ABA Section of Litigation 2012 Section Annual Conference April 18-20, 2012:
The Lessons of the Raj Rajaratnam Trial: Be Careful Who's Listening

The History and Law of Wiretapping

Howard J. Kaplan
Joseph A. Matteo
Richard Sillett
Arkin Kaplan Rice, LLP
New York, NY

The government's investigation of Raj Rajaratnam, Galleon's billionaire founder and manager, has been called the largest insider trading case in history. In one form or other, that investigation lasted more than a decade and consumed, at different times, the resources of the Securities and Exchange Commission, the U.S. Attorney's Office, and the Federal Bureau of Investigation. The government's efforts ultimately resulted in the filing of criminal charges against Rajaratnam, a two-month trial, twelve days of jury deliberations, and a jury verdict that convicted Mr. Rajaratnam on fourteen counts of conspiracy and securities fraud. Mr. Rajaratnam was sentenced to eleven years in prison, the longest sentence ever on charges of insider trading. Rajaratnam also forfeited $53 million in ill-gotten profits, and paid a $10 million fine. In addition, the SEC obtained a $92 million fine in its separate civil enforcement action against Mr. Rajaratnam. It is difficult to recall a larger or more notorious insider trading case, considering that Mr. Rajaratnam received tips of material non-public information from highly placed insiders at such reputable companies as McKinsey & Co., Intel Corporation, and IBM.

It has been widely publicized that the government's investigation featured the extensive use of wiretaps, evidence which led not only to Rajaratnam's conviction, but to criminal charges against more than twenty other people. The use of wiretap communications in criminal investigations is not a novel concept; Congress specifically authorized the use of wiretaps in 1934. Government investigators, however, have traditionally not resorted to wiretaps in white collar investigations. Indeed, prosecutors have traditionally used wiretaps to investigate drug trafficking, mob-related offenses like racketeering, and other so-called "blue-collar crimes." Eighty-six percent of the more than 2,000 federal wiretaps that were authorized between 1999 and 2009 were for crimes related to illegal drugs.[1] The leading justification for limiting wiretaps to those offenses is that the dangerous nature of those crimes necessitates extreme caution. But over the past few years, prosecutors have begun using wiretaps to investigate white-collar crimes that carry virtually no threat of violence, such as mail and bank fraud, mortgage fraud,[2] and even violations of U.S. copyright law in a case involving Chinese counterfeit sneakers.[3] Federal prosecutors have now added wiretaps to their arsenal of weapons for investigating insider trading.

From the government's perspective, wiretaps offer the ability to capture direct evidence of a suspect's intent to commit insider trading, which prosecutors and regulators traditionally had to prove circumstantially. This distinction is significant. Where prosecutors once had to persuade a jury to draw inferences of insider trading by comparing phone records with trading receipts, they could now play a recording of a suspect's own incriminating telephone conversation. The financial press and white-collar bar have heralded this innovation as a game-changer, with one commentator predicting that its effect will be "seismic."[4] Although these descriptions may seem overly dramatic, the government's use of wiretaps against employees of hedge funds, consulting firms, and other financial services companies has certainly captured the attention of those in the financial services industry.

The government has intimated that wiretaps in ordinary insider-trading investigations are here to stay. The lead prosecutor in the Rajaratnam case, U.S. Attorney Preet Bharara of the Southern District of New York, offered this warning to the financial services industry: "Today, tomorrow, next week, the week after, privileged Wall Street insiders who are considering breaking the law will have to ask themselves one important question: Is law enforcement listening?"[5]

But it remains unclear how significantly these new insider-trading wiretap cases have altered the legal landscape. Are wiretaps the "new normal" that employees at hedge funds, consulting companies, and other financial businesses must now worry about? Or is wiretapping unlikely to be repeated and even less likely to become standard practice in the government's investigation and prosecution of insider trading?

I. A BRIEF HISTORY OF WIRETAPPING

Wiretapping has existed for as long as oral communications have been transmitted over wires. After the invention of the telegraph in 1837 and the telephone in 1876, private detectives tapped wires for their clients, and businesses tapped each other's wires in a nineteenth-century version of corporate espionage. State legislatures soon recognized the intrusive nature of wiretapping, and legislation to prohibit the practice was adopted piecemeal and from state to state.

