New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 245—NO. 21
TUESDAY, FEBRUARY 1, 2011

WHITE-COLLAR CRIME

Expert Analysis

Overview of Federal Wiretap Law In White-Collar Cases

By **Robert G. Morvillo**

And **Robert J. Anello**

In what has been referred to as a "tactical sea change in pursuit of financial malefactors,"[1] the federal government has begun to employ investigative techniques typically associated with organized crime and drug cases. To date, 23 arrests have been made in the Galleon Group case, described by the U.S. Attorney for the Southern District of New York, Preet Bharara, as the "largest hedge fund insider trading case ever charged, criminally" and "the first time that court-authorized wiretaps have been used to target significant insider trading on Wall Street."[2]

Although the Galleon Group case may be the first insider trading case to rely on wiretaps, it is not the first white-collar case to be premised in large part on the use of wiretaps and other undercover investigative techniques.[3] The recent cases involving hedge fund use of experts also appear to be premised, in part, on wiretapping. Lanny Breuer, Assistant Attorney General for the Criminal Division of the Department of Justice, has heralded a "new chapter" in white-collar criminal enforcement which includes the aggressive use of all such tools.[4] This article provides an overview of federal wiretap law and the defense issues that surface with its use.

Wiretap Law

The law governing the interception of wire, electronic, and oral communications was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is set forth in 18 U.S.C. §2510, et. seq. Where the federal government is investigating one of the predicate crimes specified in the statute,[5] it can apply for an electronic surveillance order if it can demonstrate probable cause to believe that a suspect is using a location or device to communicate about such crime.[6] The application must be made under oath and include a "full and complete statement" outlining the nature of the offense, the device or location that will be intercepted, the nature of the conversations, and the identity of the people to be intercepted.[7]

The application also must include a "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[8] This showing was included by Congress to ensure that wiretapping did not occur in situations where traditional investigative techniques would suffice. Accordingly, "an affidavit offered in support of a wiretap warrant must provide some basis for concluding that less intrusive investigative procedures are not feasible."[9]

Once granted, a wiretap order remains in effect for thirty days, but can be extended for additional periods, up to thirty days, upon an application that meets the same requirements as the original application.[10] Every order issued by a court must contain a provision that the wiretap be executed as soon as practicable and "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[11]

> As described by U.S. Attorney Bharara, the Galleon Group case is 'the first time that court-authorized wiretaps have been used to target significant insider trading on Wall Street.'

Application

Many of the requirements articulated in Title III have been litigated in the criminal cases arising out the Galleon Group investigation. Perhaps the most visible case is the one brought against Raj Rajaratnam, the founder of the hedge fund. The government intercepted Mr. Rajaratnam's telephone communications, pursuant to numerous court orders, for more than a year, before arresting and charging him with conspiracy and securities fraud in October 2009.

The defendant moved to suppress evidence gathered from the government's wiretaps arguing, among other things, that: 1) the government was not entitled to use wiretaps to investigate insider trading; and 2) the government affidavits supporting the wiretap applications failed to establish probable cause and failed to establish the necessity of the wiretaps due to the inadequacy of conventional investigative techniques.[12] A brief review of the decision on that motion by Southern District of New York Judge Richard J. Holwell demonstrates the hurdles defendants must clear when challenging wiretap applications.

Wiretaps in Insider Trading Cases. In *Rajaratnam*, the defendant argued that the wiretaps should not be admissible because securities fraud is not among the predicate criminal offenses for which the government is authorized to seek a wiretap order. Although evidence of a non-predicate offense discovered "incidentally" by the government in the course of executing a lawful wiretap order may be admissible, the defendant argued that the securities fraud investigation was the government's primary objective and to allow such activity would circumvent congressional intent in enacting Title III.

Judge Holwell disagreed with the defendant's assessment, noting that the wiretap applications submitted by the government clearly stated that the wiretaps were sought to investigate wire fraud and money laundering (both of which are predicate offenses under the statute) and securities fraud. The court found this to evidence the government's good faith in seeking the wiretap orders. Further, Judge Holwell rejected the notion that the government's reliance on the wire fraud statute to justify its application was a subterfuge, noting that "unlikely is the insider trading scheme that uses no interstate wires."[13]

Probable Cause and Necessity. The probable cause standard under Title III is the same as for a regular search warrant, requiring a "fair probability that evidence of a crime will be obtained through the use of electronic surveillance." A reviewing court must determine whether the court granting the wiretap application had a "substantial basis" for the probable cause determination.

