"Tapping" into Wall Street

The Government Employs Tougher Tactics Against Money Crimes

By Mark B. Sheppard and Erin C. Dougherty

"There are more secrets, but there is no more secrecy."
—Steven Garfinkel, US Information Security Oversight Office

Confidential informants, undercover agents, and electronic surveillance—over the last few years, federal law enforcement officials have begun using tactics typically reserved for corruption and drug cases to combat white collar crimes including health care fraud, unlawful kickbacks, bank fraud, aggravated identity theft, computer crimes, and violations of the Foreign Corrupt Practices Act. As recently noted by Lanny Breuer, assistant attorney general of the Department of Justice's Criminal Division, "[o]ut are the days of resting easy in the belief that only self-reporting or tipsters will bring criminality to light. In are the days of proactive and innovative white collar enforcement." (Remarks to ABA Nat'l Inst. on White Collar Crime (Feb. 25, 2010), http://tinyurl.com/7sgylsb).

Published in *Criminal Justice*, Volume 26, Number 4, Winter 2012.

Though Wall Street once appeared immune to these "blue collar" tactics, the recent Galleon Group cases—the first Wall Street insider trading investigation where wiretaps were used—exemplify the shift in white collar investigative tactics. (*See* Gail Shifman, *Wall Street Meets "The Wire,"* White Collar Crime Prof Blog (Oct. 19, 2009).) This "tactical sea change" in the manner of investigating financial malefactors has coincided with an enhanced focus on combating financial crime. (Abigail Field, *Sorry, Judge Rakoff: You Can't Give the SEC the Galleon Wiretaps . . . Yet*, Daily Fin. (Sept. 30, 2010), http://tinyurl.com/7k8peas.) In 2009, President Obama established the Financial Fraud Enforcement Task Force, which includes senior-level officials from more than 20 federal departments, agencies, and offices, and has as its express mandate the investigation and prosecution of significant financial crimes and other violations relating to the financial crisis. (*See What Is the Financial Fraud Enforcement Task Force?*, STOPFRAUD.gov, http://www.stopfraud.gov/about.html.) One only has to pick up the paper to see that this mandate is being taken seriously.

White collar practitioners must, therefore, be prepared to contend with an increase in both the investigation and prosecution of financial crime, as well as the accompanying enhanced use of wiretap evidence. It is critical to understand the foundations of wiretap authority, the arguments available to defense counsel, and the potential impact of this evidence on white collar prosecutions. This article includes a brief primer on Title III, followed by a review of the key arguments made in the Galleon Group cases—arguments that exemplify how the procedural and evidentiary requirements of Title III provide defense counsel with ample room for creative pretrial lawyering. Also discussed are the practical considerations that defense counsel will need to take into account—preindictment through trial—as we enter this new era. Indeed, as these tactics often provide the government with direct or circumstantial evidence of a client's mens rea—the element that typically provides counsel with the most fruitful grounds for strong negotiation, pretrial motions, and trial strategies—counsel may have to rethink their typical approaches to financial fraud cases.

MARK B. SHEPPARD *is a partner in the Litigation Department at the Philadelphia office of Montgomery, McCracken, Walker & Rhoads, LLP, where his practice focuses on white collar criminal defense, SEC enforcement, and complex commercial litigation. Contact him at msheppard@mmwr.com.* ERIN C. DOUGHERTY *is an associate in the Litigation Department at Montgomery McCracken and focuses her practice on government investigations and white collar criminal defense. Contact her at edougherty@mmwr.com.*

Wiretaps: A Primer

Preliminary Requirements. The legal requirements for the use of wiretaps stem primarily from Title III of the Omnibus Crime Control and Safe Streets Act of 1968, codified at 18 U.S.C. §§ 2510 *et seq.*, and the Fourth Amendment. In recognition of the highly intrusive nature of such surveillance, Congress has limited the use of intentional interception of oral, wire, and electronic communications "to certain major types of offenses and specific categories of crime," and also devised several conditions for authorization. (18 U.S.C. §§ 2510, 2516.) Before granting the government permission to utilize a wiretap, a neutral judicial authority must, as with a search warrant, determine that: (1) probable cause exists, and (2) the "search" is "reasonable"—that is, the degree of intrusion present in the form of a wiretap is warranted because of its necessity as a law enforcement tool. (*See* 18 U.S.C. § 2518(3) (probable cause requirement); Scott v. United States, 436 U.S. 128 (1978) (discussing reasonableness as it applies to wiretaps).)

Probable Cause. A Title III wiretap warrant is predicated on a finding of probable cause to believe that: (1) the individual has committed or is about to commit one of the offenses specified by Congress in 18 U.S.C. § 2516, (2) communications concerning that offense will be intercepted, and (3) the particular telephone or device being tapped is itself being used in connection with the commission of the offense. (*See* 18 U.S.C. § 2518(3).)