Whether wiretaps were constitutionally permissible, however, was a much larger question that remained dormant until the Prohibition Era. The National Prohibition Act, the enabling legislation for the Eighteenth Amendment, required a dramatic increase in federal law enforcement. Constitutional challenges to searches and seizures soon became common, owing to

law enforcement's frequent applications for search warrants as well as the high number of warrantless searches that occurred during the period. Curiously, despite the surge in crime during Prohibition, federal law enforcement generally disapproved of wiretaps to obtain evidence in criminal investigations, and the Justice Department actually banned the practice. Nevertheless, in one case, rogue federal law enforcement officers, operating in contravention of both Justice Department policy and state law, used wiretaps to obtain evidence against notorious Washington State bootlegger Roy Olmstead, who ran a large moonshine syndicate out of Seattle. The government's wiretap evidence led to Olmstead's arrest. At trial he moved to suppress that evidence on the grounds that the wiretaps violated the Fourth Amendment. The trial court rejected Olmstead's arguments and admitted the wiretap evidence.

Olmstead was convicted. In 1928, his appeal eventually reached the U.S. Supreme Court.[6] The Court, in a 5–4 decision, held that because the government had placed its wiretaps in the street by Olmstead's house, the government had not trespassed on Olmstead's property, and that the wiretaps were not therefore a "search" under the Fourth Amendment. This reasoning may seem overly formalistic and even bizarre to our contemporary sensibilities given that Olmstead's conviction was basically upheld on principles of Eighteenth-Century trespass law. Yet *Olmstead* reflects the contours of the Fourth Amendment when it was decided and its influence can still be felt today, as demonstrated by the Court's recent decision in *U.S. v. Jones*, where the Supreme Court heavily relied on *Olmstead* in holding that the government's warrantless use of a global positioning system to monitor a suspect's whereabouts violated the Fourth Amendment.

Nevertheless, *Olmstead's* relevance largely has diminished, principally because Congress has regulated the government's use of wiretaps by statute. In 1934, Congress passed the first federal wiretapping law (The Communications Act of 1934). This statute made wiretapping a federal criminal offense and made wiretap evidence inadmissible in court. For the next thirty-four years, wiretapping would remain an illegal, and somewhat stigmatized, investigative technique. But by the late-1960s, the situation had changed. The government was struggling to enforce laws against organized crime, drug trafficking, and other highly dangerous criminal activities, all of which resulted in a profound shift in attitudes toward the propriety of wiretaps. As the collective momentum moved toward reforming wiretap law, the Supreme Court decided another landmark case that would further curb, if not overrule, *Olmstead*: *Katz v. United States*.[7]

In *Katz*, police officers planted an eavesdropping device on a public payphone to record phone conversations of a suspect in an illegal gambling operation, whose conversations were then overheard, leading to his arrest and conviction. The listening device had been planted without a warrant, and the defendant challenged his conviction on the ground that the device violated his Fourth Amendment rights. In a 7–1 ruling (with one justice abstaining), the Court held that the device violated the Fourth Amendment since conversations are subject to Fourth Amendment protections, regardless of where they occur, as long as they are made with a "reasonable expectation of privacy."[8] Beginning with *Katz*, a physical trespass was no longer required to establish a Fourth Amendment search and seizure. As another Supreme Court decision expressed it, after *Katz*, the "capacity to claim the protection for the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place."[9] And although *Katz* is technically an eavesdropping and not a wiretapping case, it effectively replaces *Olmstead* as the Court's leading articulation of the permissible scope of wiretapping under the Constitution.

Another important Supreme Court case from the same term as *Katz* was *Berger v. New York*.[10] In *Berger*, the Court took the unusual step of reviewing a facial challenge to New York's newly adopted wiretapping law to determine its constitutionality. The Court invalidated the New York

statute as unconstitutional under the Fourth Amendment. In its opinion, the Court analyzed in detail which provisions of the statute it found to be too broad to pass Constitutional muster. In doing so, the Court was fully aware that Congress was in the process of drafting sweeping federal legislation to overhaul the laws relating to wiretapping. Congress therefore regarded *Katz* and *Berger* as instructive on how to draft a constitutionally sound wiretapping law and thereafter passed the Omnibus Crime Control Act of 1968. Title III of that Act addresses interception of communications and remains to this day the law that governs the federal use of wiretaps.[11]

