Bloomberg BNA

Criminal Law Reporter™

ELECTRONIC SURVEILLANCE

Attacking Insider Trading and Other White Collar Cases Built on Evidence From Government Wiretaps: The Nuts and Bolts



BY PAMELA JOHNSTON, JAIME GUERRERO AND ALEXANDER KRAMER

A bridge has been crossed: Federal prosecutors are using federal wiretaps to obtain evidence in white collar cases, specifically, in insider trading cases. Use of such an invasive law enforcement tool in a white collar case was virtually unheard of 10 years ago. But as times change, so do the methods of investigating white collar cases. Indeed, the U.S. Attorney for the Southern District of New York ventured out and has staked the reputation of the Department of Justice on the merits of such an approach. So far, this new approach to combating insider trading has yielded approximately 70 convictions since 2009,[1] with more likely to follow around the country as the technique grabs hold in California and elsewhere. The most famous, to date, has been the prosecution and conviction of the former CEO of the Galleon hedge fund, Raj Rajaratnam. Wiretaps, and the evidence gained from them, helped convict Rajaratnam and led to numerous guilty pleas from money managers, traders, consultants, lawyers, and others associated with the insider trading charges in his case.

Pamela L. Johnston and Jaime Guerrero are partners in Foley & Lardner LLP's Los Angeles office where they specialize in representing clients in white collar criminal and other government enforcement matters. Both were federal prosecutors in the U.S. Attorney's Office in Los Angeles. Guerrero handled many wiretap issues as a prosecutor. Johnston handled insider trading and other criminal securities cases as a prosecutor and does the same as a defense lawyer. Alexander Kramer, a senior associate at Foley & Lardner, specializes in white collar matters.

Listening to recorded conversations during a trial allows a jury to hear the actual words of the defendant, and such evidence can be quite damning and difficult to counter. Thus, when arrested or charged in a white collar case that rests on wiretap evidence, the defendant should give strong consideration to allocating significant defense resources to challenge the wiretaps before trial to obtain an order that suppresses the recorded evidence, as was tried in the Rajaratnam case. Indeed, the best, and sometimes only, chance a defendant may have to mitigate the situation is a well-founded attack on the wiretap evidence. Consequently, understanding the processes for obtaining wiretaps and, more important, attacking wiretaps are important tools for white collar attorneys to wield. This article focuses on the nuts and

[1] Michael Bobelian, *The Obscure Insider Trading Case That Started It All*, FORBES, Nov. 30, 2012, available at http://www.forbes.com/sites/michaelbobelian/2012/11/30/the-obscure-insider-trading-case-that-started-it-all/.

 ISSN 0011-1341

bolts of obtaining wiretaps and attacking wiretap evidence in white collar cases.

The Rajaratnam Appeal

Rajaratnam's conviction rested soundly on wiretap evidence. He is now appealing his conviction, arguing, in major part, that the wiretaps were obtained using false statements and omissions and that the resulting recorded conversations should have been suppressed.[2] A three-judge panel of the U.S. Court of Appeals for the Second Circuit in New York heard arguments regarding the wiretaps and suppression on Oct. 25. No decision has been handed down, and the case is pending.

Rajaratnam was the head of the Galleon Group, which operated a family of hedge funds. He was charged with leading multiple conspiracies from 2003 through 2009 to trade securities of 19 public companies based on material, nonpublic information. Rajaratnam was accused of obtaining nonpublic information from senior executives at IBM, McKinsey & Co., Intel Capital, and others.

In late 2006, the Securities and Exchange Commission began investigating Rajaratnam and the Galleon Group for insider trading. As part of this investigation, the SEC obtained access to millions of pages of documents, conducted multiple interviews, subpoenaed records, and took sworn testimony from Rajaratnam and others. As was later revealed, in March 2007 the SEC believed it had found limited evidence of insider trading and briefed the U.S. Attorney's Office for the Southern District of New York and the FBI about what the SEC had uncovered.[3]

A year later, on March 7, 2008, to obtain additional evidence, the government sought a warrant to place a wiretap on Rajaratnam's cellphone. In the wiretap application, the government used information provided to it from the SEC investigation as well as a cooperating informant. The wiretap application also stated that ''normal investigative techniques'' had been tried and either failed or reasonably appeared unlikely to succeed. This was the key representation made to the district court. Absent such a representation, the wiretap cannot be ordered.

The district court approved the wiretap application, and the government began intercepting wire communications over Rajaratnam's telephone line. The government sought and received permission to intercept such wire communications a total of eight times.[4] The government intercepted 2,200 calls.

After he was criminally charged, Rajaratnam moved to suppress the wiretaps using two arguments. First, he argued that the government made false statements and omissions in establishing probable cause for the warrants, specifically arguing that the government failed to state in its application that the cooperating informant had a prior felony conviction. Second, he argued that the government made false statements and omissions regarding the necessity for a wiretap, specifically arguing that the government omitted that the SEC had been conducting an investigation and that the government had access to the documents and information from that investigation.