To permit fully informed analysis of this probable cause requirement by the authorizing court, Title III requires that law enforcement include in the wiretap application a full and complete statement of the facts and circumstances relied upon to establish probable cause as to the particular offense being investigated. In essence, though, "[t]he standard for probable cause applicable . . . is 'the same as the standard for a regular search warrant'" under the Fourth Amendment. (United States v. Diaz, 176 F.3d 52, 110 (2d Cir. 1999) (quoting United States v. Fury, 554 F.2d 522, 530 (2d Cir. 1977).) That is, "the issuing officer need only make a practical, common sense decision whether, given the 'totality of the circumstances' set forth in the affidavit requesting such warrant, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that evidence of a crime will be obtained through the use of electronic surveillance." (United States v. Funderburk, 492 F. Supp. 2d 223, 237 (W.D.N.Y. 2007).)

Reasonableness of the "Search"—Necessity. In addition to the factual predicate of probable cause, the district court judge must also determine "on the basis of the facts submitted by the applicant that . . . normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to

Published in *Criminal Justice*, Volume 26, Number 4, Winter 2012.

be too dangerous" to attempt. (*See* 18 U.S.C. § 2518(3)(c).) That is, the judge must find that the wiretap is *necessary* because alternative law enforcement methods have not or cannot succeed. (*See* United States v. Ippolito, 774 F.2d 1482, 1485 (9th Cir. 1985).) Only if necessity is present will the "search" be considered "reasonable" under the Fourth Amendment.

Although an investigative agency need not exhaust all possible investigative techniques before requesting a wiretap, it must demonstrate that "normal investigative techniques employing a normal amount of resources have failed to make the case within a reasonable period of time." (United States v. Spagnuolo, 549 F.2d 705, 710 (9th Cir. 1977).) Normal investigative techniques may include: search warrants, witness interviews, grand jury testimony, cooperating informants/witnesses, use of undercover agents, surveillance, trash and mail covers, pen registers, toll registers, etc. (*See* United States v. Castillo-Garcia, 117 F.3d 1179, 1187–99 (10th Cir. 1997).) Where ordinary investigative techniques have not yet been employed:

> the affiant must show that employment of such techniques "reasonably appear unlikely to succeed if tried or to be too dangerous." [However,] [b]oilerplate assertions that the standard is met based on an agent's knowledge and experience *will not suffice*. Instead, the affidavit must contain an "adequate factual history of the investigation and a description of the criminal enterprise sufficient to enable" the issuing court to determine on its own whether there is the requisite necessity for the use of a wiretap. The court's inquiry should be guided by common-sense and practical considerations.

(United States v. Ailemen, 986 F. Supp. 1228, 1231 (N.D. Cal. 1997) (citations omitted) (emphasis added).)

Minimization

After a wiretap application has been granted, there are additional procedural requirements with which the government must abide. For starters, Title III demands that eavesdropping on calls be minimized: "Every order [authorizing a wiretap] . . . shall contain a provision that the authorization to intercept shall . . . be conducted in such a way as to minimize the interception of communications not otherwise subject to interception . . . and must terminate upon the authorized objective, or in any event in thirty days." (18 U.S.C. § 2518(5).)

When faced with a minimization challenge, district courts will assess whether, under the totality of the circumstances, the agents' minimization efforts were reasonable. (United States v. Hull, 456 F.3d 133, 142 (3d Cir. 2006) (citing Scott v. United States, 436 U.S. 128, 140 (1978)).) "The mere *number* of intercepted, but non-pertinent, calls [will] not [be] dispositive." (*Id.* at 143.) Rather, the court will take into consideration, inter alia, the nature and scope of the criminal enterprise under investigation; "the information available to the agents at the time of interception"; and "the government's reasonable expectations as to the character of, and the parties to, the conversations." (*Scott*, 436 U.S. at 140–42.)

Sealing and Disclosure

As the Court of Appeals for the Second Circuit recently observed, "there is a distinct privacy right against the *disclosure* of wiretapped private communications that is separate and apart from the privacy right against the *interception* of such communications. . . . The tapes will have been listened to, and the privacy rights of the parties to the conversations will forever have been harmed by the very act of exposure." (SEC v. Rajaratnam, 622 F.3d 159, 169–70 (2d Cir. 2010).) In recognition of this right, Title III includes strict sealing requirements and delineates the specific circumstances when disclosure is allowed.

Under section 2518, it states that: "[i]mmediately upon the expiration of the period of the order . . . [the] recordings shall be made available to the judge issuing such order and sealed under his directions." (18 U.S.C. § 2518(8)(a).) This process should be reflected in the sealing orders and logs for the data. If this information reflects that immediate sealing did not occur, the government will be required to "provide a 'satisfactory explanation' for the delay in obtaining a seal." (United States v. McGuire, 307 F.3d 1192, 1202–03 (9th Cir. 2002).) Otherwise, the government "cannot use the intercepted communications against the surveilled individual . . . [at] trial." (*Id.*)

Title III also sets forth the specific circumstances under which disclosure and use of lawfully obtained wiretap evidence is permitted. Section 2517 states, inter alia:

> (1) Any investigative or law enforcement officer who . . . has obtained knowledge of the contents of any wire, oral, or electronic communication . . . may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.
>
> (2) Any investigative or law enforcement officer who . . . has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.
>
> (3) Any person who has received, by any means

> authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(18 U.S.C. § 2517; *see* 18 U.S.C. § 2510(7) (an "investigative or law enforcement officer" means "any officer of the United States . . . 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").)