Unlike constitutional challenges to warrantless searches, which frequently appear on the Supreme Court's docket, direct constitutional challenges to wiretaps have rarely been litigated since the passage of Title III. This is partly because Title III itself provides broader grounds for the suppression of improperly obtained wiretap evidence than the exclusionary rule, which is the usual remedy for excluding evidence when a search and seizure has been found to violate the Fourth Amendment.[12] When courts engage in an analysis concerning the propriety of a wiretap, their inquiry therefore is usually limited to the statutory language of Title III itself. Title III statute outlines in detail the steps that a federal prosecutor must take before obtaining a court order allowing the interception of communications (including electronic communications):

> (1) Each application for an order authorizing or approving the interception f a wire, oral, or electronic communication under this chapter [18 USCS §§ 2510 et seq.] 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.[13]

The United States Court of Appeals for the Second Circuit will soon address these requirements in Rajaratnam's appeal, which specifically challenges the lower Court's denial of his motion to suppress the government's wiretap evidence on the grounds that (1) the government was not authorized under Title III to use wiretaps for the investigation of insider trading, (2) the government obtained authorization to use wiretaps without probable cause, (3) the government's use of wiretaps were not necessary because other, less intrusive investigative techniques were available, and (4) the government failed to minimize the conversations it overheard.

II. THE USE OF WIRETAPS IN WHITE COLLAR INVESTIGATIONS

Recent advancements in technology have irrevocably altered how people communicate. Blackberrys, cell phones, and internet-based social media – all technologies that today seem commonplace – were nonexistent a generation ago. This revolution in communication has created a world of virtually instantaneous sharing of information through electronic means, and the ability to obtain information from a wide range of sources. At the same time, given the increasing use of electronic communications and cell phones, the government's opportunity to intercept communications has increased. Taking the Galleon case as an example, prosecutors tapped Rajaratnam's cell phone and subsequently obtained authorization to tap nine additional phones over sixteen months. Those efforts captured conversations among 550 individual callers and 18,150 separately recorded phone calls.[14] This evidence resulted in criminal charges against more than 20 suspects (including Rajaratnam).

The government has had several widely publicized successes in insider trading cases using evidence obtained by wiretaps. In addition to the Rajaratnam conviction, the government has obtained convictions of James Fleishman and Winifred Jiau of consulting company Primary Global Research. A wider probe of Primary Global Research led to twelve additional guilty pleas, including those of Samir Barai, the founder of hedge fund Barai Capital Management, and Noah Freeman, formerly a portfolio manager with SAC Capital Advisers. The government also obtained the convictions of brothers Zvi and Emanuel Goffer, who illegally profited from Zvi Goffer's role as a trader at the hedge fund Galleon Group. The government's current proceeding against Rajat Gupta also implicates wiretap evidence. In that case, the government is attempting to use wiretap evidence obtained in the Rajaratnam investigation to convict Gupta of securities fraud, even though there are no recordings of Gupta actually giving inside information to Rajaratnam.

The appeal of using wiretaps in white-collar investigations is obvious. White collar cases are frequently based on circumstantial evidence, and are critically dependent on inferences to be drawn regarding scienter (*i.e.*, a defendant's intent to violate the law). Having direct evidence of a defendant's receipt of confidential information and the defendant's intention to trade based on

such information is compelling. And the government has made clear that it intends to continue to seek this type of direct evidence in white collar cases. Assistant Attorney General Lanny A. Breuer of the Department of Justice has publicly commented that the government is increasingly relying on wiretaps in white-collar cases and that the number of wiretaps the Department of Justice has pursued "in all types of cases…has gone up."[15]

Given these statements and the recent publicity of these insider-trading wiretap cases, many financial industry employees now have the impression that the government's burden in using wiretaps in suspected insider trading cases is somehow easier than it used to be and that wiretaps will now be used more frequently in white collar investigations. However, the government's practical difficulties and legal limitations make obtaining wiretaps in insider trading cases anything but easy. Below we address several key issues relating to the use of wiretaps in white collar cases.