The standard for reviewing the necessity of the wiretap is similar, requiring a determination as to whether the facts set forth were "minimally adequate" to support a finding that normal

ROBERT G. MORVILLO *and* ROBERT J. ANELLO *are partners at Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer.* GRETCHAN R. OHLIG, *an associate of the firm, assisted in the preparation of this article.*

investigative techniques have been tried and failed or reasonably appear to be unlikely to succeed if tried.

Where a defendant makes a preliminary showing that the government's affidavit in support of a wiretap application misstates or omits material information, the defendant may be entitled to an evidentiary hearing, called a *Franks* hearing. The wiretap evidence may be suppressed where the defendant demonstrates that: 1) the false statements and omissions were made knowingly and intentionally or with reckless disregard for the truth, and 2) the allegedly false statement or omission was material.[14] Mr. Rajaratnam sought a *Franks* hearing on both the probable cause and necessity issues with respect to the wiretap orders issued by Judge Gerard E. Lynch.

In reviewing Judge Lynch's probable cause determination, Judge Holwell found that although the government's wiretap applications did in fact contain certain misstatements and lacked a level of frankness that should be in all ex parte applications, the defendants were not entitled to a *Franks* hearing on the question of probable cause because the statements were not material. The government's affidavits omitted the criminal record of the government's cooperating witness and failed accurately to represent the substance of some of the telephone conversations. Despite these errors, the court found other indicia of the evidence's reliability. "Adding it all up, and correcting the affidavit to account for the government's misstatements and omissions, the Court believes that there were enough facts for [the district court] to have found probable cause."[15]

Judge Holwell felt differently with respect to the necessity issue, however, finding "good grounds" for a *Franks* hearing on whether that requirement had been satisfied given a "glaring omission" from the government's wiretap application. Specifically, the government failed to disclose to Judge Lynch that "the SEC had for several years been conducting an extensive investigation into the very same activity the wiretap was intended to expose using many of the same techniques the affidavit casually affirmed had been or were unlikely to be successful."[16] Although these tools may have proven inadequate in retrospect, Judge Holwell stated that he was "at a loss to understand" how the government could have believed Judge Lynch could make a determination regarding the wiretaps' necessity without this information.

Although the government "failed to disclose the heart and soul of its investigation, without which a reasoned evaluation of the necessity of employing wiretaps was impossible," Judge Holwell noted that a misleading affidavit alone is not grounds for suppression of the wiretap evidence. Rather, the defendant was required to establish that the omissions were deliberately made or made with a reckless disregard for the truth and that, after inserting the omitted information and setting aside any misstatements, the affidavit failed to establish necessity. In the court's opinion, Mr. Rajaratnam was able to demonstrate the former, but not the latter.

Minimization. Title III also requires that government agents make a "reasonable effort" to conduct wiretaps so as to minimize the interception of communications that are not related to the crime being investigated. Once the government makes a prima facie showing that it properly minimized intercepts, the burden shifts to a defendant to show that, despite good faith compliance, "a substantial number of non-pertinent conversations have been intercepted unreasonably."[17]

The government's obligation to minimize wiretap interceptions is a pending issue in another Galleon Group case, *United States v. Goffer*. Upholding the government's right to wiretap the five defendants charged with insider trading, Southern District of New York Judge Richard Sullivan nevertheless ordered the government to produce a written response to claims by one of the defendants that the government had intercepted more than 300 calls between the defendant and his wife and other family members. According to the defendant's lawyer, this represented a quarter of the call time captured by the wiretaps and demonstrated a "cavalier disregard for marital privacy" by the government. Judge Sullivan indicated that he would suppress some of the wiretap evidence if he found that the government failed appropriately to minimize the intercepts.[18]

Parallel Proceedings

Another issue highlighted by the *Rajaratnam* case is the availability of wiretap recordings produced in a criminal case in parallel civil proceedings. The SEC filed a civil complaint against Mr. Rajaratnam and others the same day criminal complaints were filed based on the same conduct. As part of criminal discovery, the United States Attorney's Office for the Southern District of New York produced to the defendants wiretap intercepts of more than 18,000 communications involving 550 separate individuals. The SEC sought access to the recordings through discovery requests in the civil case.[19]

Each year, the communications of approximately 200,000 individuals are intercepted through the approximately 2,000 wiretaps placed by law enforcement officials. If this technique produces probative evidence of wrongdoing, it can be anticipated that it will be used more frequently in the future.