Thus, disclosure of the information may be permitted under section 2517 where "appropriate to the proper performance of the official duties" of the investigative or law enforcement officer. (*See* United States v. Gerena, 869 F.2d 82, 84–86 (2d Cir. 1989); United States v. Ricco, 566 F.2d 433, 435 (2d Cir. 1977).) Disclosure during the course of federal grand jury or district court proceedings is also permitted. (18 U.S.C. § 2517(3); *but see* Fed. R. Crim. P. 6(e)(2)(B) (providing that certain persons, including government attorneys, "must not disclose a matter occurring before the grand jury," except as provided for under Rule 6(e)(3)).) However, the final arbiter of any third-party disclosures is the court, not the government. (*Gerena*, 869 F.2d at 86 ("we believe that the district court must assume responsibility for the balancing required" between the public's right of access and defendants' privacy interests).)

Franks Hearings and Exclusion

Title III does authorize persons whose communications have been unlawfully intercepted to seek suppression. (*See* 18 U.S.C. § 2518(10)(a).) Indeed, as the Supreme Court has recognized, Title III "require[s] suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." (United States v. Giordano, 416 U.S. 505, 527 (1974).) To date, the grounds for suppression have included: (1) facial insufficiency of the orders, (2) failure to demonstrate necessity, (3) false or misleading statements in the application, (4) minimization issues, and (5) sealing issues. (*See* Daniel E. Monnat and Anne L. Ethen, *A Primer on the Federal Wiretap Act and Its Fourth Amendment Framework*, J. Kan. Trial Law. Ass'n, Mar. 2004, at 14 n. 50–54 (collecting cases).)

Defendants challenging the issuance of an order authorizing a wiretap under Title III and the Fourth Amendment will typically do so through a three-step analytical process:

> First, they must prove that the affidavit on which the issuing judge relied contained misstatements or omissions. Second, they must prove that the misstatements or omissions were either intentional or the product of recklessness. Third, they must show that if the misstatements were deleted or corrected, and if the information that was omitted was added, a district court would conclude that the required showing[s] of [probable cause] and "necessity" for the wiretap had not been made.

(United States v. Ailemen, 986 F. Supp. 1228, 1243 (N. Cal. 1997), (internal citations omitted).)

Courts vary in their approach to this analytical process. Some require the defendant to make a preliminary showing that the government's affidavit misstated or omitted material information. The district court will then "hold a [*Franks*] hearing to determine if the misstatements or omissions were made intentionally or with reckless disregard, and if so, determine . . . whether, 'after setting aside the falsehoods, what remains of the warrant affidavit is insufficient to support a finding of probable cause' [or necessity]," warranting suppression of the fruits of the wiretap. (United States v. Rajaratnam, No. 09-CR-1184, 2010 WL 4867402, at *7 (S.D.N.Y. Nov. 24, 2010) (Holwell, J.).)

Other courts have set a higher bar for obtaining a *Franks* hearing, requiring the defendant to: (1) specifically state which portions of the affidavit are allegedly false or misleading due to omissions; (2) contend that the false statements or omissions were deliberately or recklessly made; (3) present a detailed offer of proof, including affidavits, to support the allegations; (4) challenge only the veracity of the affiant (and not an informant); and (5) show that the challenged statements are material to the court's finding of necessity or probable cause. (*See* United States v. Shryock, 342 F.3d 948, 977 (9th Cir. 2003) (necessity context).) This will require substantial, upfront effort on the part of defense counsel to gain a hearing and suppression of the wiretap evidence.

Galleon Wiretaps: Government Missteps and Defense Tactics

As a general matter, "courts are extraordinarily reluctant to suppress the fruits of a wiretap no matter how apparent the flaws in the application or how sloppy the government is in executing the surveillance." (J. Bradley Bennett, *White Collar Crime, Blue Collar Tactics: A Defense Law-*

yer's Perspective, 28 W. St. U. L. Rev. 65, 69 (2000).) While the bar for obtaining a *Franks* hearing and, ultimately, exclusion of wiretap evidence is extremely high, the aforementioned substantive and procedural requirements of Title III *do* provide a wealth of opportunity for creative, successful lawyering. (*See, e.g.*, United States v. Rice, 478 F.3d 704 (6th Cir. 2007); United States v. Novaton, 271 F.3d 968 (11th Cir. 2001); *Ailemen*, 986 F. Supp. at 1231.)