A. "Predicate Acts" Under The Wiretap Act.

Title III lists a limited number of specific predicate offenses which the government may investigate using wiretaps. These include mail fraud, wire fraud, kidnapping, and money laundering.[16] The Act has been amended over the years to include additional predicate offenses, including bank fraud and computer fraud.[17] Notably, however, the Act does not include securities fraud as a predicate offense. This is not to say, of course, that the government cannot use wiretap evidence in connection with an insider trading prosecution. The drafters of Title III anticipated that the government, when investigating a Title III predicate offense, may learn of crimes not listed under Title III, and provided what is in essence a plain-view exception allowing the government to present evidence of other crimes discovered while investigating an authorized offense. The court in Mr. Rajaratnam's criminal trial expressed the test in these terms: "The government must obtain wiretap warrants in good faith – that is, in connection with an offense for which Title III permits wiretapping – not as a subterfuge for gathering evidence of other offenses."[18]

In the Rajaratnam investigation, the government brought its original application for a wiretap before Judge Gerard Lynch of the Southern District of New York in 2007. Attached to the application was a 53-page sworn affidavit by an FBI special agent, which listed wire fraud and money laundering as the Title III predicate acts as to which the government sought wiretap evidence. Importantly, however, the application also indicated that the evidence obtained by the wiretap was likely to procure evidence of securities fraud, even though it was not a predicate offense under the Wiretap Act. In granting the application for a 30-day wiretap, Judge Lynch found that the government had provided sufficient probable cause that Rajaratnam had engaged in wire fraud and that a wiretap was necessary because standard investigative techniques were unlikely to uncover evidence of Rajaratnam's illegality. Over the next year and a half, the government would apply for the reauthorization of its original wiretap six more times.[19] The results of these wiretaps formed a significant portion of the evidence against Rajaratnam.

Prior to trial, Rajaratnam sought to suppress all of the government's wiretap evidence on the grounds that the government was not entitled to use wiretaps to investigate securities fraud because securities fraud is not listed as a predicate act under Title III. The court rejected Rajaratnam's argument and denied his motion to suppress because, among other reasons, the government candidly revealed in its application for a wiretap its intention to investigate insider trading. The court thus was satisfied that the government's actions were not a mere subterfuge to search for other crimes. That the government ultimately brought charges only for non-predicate offenses under Title III was of no consequence to the court. What it found significant was that

the government's investigation of *wire fraud* was made in good faith, a standard the court suggested is not difficult to meet, given the similarities between wire fraud and securities fraud. As the court itself acknowledged, "[U]nlikely is the insider trading scheme that uses no interstate wires."[20]

Importantly, the court cautioned that it was *not holding* that insider trading is a predicate offense for a wiretap. Rather, it narrowly held that where the government conducts a bona fide investigation of wire fraud and collects evidence of insider trading in the process, the evidence is admissible in a subsequent prosecution for insider trading.[21]

B. The "Necessity" Requirement.

Title III places a high burden on prosecutors before a court will authorize a wiretap, making this investigation technique something of a last resort for prosecutors, who must first demonstrate "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."[22] This is Title III's so-called "necessity" requirement under 18 USCS § 2518(1)(i). This showing requires a "full and complete statement" that wiretaps are necessary to further the government's investigation.

This requirement was also at issue in the Rajaratnam prosecution. Mr. Rajaratnam argued that the government's original affidavit in support of its application for a wiretap failed to disclose the nature and extent of the SEC's lengthy investigation of Mr. Rajaratnam; the FBI's prior investigation of Mr. Rajaratnam for insider trading; the large amount of evidence the SEC amassed during its investigation; and the prosecutor's unfettered access to that information. Considering the government's nondisclosure of this information, the court found that sufficient grounds existed for holding an evidentiary hearing, known as a *Franks* hearing, to test the veracity of the affidavit underlying the government's wiretap application.[23]

At the *Franks* hearing, the court found that the prosecutor's failure to disclose the SEC's extensive independent investigation in its original wiretap application was a "glaring omission," given that the SEC's traditional investigative techniques were identical to the techniques which the U.S. Attorney's Office now claimed were unlikely to succeed. In fact, those techniques had yielded an enormous amount of evidence for the SEC, including more than four million documents, witness interviews, and multiple depositions, including a deposition of Mr. Rajaratnam himself, all of which formed a solid, if circumstantial, case against Mr. Rajaratnam for insider trading. Moreover, the SEC had shared all of this evidence with the U.S. Attorney's Office. The volume of evidence was so overwhelming that one of the defense witnesses admitted at the *Franks* hearing that the U.S. Attorney's Office and the FBI spent a majority of their time on the Rajaratnam investigation analyzing the information already gathered by the SEC. By omitting this information in its original wiretap application, the court found that the government essentially "deprived Judge Lynch of the opportunity to assess what a conventional investigation of Rajaratnam could achieve by examining what the SEC's contemporaneous, conventional investigation of the same conduct was, in fact, achieving."[24] In short, this omission "failed to disclose the heart and soul" of the government's investigation.[25]