The district court ordered a hearing on the issue and held that while the government recklessly made false statements and omissions when seeking approval of the wiretaps, they were not material and that necessity was shown after the fact during the hearing held before the district court. Therefore, the court did not suppress the wiretaps. Rajaratnam's appeal argues that the district court erred in this ruling.[5]

Title III Wiretaps: Nuts and Bolts

The applicable law that governs federal wiretaps is Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522. Title III permits district courts to authorize electronic surveillance by government officers in specified situations. Specifically, Title III authorizes the interception of wire communications if the crime under investigation is one of the enumerated offenses listed under 18 U.S.C. § 2516. Section 2516 lists numerous crimes and categories of crimes for which wiretaps may be authorized. This list has been expanded over time and includes crimes related to organized crime, narcotics, and other felonies such as mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), money laundering (18 U.S.C. §§ 1956 and 1957), obstruction of justice (18 U.S.C. § 1503), and bank fraud (18 U.S.C. § 1344). While the specific securities fraud offenses and foreign corruption offenses in Title 15 are not on the list of offenses under Section 2516, prosecutors can usually seek to characterize an insider trading case, a foreign corruption scheme, or other white collar scheme as a species of wire fraud to avoid this omission in the statute.[6] Further, Section 2517 allows use of properly obtained recorded communications to prosecute crimes not listed in Section 2516.[7] These provisions act to permit a very broad set of circumstances where wiretaps are permitted to be used. It should be expected that government authorities will increasingly look to use wiretaps in white collar investigations and prosecutions.

Title III sets forth specific criteria that must be included by the government in an application to obtain a warrant for a wiretap. This procedure is governed specifically by 18 U.S.C. § 2518(1), and the required factual elements are:

> (a) The identity of the law enforcement officer submitting 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, in particular:
>
> (i) details of the alleged offense specified in Section 2516;
>
> (ii) the nature and location of the facilities from which the communications are to be intercepted (i.e. the telephone number, the type of telephone, and its location);

[2] Brief for Defendant-Appellant at 18-20, *United States v. Rajaratnam*, No. 11-4416 (2d Cir. Jan. 25, 2012).

[3] Brief for the United States at 18-20, *United States v. Rajaratnam*, No. 11-4416 (2d Cir. Jan. 25, 2012).

[4] Id. at 20-22.

[5] Brief for Defendant-Appellant at 3, *United States v. Rajaratnam*, No. 11-4416 (2d Cir. Jan. 25, 2012).

[6] Section 2516.

[7] Section 2517.

  CRL ISSN 0011-1341

(iii) a particular description of the type of communications sought to be intercepted; and

(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 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 (this is the so-called ''necessity'' requirement at issue in the Rajaratnam appeal);

(d) a statement of the period of time for which the interception is required to be maintained;

(e) a full and complete statement of the facts concerning all previous applications involving any of the same people, facilities, or places; 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.

Thus, the applicant must state under oath to the district court that all other reasonable means to obtain evidence will be unlikely to succeed if tried, that wiretap evidence is necessary, that probable cause exists to believe that the person under investigation is currently committing or has committed the specific crime listed, and that the information about the person and the telephone to be tapped are not stale. In connection with such an application, a judge may require the applicant to provide additional information.[8]

After such an application is made, the district court may enter an order approving the wiretap if it determines on the basis of the facts submitted by the applicant that there is probable cause to believe (a) that an individual is committing, has committed, or is about to commit a particular offense covered by Title III; (b) that particular communications concerning the offense will be obtained through the wiretap; and (c) that the premises to be wiretapped were being used for criminal purposes or were about to be used or owned by the target of the wiretap.[9] Additionally, the district court *must* find that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[10] The intended purpose of this so-called ''necessity'' requirement is to ensure that wiretaps are not resorted to in situations where traditional investigative techniques would suffice.[11]

Judicial oversight of wiretaps is critical to enforcing the strict limitations placed on wiretapping by Title III. By their very nature, wiretaps involve an intrusion on privacy that is very broad in scope. Consequently, Title III demands close judicial oversight of wiretaps. But district judges can perform this role only if the government is forthright during the wiretap application process, particularly because the proceedings are in camera and ex parte. District judges are required to carefully scrutinize wiretap applications and their supporting documents to determine whether Title III's requirements are satisfied prior to approving a wiretap.[12]

With all that said, the practical reality is that even with the significant judicial oversight called for by Title III, wiretaps are overwhelmingly approved by federal judges on the basis of the representations made in wiretap applications. In fact, in 2010, only one out of 3,195 intercept applications was ultimately denied.[13] In 2011, only two out of 2,732 applications were ultimately denied.[14] Considering how damaging evidence from wiretaps can be, coupled with the frequency with which wiretaps are ultimately being approved, defendants must be prepared to take a serious look at challenging improperly obtained wiretaps and attempting to suppress any related evidence.