The court in the Galleon Group cases disagreed that the government was not entitled to use wiretaps to investigate insider trading.

The arguments raised by counsel for the indicted defendants proceeding to trial in the Galleon Group cases, though unsuccessful at the district court level, demonstrate the wide range of arguments that are available to white collar practitioners. The arguments raised by defense counsel included, inter alia:

- The government was not entitled to use wiretaps to investigate insider trading as it is not a crime specified by Congress in 18 U.S.C. § 2516;
- Excluding erroneous information and correcting material misstatements or omissions, the government's application and supporting affidavits failed to establish probable cause;
- The government's application and supporting affidavits did not establish the inadequacy of conventional investigative techniques and, therefore, the necessity of using wiretaps;
- The government failed to abide by the minimization requirement; and
- The government's "inadvertent" disclosure of the wiretap evidence to the SEC warranted suppression.

(Defendants' Joint Motion to Dismiss and Suppress, United States v. Goffer, 756 F. Supp. 2d 588 (S.D.N.Y. 2011) (No. 10-CR-0056); Defendant Raj Rajaratnam's Memorandum of Law in Support of His Motion to Suppress Evidence Derived from Wiretap Interceptions of His Cellular Telephone, United States v. Rajaratnam, No. 09-CR-1184 (S.D.N.Y. Oct. 16, 2009).)

Use of Title III to Investigate Financial Offenses

One of the initial arguments made by defendants in the Galleon Group cases was that the government was not entitled to use wiretaps to investigate insider trading as insider trading is not a crime specified by Congress in 18 U.S.C. § 2516. While the "bread-and-butter white-collar charges of mail and wire fraud" are delineated Title III offenses, financial and securities-related offenses are not. (*See, e.g.*, Bennett, *supra*, at 67.) Had Congress felt that wiretaps were necessary and appropriate for investigating these crimes, they could and would have explicitly included insider trading or other financial crimes under Title III.

The district court strongly disagreed with this argument, concluding that, while "[w]iretaps may only be authorized to investigate offenses specified in Section 2516," Title III "contains what is in some sense a plain-view exception" that allows for evidence of securities fraud to be collected. (*See Rajaratnam*, No. 09-CR-1184, 2010 WL 4867402, at *3.) More specifically, the court found that where a law enforcement officer had in good faith obtained the wiretap to collect evidence of an offense or offenses for which Title III permits wiretapping, such as wire fraud or mail fraud, he or she need not "ignore" evidence of a second, nondelineated crime, such as insider trading, and could "incidentally" obtain evidence thereof. The court observed that, to conclude otherwise would "bar the government from using wiretaps for wire fraud investigations whenever the fraud concerns securities" or another nondelineated crime—a "carve-out Congress has not made and th[e] Court [felt it was] not permitted to make in [Congress's] stead." (*Id.* at *6.) Here, there was no subterfuge; the government made it clear in its Title III application that it would be searching for evidence of wire fraud and would find evidence of a second offense—securities fraud—not set forth under Title III. Under such circumstances, it was appropriate for the reviewing judge to grant a wiretap warrant. (*Id.* at *4–6.)

It should be noted that district courts have long held the view that, in the context of electronic surveillance, the government is not limited to investigating the crime or crimes delineated in the wiretap application. "The statute, as well as the 'plain view doctrine,' give[] the government more than enough leeway to use the evidence amassed in an electronic surveillance in support of *any* criminal charge, whether or not it is one for which Title III permits electronic surveillance." (Bennett, *supra*, at 67 (emphasis added).) Indeed, "it is increasingly unusual for the defendant to be charged with the violations set forth in the wiretap application." (*Id.*)

This "plain hear" exception, while certainly problematic, is not necessarily a death knell. In the Galleon

Published in *Criminal Justice*, Volume 26, Number 4, Winter 2012.

Group case the government made it clear that it would find evidence of both wire fraud and securities fraud—that, however, may not always be the case. Counsel should closely review the government's application and then use the discovery process to try to uncover any evidence that would allow an inference that the government engaged in an effort at subterfuge to circumvent the clear statutory requirements. Regardless of whether it seems particularly meritorious at the district court level, counsel should argue that the wiretap was not issued to investigate a crime specified by Congress in 18 U.S.C. § 2516 in order to preserve this issue for appeal.

Probable Cause and Necessity

Misstatements, Omissions, and the Rat. In his motion to suppress evidence derived from the wiretap interception of his cellular telephone, Raj Rajaratnam also argued that—excluding erroneous information, such as false summaries of conversations between Rajaratnam and a key confidential informant, Roomy Khan, and correcting material omissions, including facts relating to the criminal history, reliability, and ongoing criminal conduct of Khan—the government's application and supporting affidavits failed to establish probable cause. (*See* Defendant Rajaratnam's Memorandum of Law, *supra*.)