The government's omission, however, was not dispositive on the question of whether the wiretaps were improper, since a misleading affidavit, in itself, does not justify suppression. To exclude the evidence, the defense needed to make two additional showings: (1) that the government's omissions were the result of deliberate falsehood or a reckless disregard for the truth, and (2) that once the defective affidavit was corrected to account for the omissions and misleading information, it would still fail to establish that the wiretaps were necessary for the

government's investigation. Although the court concluded that the government had acted with reckless disregard for the truth, it also found that after the omitted information was inserted into the affidavit, and after it had been corrected for misstatements, the affidavit would still demonstrate that traditional investigative techniques would be unlikely to succeed. The court reasoned that given the nature of insider trading, which is typically conducted orally and usually leaves no paper trail, Judge Lynch would "not have required the criminal authorities to repeat the SEC's effort."[26] By using the same traditional investigative techniques that the SEC had used, the government would likely only have obtained qualitatively similar evidence to what had already been gathered. Further, the court noted that "the government is not required to exhaust all conceivable investigative techniques before resorting to electronic surveillance."[27] For these reasons, the court refused to suppress the wiretap evidence.

On appeal, Mr. Rajaratnam now argues that the government's failure to make a "full and complete statement" about the SEC's prior investigative techniques requires both statutory suppression under Title III and suppression under the Fourth Amendment. Although some have called Mr. Rajaratnam's appeal a "long shot,"[28] the crux of his argument is that the district court was bound to consider the original affidavit in support of the government's wiretap application based only on the facts available to the issuing court at the time the original wiretap was authorized, not after the affidavit has been "corrected for misstatements" and after "omitted information" has been inserted into the affidavit. According to Rajaratnam, the Fourth Amendment mandates that the preapproval of a government wiretap requires full and complete disclosure that cannot later be corrected after the government has obtained that wiretap.

C. Probable Cause Requirement.

The government must also support its wiretap application with sufficient probable cause. Under 18 USCS § 2518(1)(b), this showing requires a "full and complete statement of the facts and circumstances relied upon by the applicant" in making an application.[29]

Similar to his argument regarding Title III's necessity requirement, Mr. Rajaratnam's probable cause argument also focused on the government's omission that it had the SEC's enormous cache of evidence at its disposal, but it also relied on additional evidence which it claims the government unlawfully manipulated to strengthen its case for a wiretap. In support of showing probable cause in its original affidavit, the government included statements exchanged between its cooperating witness – Roomey Khan – and Mr. Rajaratnam that contained material, nonpublic information. The government specifically averred that Ms. Khan had yet to be charged with any crimes. The supporting affidavit omitted that she had previously been arrested for felony wire fraud, to which she had pleaded guilty some six years earlier. Because this information had been omitted, it was not available to Judge Lynch when he authorized the government's wiretap. Although the court regarded this omission to be "particularly disturbing,"[30] it found it insufficient to invalidate the affidavit and suppress the wiretap evidence.

Further, the defense argued that the government's affidavit also paraphrased summaries of telephone conversations between its witness and Mr. Rajaratnam in ways that subtly changed the content of Mr. Rajaratnam's statements to appear more incriminating than they actually were. Despite these shortcomings, and correcting the affidavit to account for the government's misstatements and omissions, the court still found that enough facts remained before Judge Lynch for him to have found probable cause in authorizing the original warrant. As the court concluded, "Adding it all up, and correcting the affidavit to account for the government's misstatements and omissions, the Court believes that there were enough facts for Judge Lynch to have found probable cause."[31]

This issue is also on appeal, where Mr. Rajaratnam agues that neither Title III nor the Fourth Amendment permits post-hoc factual justification for the authorization of warrants.