Attacking Wiretap Evidence In a White Collar Case

In addition to providing the procedures regarding obtaining wiretaps, Title III also provides a procedure for any aggrieved person to move to suppress the contents of a wiretap, or evidence obtained from a wiretap, where the wiretap was obtained in violation of the statute.[15] An aggrieved person is any person who was a party to any intercepted wire or a person against whom the interception was directed.[16] An aggrieved person may move to suppress unlawfully intercepted wire communications under both Title III and the Fourth Amendment.

For purposes of a criminal trial, a suppression motion must be made prior to trial unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion. If the government wishes to use the contents of a wiretap at trial or in any other proceeding, it must provide each party with a copy of the application and court order approving the wiretap at least 10 days before the proceeding.[17] Defendants must be careful to submit a motion to suppress in a timely manner.[18]

Title III specifically requires suppression of any wiretap, or any evidence derived therefrom, if the wiretap fails to satisfy the requirements set forth in Title III (as discussed in more detail above).[19] This includes where the wiretap application or approval fails to meet the ''necessity'' requirement. Failure to show that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried mandates suppression.[20] Further, Title III states that any aggrieved party may move to suppress a wiretap where: (1) the communication was unlawfully intercepted; (2) the order of authorization or approval under

[8] Section 2518.
[9] Id.
[10] Id.
[11] *United States v. Torres*, 901 F.2d 205, 231 (2d Cir. 1990).
[12] *United States v. Marion*, 535 F.2d 697, 703 (2d Cir. 1976).
[13] Administrative Office of the U.S. Courts, *2010 Wiretap Report* 7 (2011).
[14] Administrative Office of the U.S. Courts, *2011 Wiretap Report* 7 (2012).
[15] 18 U.S.C. § 2518(10).
[16] Section 2510(11).
[17] Section 2518(9).
[18] *United States v. Torres*, 908 F.2d 1417, 1424 (9th Cir. 1990).
[19] Section 2515.
[20] Id.; see also *United States v. Forrester*, 616 F.3d 929, 943 (9th Cir. 2010) (citing *United States v. Khan*, 415 U.S. 143, 153 n.12 (1974)).

which it was intercepted is insufficient on its face; or (3) the interception was not made in conformity with the order of authorization or approval.[21]

A motion to suppress may also be brought under the Fourth Amendment. Where a defendant challenges a wiretap on the ground that it contains false statements or omits information, the court applies the analysis set forth in *Franks v. Delaware*, 438 U.S. 154 (1978). In a *Franks* hearing, a wiretap obtained by relying on false statements or omissions in an application may be suppressed if a defendant can establish: (1) that the false statements and/or omissions were the product of a deliberate falsehood or reckless disregard for the truth and (2) that after setting aside the falsehoods and adding the omitted material, what remains of the application is insufficient to support the warrant.[22] If what is left no longer supports a finding of probable cause, the information garnered from the warrant should be suppressed. The district court's analysis in *Rajaratnam* will need to be examined carefully in light of this standard because the district court permitted evidence developed during the *Franks* hearing to be used to uphold the wiretap.

Using the *Franks* analysis as it pertains to the necessity requirement, a bifurcated standard of review applies. First, the court reviews whether a wiretap application is supported by a full and complete statement of the facts in compliance with Title III. If a wiretap is so supported, the court then reviews whether the wiretap, based on the supporting documentation, meets the necessity requirement.[23] An example of how this is applied comes from analyzing how the Ninth Circuit approaches reviewing the necessity requirement.

When reviewing the necessity requirement, the Ninth Circuit employs a common sense approach to evaluating the reasonableness of the government's good-faith efforts to use traditional investigative tactics or its decision to forgo such tactics based on the unlikelihood of their success or the probable risk of danger involved with their use.[24] Simply stating in a conclusory manner that traditional investigative techniques are unlikely to succeed is insufficient in the Ninth Circuit to establish necessity.[25] The government must provide *specific* information that explains, in reasonable, case-specific detail, why traditional investigative techniques will not suffice.[26] Failure to do so can result in suppression.

United States v. Gonzales Inc., 412 F.3d 1102 (9th Cir. 2005), provides an example of where evidence derived from a wiretap was suppressed. While it is not a white collar case, the court's analysis is still instructive. In *Gonzales*, the Ninth Circuit affirmed a district court order suppressing evidence from a wiretap because the wiretap application did not meet the necessity requirement. Specifically, the court held that normal investigative procedures had not been adequately utilized and that such procedures were reasonably likely to succeed.[27] The court found a lack of necessity because the investigation conducted prior to requesting the wiretap was very brief, lasting only five days, and attempted only very limited physical surveillance.[28] More was expected before a wiretap application could satisfy the necessity requirement.