The district court agreed with Rajaratnam that the government had made "[p]articularly disturbing" omissions as to Khan's criminal history and had demonstrated a complete "lack of frankness" when summarizing at least two conversations between Khan and Rajaratnam. (*See Rajaratnam*, No. 09-CR-1184, 2010 WL 4867402, at *9–13.) And these omissions and misstatements did give the court serious "pause." (*Id.* at *11.)

However, the court concluded that probable cause had been established by the agent's affidavit. The court found that, even though she had a criminal history, the information provided by Khan did have some indicia of reliability. She was a known informant and there was evidence corroborating certain of her allegations. While the evidence was "far from conclusive of Rajaratnam's culpability," when you "[a]dd[ed] it all up, and correct[ed] the affidavit to account for the government's misstatements," there were still enough facts to meet the low bar that is the probable cause standard. (*Id.* at *12–13.)

Though unsuccessful, this line of argumentation demonstrates the potentially fruitful lines of argumentation that can stem from upfront preparation by counsel in arguing for suppression and a *Franks* hearing. (*See infra* (discussing techniques for obtaining a *Franks* hearing).)

Parallel Investigations That "Hit the Wall"

In addition to the errors regarding Kahn, Rajaratnam also pointed out that the government's application and supporting affidavits failed to so much as mention the government's nine-year investigation of Rajaratnam and Galleon. During this lengthy investigation, Galleon fully cooperated and had provided the government with four million pages of records and dozens of hours of sworn testimony, including a lengthy deposition of Rajaratnam himself. (*See Rajaratnam*, No. 09-CR-1184, 2010 WL 4867402, at *15–18.) Rajaratnam, therefore, argued that the government had not established the inadequacy of conventional investigative techniques or the necessity of using wiretaps.

The government received a slight backhand for recklessly failing to mention, or provide a description of, the SEC investigation. The district court observed that "the prosecutor's investigation was, in sum and substance, the SEC investigation" and the government's broad omission of that investigation from its application "rendered several specific statements in the affidavit misleading." (*Id.* at *17.) The court stated:

> For example, the affidavit blandly assures Judge Lynch that interviewing Rajaratnam and other targets is an "investigative route" that is "too risky at the present time." Yet during that same time period, the SEC . . . had interviewed or deposed . . . over twenty Galleon employees, including two interviews and a day-long deposition of Rajaratnam. [The SEC had met with the prosecutor before the Rajaratnam interrogations to discuss "strategy" and] [t]he results of these interrogations were promptly provided to the prosecutor.

(*Id.* (citation omitted).)

This information was "'clearly critical' to assessing the legality of employing a wiretap." (*Id.* at *19 (quoting United States v. Reilly, 76 F.3d 1271, 1280 (2d Cir. 1996)).) Though the government contended that the interview results were useless and "disclosure of a criminal as opposed to an SEC investigation [to Rajaratnam or others] would have been harmful," the court found that this was "the very decision a reviewing court, not the government, should be making." (*Id.* at *17.)

As corporations and individuals are often subject to parallel regulatory and criminal investigations, this is fertile ground for arguing that requisite "necessity" for a wiretap is lacking. However, where those parallel investigations are not progressing, counsel's arguments—as in *Rajaratnam*—may fall on deaf ears.

Indeed, despite its disapproval of the government's conduct, the district court concluded that the omission of the SEC investigation was immaterial. (*Id.* at *19–24.) The court observed that "[g]iven the advances made in [the SEC and FBI investigations] through the applica-

tion of conventional investigative procedures, it [wa]s surely incorrect to say that these investigative techniques had 'failed' in an abstract sense." (*Id.* at *21.) However, "'failure' in the Title III sense is not an abstract proposition." (*Id.*) Though the government had been able to compile "much circumstantial evidence of insider trading" through the documents obtained, this evidence also "confirmed what one would expect: insider trading is typically conducted verbally." (*Id.* at *22.) The interviews of Galleon employees had resulted in no admissions and none of these employees appeared that they—unlike Kahn—were the sort who could "be flipped." Thus, the government had "'hit a wall' of sorts." (*Id.* at *23.) The court concluded that where, as here, "an investigation develops strong circumstantial evidence of wrongdoing but then is confronted by 'stonewalling' by witnesses, the case for wiretapping is surely strengthened." (*Id.*)

Noncompliance with Minimization Requirement

In addition to the above arguments, one of the Galleon Group defendants, Craig Drimal, asked the district court for a blanket suppression of the first month of calls in light of the government's blatant and excessive violation of the minimization requirements. Drimal alleged that agents listened to and recorded some 180 calls between him and his wife—none of which provided agents with any incriminating evidence relating to the charges of the case and "many of which were of a profoundly personal nature." (*See* Defendant's Memorandum of Law in Further Support of Motion to Suppress, at 2, United States v. Goffer, 756 F. Supp. 2d 588 (S.D.N.Y. 2011) (No. 10-CR-0056).)

