2007). *See Seminole Tribe v. Florida*, 517 U.S. 44, 67 (1996) ("When an opinion issues for the Court, it is not only the result but also those portions of the opinion necessary to that result by which we are bound.").

This Court accordingly should reverse the convictions on counts 6-14 for failure to instruct on the actual or proximate causation element as required by *McBride, O'Hagan*, 521 U.S. at 652, the law of other circuits, *United States v. Anderson*, 533 F.3d 623, 630 (8th Cir. 2008); *SEC v. Lipson*, 278 F.3d 656, 660 (7th Cir. 2002) (information actually "influenced" trade); *SEC v. Adler*, 137 F.3d 1325, 1337 (11th Cir. 1998), and *United States v. Smith*, 155 F.3d 1051, 1066 (9th

Cir. 1998) ("significant factor"), and the rule of lenity, *see United States v. Banki*, 660 F.3d 665, 675 (2d Cir. 2011).

The error in this case, moreover, was prejudicial. The instruction permitted the jury to convict even though substantial evidence showed that Appellant had other legitimate bases, such as the extensive expert reports of Galleon analysts, for the same trade, *see*, *e.g.*, Tr. at 3910-4049; 4070-4266; 4273-4373; 4686-4751; 4763-4910, and where Appellant had implemented a preexisting trading position in the stock *before* receiving any inside information, as occurred with respect to numerous charged stocks (*e.g.*, Akamai (Counts 8, 9, and 10), JA367-71. Indeed, the "factor however small" instruction was especially prejudicial here because, as an investment professional, Appellant was "in the business of formulating opinions and insights—not obvious to the general investing public—concerning the attractiveness of particular securities." *See Exchange Act Release No. 17,480*, 21 S.E.C. Docket 1401, 1981 WL 36329, *6 (Jan. 22, 1981). And this Court and the Supreme Court have both cautioned against applying the prohibition on insider trading in a manner that "could have an inhibiting influence on the role of market analysts," *Dirks*, 463 U.S. at 658, by making analysts and investment advisers "act at their peril" whenever they "are attracted to a particular security on the over-the-counter market and seek to obtain further information about it," *SEC v. Monarch Fund*, 608 F.2d 938, 943 (2d Cir. 1979). In short, a "skilled analyst" like Appellant

"with knowledge of the company and the industry may piece seemingly inconsequential data together with public information into a mosaic which reveals material non-public information" that the analyst is free to exploit on behalf of his or her clients. *Elkind v. Liggett & Myers, Inc.*, 635 F.2d 156, 165 (2d Cir. 1980). Because the virtually non-causal "however small" jury instruction prevented the jury from crediting the multiple sources of information provided to Appellant and prevented them from distinguishing between trades caused by legal sources of information and those that were alleged to be the product of inside information, reversal is required.

* * * * *

Suppression is a hard decision that no court relishes making. But costlier still would be the enduring harm to the judicial system and individual privacy of letting stand the disregard of constitutionally mandated process and the disrespect for independent judicial review that occurred here. The harsh reality is that the government swore under oath to a federal judge paragraph after paragraph after paragraph of an affidavit that factually defied the on-the-ground truth of what it was doing and what it was not doing. It did that, moreover, in an *ex parte* proceeding where there was no adversarial check and where the court could not know what the government chose not to tell it. The government has never explained—because it cannot—how Judge Lynch could possibly have discharged

his statutory and constitutional duty to independently and genuinely assess the need for this wiretap on this affidavit. Quite simply, the government cut the judicial half of the warrant process out of the picture. And it did so unblinkingly.

This, the government has repeatedly announced, is their flagship case and the model for the investigative use of wiretaps to come. *See generally* Def. Mot. to Suppress (DCT Docket No. 86) Ex. A.40 (Oct. 16, 2009 press conference).

That is exactly the fear. "To ignore or gloss over [wiretap] restrictions, or view them as mere technicalities to be read in such a fashion as to render them nugatory," as the government would have this Court do, "is to place in peril our cherished personal liberties." *Marion*, 535 F.2d at 706. The practical reality is that today's low water mark commonly becomes tomorrow's starting point. Absent suppression, the government will know going forward that "the ploy was worthwhile" because the evidence was obtained and was not suppressed. *Franks*, 438 U.S. at 168. Imagine what the next wiretap application will look like.

## CONCLUSION

For the foregoing reasons, the judgment of conviction and sentence should be reversed.

Respectfully submitted,

/s/Patricia A. Millett

Samidh Guha
AKIN GUMP STRAUSS
HAUER & FELD LLP
One Bryant Park
New York, NY 10022

Patricia A. Millett
Terence J. Lynam
James E. Sherry
Hyland Hunt
AKIN GUMP STRAUSS
HAUER & FELD LLP
1333 New Hampshire Ave., NW
Washington, D.C. 20036

*Attorneys for Appellant*
*Raj Rajaratnam*

January 25, 2012

## CERTIFICATE OF COMPLIANCE

The foregoing brief is in 14-point Times New Roman proportional font and contains 13,886 words, and thus complies with the type-volume limitation set forth in Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure.

/s/Hyland Hunt
Hyland Hunt

January 25, 2012

# STATUTORY ADDENDUM

**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 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.

**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.

**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.