D. The Government Must Minimize Its Interception of Irrelevant Communications.

Section 2518(5) of Title III mandates that the government must minimize listening to conversations that do not implicate the predicate acts under Title III. Perhaps more than anything else in Title III, this requirement highlights the tension between privacy rights and the government's need to investigate crime. By failing to minimize its interception of irrelevant communications, prosecutors not only risk violating Title III, they also risk offending the court. In the recent insider-trading prosecution of Craig Drimal, formerly of Galleon, the federal judge overseeing the case criticized the government for listening to the suspect's personal calls, calling the government's behavior "nothing short of disgraceful."[32]

Mr. Rajaratnam has also argued that the government failed to conduct its surveillance in a way that minimized the interception of nonrelevant conversations. Yet under the case law interpreting Title III, the government needs only to make a "reasonable" effort to minimize the interception of nonrelevant calls. This "reasonableness" is determined on a case-by-case basis, depending on the scope and nature of each investigation. Once the government demonstrates that its efforts to minimize the interception of nonrelevant calls was reasonable, the burden shifts to the defendant to show that "a substantial number of non-pertinent conversations have been intercepted unreasonably."[33]

Moving to suppress the wiretap evidence against him on the ground that the government failed to minimize its interception of nonrelevant calls, Mr. Rajaratnam pointed to 150 calls which had been recorded despite being nonrelevant to the investigation. But when contrasted with the vast majority of the recorded calls which were relevant –nearly 19,000 – the court found that the government's recording of these 150 nonrelevant calls was objectively reasonable and that suppression was therefore not required.

III. THE SEC LACKS THE AUTHORITY TO OBTAIN WIRETAPS.

The *Columbia Business Law Review* speculated, "Perhaps . . . we will see more evidence of similarly unabashed behavior [by insider traders] in future cases if the SEC continues to employ the aggressive wiretapping tactics that significantly bolstered their case against Rajaratnam."[34] This conjecture, however, belies a common misconception about wiretaps: that the SEC has the authority to issue wiretaps in the first place.

The SEC's investigation of Mr. Rajaratnam spanned a decade. In 1999, the SEC began investigating Galleon's California office for possible violations of federal securities laws. The SEC eventually issued a formal order of investigation of Galleon in November 2003 and served subpoenas on the company. The SEC also sought evidence from third parties, and took extensive testimony during its investigation. Galleon produced more than four million pages of business records to the SEC and also made available more than twenty Galleon employees for testimony, including Mr. Rajaratnam himself. None of this evidence was obtained by interception of Rajaratnam's communications.

Nevertheless, in the SEC's own civil enforcement action against Mr. Rajaratnam, it largely relied on the incriminating phone conversations recorded by the U.S. Attorney's Office. How, then, did the SEC obtain this evidence?

Surprisingly, not from the U.S. Attorney's Office. As noted above, the U.S. Attorney's Office launched its own investigation in March 2007, and only after the SEC briefed that office on Mr. Rajaratnam's suspected wrongdoing. A year later, in March 2008, the U.S. Attorney's office, with the assistance of Roomy Khan, a former associate of Mr. Rajaratnam whom the government was able to turn into a government witness, obtained enough information to persuade Judge Lynch of the Southern District of New York to approve the government's application for a thirty-day wiretap on Mr. Rajaratnam's cell phone. Evidence obtained from that first wiretap led the government to apply for wiretaps on other phone lines, and for additional thirty-day extensions to their existing wiretaps. By the end of their investigation, the U.S. Attorney's Office and FBI had recorded more than 18,000 separate phone conversations. But with the exception of a few leaked recordings, apparently none of this evidence was shared with the SEC.

There was, however, another way for the SEC to obtain that evidence. The U.S. Attorney's Office produced its wiretap evidence to Mr. Rajaratnam, including copies of the wiretapped communications, the orders authorizing the wiretaps, and the government's applications for those orders. The SEC, in turn, served document requests directly on Mr. Rajaratnam for the production of that same evidence. Mr. Rajaratnam refused, prompting the SEC to file a motion to compel. Judge Rakoff, who presided over Mr. Rajaratnam's civil proceeding, granted the SEC's motion and issued a discovery order compelling the production of the wiretap evidence to the SEC. The defense appealed that decision to the Second Circuit. At the same time, Rajaratnam had filed his motion to suppress in the criminal proceeding.

The Second Circuit found that Judge Rakoff, in the civil proceeding, had acted prematurely in granting the SEC's motion to compel, because the court had yet to rule whether the wiretaps were legal in the criminal proceeding. The court thus vacated Judge Rakoff's discovery order and remanded for further proceedings. The Second Circuit noted, however, that the SEC had a presumptive right of access to wiretaps where the defendants, in a parallel criminal case, had already obtained those wiretaps. As long as the wiretap itself was legal, the SEC could obtain the wiretap evidence directly from the defendant in the criminal proceeding. By the time the case had been remanded to the district court, the court in the criminal proceeding had already ruled that the wiretaps were legal. The SEC then renewed its motion to compel, which Judge Rakoff granted. Soon the SEC had the wiretap evidence it would use to successfully prosecute Mr. Rajaratnam in its civil case.