The district court, however, concluded that the government's isolated failures to minimize privileged spousal communications—while "disgraceful"—did not warrant suppression of all wiretapped conversations. (*See* Andrew Longstreth, *White-Collar Wiretaps Can Lead to Legal Challenges*, Reuters (Mar. 17, 2011), http://tinyurl.com/7uza89u.) The calls that were not appropriately minimized only constituted a small percentage of the more than 1,000 intercepted calls. Such "isolated violations [we]re insufficient to demonstrate the type of 'pervasive disregard of the minimization requirement' that would warrant total suppression." (United States v. Goffer, 756 F. Supp. 2d 588, 597 (S.D.N.Y. 2011) (quoting United States v. Pierce, 493 F. Supp. 2d 611, 636 (W.D.N.Y. 2006)).) The district court noted that blanket or widespread suppression was only an appropriate remedy "where the agents' minimization efforts *as a whole* were not objectively reasonable." (*Id.* at 595.)

This result is not unsurprising. Challenging a wiretap on minimization grounds is time intensive, fact-specific, and often—at least in the "blue collar" context—of limited benefit. Courts typically limit suppression to the specific interceptions where the minimization order was violated or simply suggest that defendants file a civil suit. A blanket suppression is a highly unlikely result, reserved for the most egregious, wide-spread violations. (*See, e.g.*, United States v. Cox, 462 F.2d 1293, 1302 (8th Cir. 1972) (noting that possible remedy for failure to minimize may be a civil suit under § 2520); United States v. LaGorga, 336 F. Supp. 190, 196 (W.D. Pa. 1971) (indicating that suppression of the specific interceptions determined to be unlawful—not a blanket suppression—is appropriate).)

While these egregious violations are rarely present in the blue collar context, they may be more prevalent in financial fraud cases. Conversations regarding illegal activity will typically be buried amidst legitimate business communications, providing grounds to argue that the government failed to appropriately minimize. Counsel should point to the government's listening to information protected under federal privacy laws, such as financial data (Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 15 U.S.C. §§ 6801 *et seq.*) or health care data (Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936), and to the large percentage of the intercepted calls that were not properly tailored.

Furthermore, because these legitimate conversations may include discussions of protected information, counsel may have grounds for arguing that issuing judges should, in financial fraud cases, supplement the typical minimization language on the wiretap warrant with stricter standards by which the prosecution and/or law enforcement agents must abide. Recent case law regarding the seizure of electronic evidence may provide interesting avenues for such novel minimization arguments. For example, in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009), the Court of Appeals for the Ninth Circuit imposed requirements designed to regulate the manner in which warrants for computer evidence are issued and executed in order to prevent "overreaching" and government review of data falling outside the scope of the warrant. Though the Ninth Circuit ultimately rejected making these procedures binding, *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (per curiam), the court still recognized that the following requirements could be "useful tool[s] for [magistrates in] the future":

1. Magistrates insisting that the government waives reliance upon the plain view doctrine in digital evidence cases.
2. Segregation and redaction must be doner either by specialized personnel or an independent third party.

If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

3. Warrants and subpoenas must disclose prior efforts to seize that information in other judicial fora.
4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
5. The government must destroy or, if the recipient may lawfully possess it, return nonresponsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

(*Id.* at 1180 (citations omitted); *see also* United States v. Kim, 677 F. Supp 2d 930 (S.D. Tex. 2009); People v. Gutierrez, 222 P.3d 925 (Colo. 2009).)

There are certainly grounds to argue that, under the Fourth Amendment, wiretap warrants should be executed under similar procedural requirements that would prevent officers from listening to extraneous conversations in which personal identifying information and/or financial data is shared.

Violation of the Sealing/Disclosure Requirements

Drimal and his codefendants, Emanuel Goffer, Zvi Goffer, Jason Goldfard, and Michael Kimelman, also argued that the wiretaps should be suppressed as a result of the government's "inadvertent" disclosure of the seized evidence to the SEC, which had been denied access thereto in the related civil proceedings. (*See* Defendants' Joint Motion to Dismiss and Suppress, at 65–73, United States v. Goffer, 756 F. Supp. 2d 588 (S.D.N.Y. 2011) (No. 10-CR-00056).) Counsel argued that these disclosures were a violation of the defendants' Fourth Amendment right to privacy, and were also a violation of Title III's sealing requirement. Unfortunately, these arguments were also rejected by the district court.

However, a wide-scale, deliberate disclosure—something all the more likely given the prevalence of parallel investigations—may warrant suppression for violation of Title III. While section 2517 does permit disclosure of wiretap information where "appropriate to the proper performance of the official duties" of the investigative or law enforcement officer, in the Galleon case the US Attorney's Office deemed disclosure to the SEC unwarranted under these provisions. Furthermore, as the *Goffer* defendants noted, "[c]ourts have interpreted this provision narrowly to permit limited and carefully-curtailed disclosures for law enforcement purposes." (*Id.* at 66–67 n.14 (citing United States v. Gerena, 869 F.2d 82, 84–86 (2d Cir. 1989), and United States v. Ricco, 566 F.2d 433, 435 (2d Cir. 1977)).) Thus, counsel will have strong arguments for suppression in the instance of unwarranted, large-scale disclosure to a regulatory agency and/or the civil division.