Evidence obtained from a wiretap has also been suppressed where the information used in an application for a wiretap has become stale. This issue is particularly relevant to extensions for wiretaps. Title III requires that each extension of the time period for an initial wiretap be supported by independent probable cause.[29] Simply restating and rehashing information from earlier applications and wiretaps does not give rise to a sufficient level of probable cause for a wiretap to be approved.[30] Information regarding extensions of wiretaps must be fresh and take into account what has been learned from the prior wiretaps and other sources.

United States v. Williams, 2000 U.S. Dist. LEXIS 13172 (E.D. La. Sept. 5, 2000), provides an example of a situation where evidence was suppressed because an extension for a wiretap relied on stale information. In *Williams*, a drug case, the court held that the first two wiretaps were validly supported and necessary.[31] However, by the time the second and third extensions were being requested, facts had changed significantly but were largely not taken into consideration in the applications. For example, the defendant in the case had since been arrested and search warrants had been executed.[32] The court found that information came to light that should have led the government to return to normal investigative techniques.[33] Despite these developments, the applications for the wiretap extensions largely rehashed the earlier applications regarding the necessity for the wiretap and ignored these new facts. Consequently, the court held that the applications relied on stale information and failed to establish the continuation of the necessity requirement, and it suppressed the evidence from the wiretaps.[34]

Information regarding how wiretaps are obtained and the required components of a wiretap application and order are necessary to be able to attack a wiretap. Substantive errors and omissions in the application process provide defendants with an opportunity to defeat the warrant and prevent the recorded conversations from being heard by a jury.

Wiretaps in the White Collar Context

When the government's white collar case rests on wiretap evidence, it would be wise for a defendant to consider expending precious defense resources to analyze and potentially attack the wiretap application. In some of these situations, the wiretap was not necessary, and the government's application for it was not adequately supported in light of the caselaw. There is a

[21] Section 2518(10).
[22] See *United States v. Coreas*, 419 F.3d 151, 155 (quoting *Franks*, 438 at 171-72).
[23] *United States v. Forrester*, 616 F.3d 929, 934 (9th Cir. 2010).
[24] *United States v. Garcia-Villalba*, 585 F.3d 1223, 1228 (9th Cir. 2009).
[25] *United States v. Gonzales Inc.*, 412 F.3d 1102, 1115 (9th Cir. 2005).
[26] *Garcia-Villalba*, 585 F.3d at 1229-30.
[27] *Gonzales Inc.*, 412 F.3d at 1112-15.
[28] Id. at 1108.
[29] Section 2518(5); *United States v. Shipp*, 578 F. Supp. 980, 988 (S.D.N.Y. 1984).
[30] *United States v. Williams*, 2000 U.S. Dist. LEXIS 13172, at *10 (E.D. La. Sept. 5, 2000).
[31] Id. at *8-12.
[32] Id.
[33] Id.
[34] Id.

  CRL ISSN 0011-1341

reason white collar cases have not traditionally rested on wiretap evidence.

Wiretaps have never been more important in the white collar context. In a post-2008 financial crisis world, government prosecutors and investigators are opening up their arsenals and using every possible weapon they have in pursuing white collar cases. Investigative techniques such as undercover agents, confidential informants wearing hidden wires, and wiretaps are no longer being reserved for violent crimes. DOJ and U.S. Attorney's Offices have demonstrated they intend to use these tools as part of their white collar investigations.

As emphasized by the incredible amount of media attention it has received, the Rajaratnam case is one of the most prominent examples of this. But it is definitely not the only example. In the context of the Foreign Corrupt Practices Act, the SHOT Show investigation and ensuing trials saw the use of undercover agents, confidential informants, and consensually recorded meetings.[35] While wiretaps were not used in that case, DOJ officials have stated they continue to look to investigate FCPA violations and will use whatever tools they can to prosecute violators. It is widely speculated that wiretaps are already being used to investigate potential FCPA violations.

It is also likely that wiretaps are being used beyond New York to investigate additional insider trading cases and other white collar cases. While the Galleon-related cases marked the first widespread use of wiretaps in an insider trading case, prosecutors have sparingly used wiretaps in criminal investigations of mail and wire fraud conspiracies, bank fraud schemes, and healthcare fraud schemes in the past. The Rajaratnam case and others have put the world on notice that federal criminal prosecutors are expanding the use of these invasive tools to investigate insider trading and other types of sophisticated white collar cases. Defendants and their attorneys must be ready to confront these tactics and appropriately challenge the use of evidence they yield.

---

[35] Press release, Department of Justice, Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme (Jan. 19, 2010) (available at http://www.justice.gov/opa/pr/2010/January/10-crm-048.html).