Defendants refused to comply with the SEC's requests, arguing that disclosure was prohibited by Title III. Southern District of New York Judge Jed S. Rakoff, presiding over the civil proceedings, ordered production to the SEC of copies of all the wiretap recordings received from the government in the criminal case. On appeal, the U.S. Court of Appeals for the Second Circuit found that Title III did not prohibit the disclosure at issue and further stated that the "informational imbalance" would give the defendants an unfair advantage in the civil proceeding.

Nevertheless, the Second Circuit reversed Judge Rakoff's order, holding that the district court was unable to balance the SEC's right of access with the privacy interests at stake prior to a determination on the legality of the wiretaps. At that time, the defendants' suppression motions in the criminal case were still pending. Since Judge Holwell's denial of the suppression motions, the SEC has renewed its motion to compel the production of the wiretaps in the civil action.[20]

Conclusion

Each year, the communications of approximately 200,000 individuals are intercepted through the approximately 2,000 wiretaps placed by law enforcement officials.[21] The expanded application of these undercover techniques in white-collar investigations requires white-collar defense attorneys to become familiar with wiretap law and potential issues. If this technique produces probative evidence of wrongdoing, it can be anticipated that it will be used more frequently in the future.

1. Abigail Field, "Sorry, Judge Rakoff: You Can't Give the SEC the Galleon Wiretaps…Yet," DailyFinance.com (Sept. 30, 2010) (available at http://www.dailyfinance.com/story/investing/galleon-wiretaps-insider-trading-rakoff-overturned-sec-justice-trial/19655156/).
2. Prepared Remarks for U.S. Attorney Preet Bharara, "*United States v. Raj Rajaratnam, et al.*; *United States v. Danielle Chiesi, et al.*, Hedge Fund Insider Trading Takedown" (Oct. 16, 2009) (available at http://www.justice.gov/usao/nys/hedgefund/hedgefundinsidertradingremarks101609.pdf).
3. Undercover investigative techniques, including wiretaps, have been used in mortgage fraud and foreign bribery investigations. See, e.g., Holly A. Pierson, "Mortgage Fraud Boot Camp: Basic Training on Defending a Criminal Mortgage Fraud Case," NACDL Champion (September/October 2007); Department of Justice Press Release, "Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme" (Jan. 19, 2010).
4. Remarks by Assistant Attorney General Lanny A. Breuer at the American Bar Association National Institute on White Collar Crime (Feb. 25, 2010) (available at http://www.mainjustice.com/2010/02/25/breuer-tells-white-collar-bar-to-ease-up-on-prosecutors/).
5. 18 U.S.C. §2516.
6. Id. §2518.
7. Id. §2518(1)(b).
8. Id. §2518(1)(c).
9. *United States v. Lilla*, 669 F.2d 99, 103 (2d Cir. 1983).
10. 18 U.S.C. §2518(5).
11. Id.
12. *United States v. Rajaratnam*, 2010 WL 4867402, at 3 (S.D.N.Y. Nov. 24, 2010).
13. Id. at 4. Judge Holwell found that the fact that neither defendant was charged with either wire fraud or money laundering "does not imply it had no legitimate reason for the wiretap to begin with." Id. at 4, n. 5. Some have suggested that at the time the government initiated the investigation, it intended to rely on the honest services provision of the mail and wire fraud statutes to prosecute the defendant—an option that was no longer available after the Supreme Court's decision in *Skilling*. See Gail Shifman, "Wall Street Meets 'The Wire,'" White Collar Crime Prof Blog (Oct. 19, 2009).
14. 2010 WL 4867402, at 8 (internal citations omitted).
15. Id. at 13.
16. Id. at 15.
17. Id. at 27 (internal citations omitted).
18. See *United States v. Goffer*, 10-cr-0056 (Oral Order issued on Jan. 5, 2011); Larry Neumeister, "Judge Questions U.S. Use of Wiretaps on Husband-Wife Calls in Trading Case," NYLJ (Jan. 7, 2011).
19. *SEC v. Rajaratnam*, 622 F.3d 159 (2d Cir. 2010). The United States Attorney's Office took the position that it could not produce the wiretaps to the SEC without any law enforcement purpose. The Second Circuit declined to reach this issue.
20. *SEC v. Galleon Management, LP*, 09-cv-8811 (S.D.N.Y.).
21. Administrative Office of the U.S. Courts, "2009 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications" at p. 5.