Practical Considerations

Mum's the Word. By the time an individual suspects that he or she is the target of a grand jury investigation and retains counsel, it is unlikely, though possible, that a wiretap is still being utilized. Regardless, at the very first attorney-client meeting, counsel should advise the client to refrain from speaking or corresponding about any matter or conduct believed to be the subject of the investigation—even with friends and colleagues. Even though, as a result of your representation, the prosecutor may not directly contact your client, the government may use cooperators and consensual recordings as wiretap-alternatives in order to gather additional evidence against your client. (*See, e.g.*, United States v. Brown, 595 F.3d 498 (3d Cir. 2010) (finding that prosecutors did not violate Model Rule 4.2, the "no contact rule"; their use of a confidential informant to communicate with a represented suspect during the course of a preindictment investigation was "precisely the type of contact exempted from the Rule as 'authorized by law'").) This "mum's the word" mantra is one that should frequently be repeated to clients throughout the course of the representation.

To Plea or Not to Plea. Once counsel has started to get up to speed on the facts and evidence, he or she will undoubtedly start contemplating and discussing with the client whether pleading is necessary and/or appropriate. Often, one of the key considerations in financial crimes cases is whether the government will be able to produce sufficient circumstantial evidence to establish a defendant's mental state. The ultimate resolution of the Galleon Group cases shows the power of wiretaps

Published in *Criminal Justice*, Volume 26, Number 4, Winter 2012.

to provide this necessary evidence. Indeed, "[j]urors reported that the wiretaps of Mr. Rajaratnam were the deciding factor in rendering their decision." (*See* Charles Mitchell, *Bugging the Boardroom: White Collar Prosecutions and Wiretapping*, Law Week Colo. (Aug. 1, 2011), http://tinyurl.com/7orpx6n.) Thus, counsel will have to include, amongst their laundry list of considerations, the possible presence of wiretap evidence when formulating their pre- and postindictment strategies.

Preindictment, there are several strategies that counsel could use to try to ascertain whether wiretaps were used, the number and scope of the intercepted conversations, and the content of these conversations. For starters, counsel can reach out to the prosecutor assigned to the matter, who may be willing to provide you with the general flavor of the tapes or even play/provide transcripts of particular tapes. (United States v. Martinez, 101 F.3d 684 (2d Cir. 1996) (holding that Title III authorizes government to play wiretap recordings to witness in course of investigation).) The prosecution's unwillingness to do so may itself give you reason to question the strength of the wiretap evidence and the government's case.

Another avenue to obtain this information may be through Title III's notice and/or civil damages provisions. Under 18 U.S.C. § 2518(8)(d), notice shall be given within 90 days of the termination or denial of a wiretap order to the individual(s) named in the surveillance order. It also gives the authorizing or denying judge discretion to: (1) require notice to any other individuals whose communications were intercepted under the order, and (2) allow individual(s) subjected to surveillance access to such portions of the intercepted communications as the interests of justice may require. Thus, your client may receive a Title III notice and, through a motion, could request and/or obtain access to portions of the intercepted communications. Alternatively, your client could bring a civil action for damages under 18 U.S.C. § 2520. Through the civil discovery process, various information regarding the wiretap(s) and the resultant evidence could be obtained. However, civil discovery is a two-way street and, as such, is a street that must be traveled cautiously when a criminal investigation is pending.

It should be noted that prosecutors seeking to postpone Title III notice may do so by making an ex parte showing of good cause to "a judge of competent jurisdiction." (18 U.S.C. § 2518(8)(d).) Thus, targets of an investigation may not receive notice. In the event that your client has not received notice but the employer and/or an individual with a common interest has, the company/individual may be able to request or obtain access and share information (pursuant to a common interest or joint defense agreement).

The information gathered through these means—as well as the client's ability to explain the content of the tapes and/or the likelihood for a successful suppression motion—may dictate how to proceed. Counsel for many of the targets of the government's Galleon Group investigation appeared to recognize the noose their clients' recorded conversations could be, and took their clients in to cooperate and cut a plea deal. Such a quick response may, however, not always be necessary or appropriate. Depending on the client's tolerance for risk—as well as counsel's relationship with the prosecutor and/or the flexibility of the prosecutor's office—defense counsel may want to consider waiting to see whether a suppression motion will be successful. If that motion is successful, it could greatly enhance counsel's likelihood of negotiating a favorable plea or successfully trying the case.

Preparing to Obtain a *Franks* Hearing. If the case is proceeding towards trial and counsel decides to seek a *Franks* hearing and suppression of the wiretap evidence, there are several steps that can be taken towards that end. As soon as possible, counsel should:

- Go to the clerk's office to obtain copies of the application and supporting affidavits, and the resultant warrant, on record;
- Assess what necessary documentation may have been missing from the government/agent's submission;
- Obtain any police reports regarding the warrant;
- Visit the facility housing the original tapes and examine the sealing orders and logs for the tapes; and
- Seek copies of the tapes and any corresponding transcripts.