An interesting question which the Second Circuit's decision leaves open, and which may have a far-reaching impact, is whether wiretap evidence, after it has been produced to a criminal defendant under Title III, may also be obtained by private litigants who have viable, related causes of action against the same defendant.

IV. CONCLUSION

The government has recently used wiretaps in white collar investigations with great success. The government without question will continue to resort to interception of a suspect's communications in appropriate white collar investigations. Indeed, given its substantial success (both through pleas and convictions) based on this type of evidence, it is expectable that the government will seek to intercept communications far more frequently than in the past.

Of course, the government still must meet the standards of Title III. The pending Second Circuit appeal in the Rajaratnam case will likely begin to clarify the limits of the government's authority under Title III in white collar cases.

* * *

---

[1] U.S. Courts, 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 (2009).
[2] James Vicini, "FBI Sets Up Mortgage Fraud Team, Uses Wiretaps," Reuters, May 20, 2009, available at http://www.reuters.com/article/2009/05/20/us-fbi-mortgage-fraud-idUSTRE54J5RO20090520..
[3] Nicholas Schmidle, "Inside the Knockoff-Tennis-Shoe Factory," *The New York Times*, August 19, 2010.
[4] Stephan A. Miller, "Will There Be a 'CSI' Effect for Wiretapping?," *The National Law Journal*, May 10, 2011.
[5] Max Abelson, "Wall Street's New Eliot Ness," *The New York Observer*, December 21, 2010.
[6] *Olmstead v. United States*, 277 U.S. 438 (1928).
[7] *Katz v. United States*, 389 U.S. 347 (1967).
[8] *Katz*, 389 U.S. at 360 (concurrence by J. Harlan).
[9] *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).
[10] *Berger v. New York*, 388 U.S. 41 (1967).
[11] 18 U.S.C.S. § 2510–2522.
[12] 18 U.S.C.S. § 2515.
[13] 18 USC § 2518(1)(a) – (f)
[14] *SEC v. Rajaratnam*, 622 F.3d 159, 165 (2d Cir. 2010).
[15] The United States Department of Justice, "Assistant Attorney General Lanny A. Breuer Speaks at Practicing Law Institute," November 4, 2010, available at http://www.justice.gov/criminal/pr/speeches/2010/crm-speech-101104.html.
[16] 18 U.S.C.S. § 2516(1).
[17] 18 U.S.C.S. § 2516(1)(c).
[18] *United States v. Rajaratnam*, 2010 WL 4867402, at *3 (S.D.N.Y. 2010 Nov. 24, 2010).
[19] *United States v. Rajaratnam*, 2010 WL 4867402 at *2 (S.D.N.Y. Nov. 24, 2010).
[20] *Id.*, at *4.
[21] *Id.*, at *6.
[22] 18 U.S.C.S. § 2518(1)(c).
[23] In a separate order, the Court found that Rajaratnam had "at least established good grounds for holding a *Franks* hearing regarding the veracity of the March 7, 2008 affidavit and the issue of whether the necessity requirement has been satisfied." *United States v. Rajaratnam*, 2010 WL 3219333 at *2 (S.D.N.Y., Aug. 12, 2010).
[24] *United States v. Rajaratnam*, 2010 WL 4867402, at *17 (S.D.N.Y. 2010 Nov. 24, 2010).
[25] *Id.*, at *18.
[26] *Id.*, at *22.
[27] *Id*.
[28] "Rajaratnam Appeal May Be Long Shot," www.reuters.com, May 11, 2011.
[29] 18 U.S.C.S. § 2518(1)(b).
[30] *United States v. Rajaratnam*, 2010 WL 4867402, at *11 (S.D.N.Y. 2010 Nov. 24, 2010).
[31] *Id.*, at *13.
[32] Dennis K. Berman, "The Galleon Legacy: White-Collar Wiretaps," *The Wall Street Journal*, May 11, 2011.
[33] *Id.*, at *27.

[34] Jennifer Warne, "Future Effects of the Galleon Trial," *Columbia Business Law Review*, November 28, 2011.