Once this information has been obtained, counsel may:

- Along with the client, review the statements made in the application and affidavits and consider possible omissions;
- Attempt to determine the identity of any unnamed, confidential informants or cooperating witnesses;
- Investigate (or hire a private investigator to investigate) the veracity of particular statements; possible unknown omissions; and/or the background, character, and criminal history of any informants, witnesses, or other individuals named in the application or affidavits;
- Obtain copies of other applications/affidavits of agents or officers (which can be used to argue the use of "boilerplate" language and/or the failure to utilize certain investigative techniques they previously employed before obtaining a wiretap); and
- Review the tapes or transcripts to assess any failure to minimize.

With this information gathered, counsel can pull together their motion to suppress with a request for a *Franks* hearing. It may be worth discussing this draft, and the arguments contained therein, with your colleagues who: (1) do predominantly "blue collar" defense work, and/or (2) have filed Title III suppression motions before the district court judge handling the case.

Combating Wiretap Evidence at Trial

As the adage goes, you can cross-examine a witness, but you can't cross-examine a tape. Though this is an unfortunate reality, there are still tactics that counsel can use to handle wiretap evidence at trial.

Fight the Recordings Themselves. The transcripts and the recordings themselves will typically be wide open to interpretation. When engaging in everyday conversation with colleagues and professional associates, individuals rarely speak in a clear and precise manner. Furthermore, they may use financial jargon and, with individuals with whom they have long-standing relationships, inside references. Their conversations will vary as far as the types of statements and the form—from brainstorming and thinking out loud to well-formed comments and arguments, and from asking rhetorical questions to sharing jokes. When taken out of context, certain statements may sound incriminating, but taken in the context of the relationship of the parties and the type and form of the statements, it may be completely innocent.

Law enforcement agents and prosecutors viewing this evidence through a lens that may be clouded with preconceived notions of a client's character or industry misconduct may hear things that do not exist or misinterpret conversations. Defense counsel should work collaboratively with his or her client(s) to learn the identities of the parties involved in the calls, the context, and the meaning of each and every conversation. This effort will assist counsel in determining the actual value the call has in supporting the prosecution's case and will shape how the call is dealt with at trial, either by bringing in fact witnesses or experts to discuss and/or explain the tape, having the client testify, or simply not responding.

Find the Needle(s) in the Haystack. In the spring, we learned that, more than 17 months after Raj Rajaratnam had been arrested, federal prosecutors continued to use cooperating witnesses and wiretaps to investigate traders in the billionaire's orbit. (*See* Peter Lattman, *The Newest Wiretaps in the Galleon Investigation*, DealBook (Mar. 22, 2011), http://tinyurl.com/7p5elgo.) Adam Smith, a portfolio manager at Galleon, began cooperating with the government on January 14, 2011, and, at the FBI's direction, had three conversations with Ian Horowitz, Rajaratnam's personal trader at Galleon, attempting to get Horowitz to admit that he had been tipped off about a possible deal back in October 2009. This attempt ultimately failed, with Horowitz denying that he knew anything.

The risk the government had taken, however, became apparent when Rajaratnam sought to introduce the conversations as evidence that he—and his traders—did not have knowledge of any inside information when they executed trades. The government, however, argued that: "The fact that the government's effort to develop evidence against Horowitz—in the form of an undercover recording—did not work is entirely inadmissible. . . . Indeed, it is not at all surprising that the effort failed in light of Horowitz's knowledge of the highly public investigation. (*See* Government's Motion to Preclude Certain Evidence, United States v. Rajaratnam, No. 09-CR-1184 (S.D.N.Y. Oct. 16, 2009).) Thus, they argued that the recordings should not be admissible. The district court, however, disagreed and allowed at least one of the tapes to be played during defense counsel's cross-examination of Adam Smith.

This episode reveals one important fact: Not all tapes will be harmful; indeed, some may even be helpful. Like defense counsel, prosecutors and federal agencies dealing with financial crimes still have a steep learning curve to climb when it comes to certain "blue collar tactics." Slip-ups along the way may provide for unique arguments regarding probable cause, necessity, minimization, and sealing; at the same time, the resultant records may themselves provide useful content for defense counsel. White collar practitioners should keep this in mind as they and their clients review the tapes.

Conclusion

The expansion of the use of wiretaps to investigate and prosecute Wall Street bankers and traders—exemplified by the Galleon Group case—reflects a marked shift in the government's tolerance for white collar crime following the financial crisis. The defense bar must be prepared to address this emerging trend and the reality that, though "[t]here are more secrets . . . there is no more secrecy." ■

Published in *Criminal Justice*, Volume 26, Number 4, Winter 2012.