New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 246—NO. 14
THURSDAY, JULY 21, 2011

Outside Counsel

# White Collar Wiretaps: Will Your Own Words Come Back to Haunt You?

By **Jonathan B. New**

And **Sammi Malek**

The impact of the recent conviction of Galleon Group's co-founder, Raj Rajaratnam,[1] for insider trading has been called "seismic,"[2] due to the novel use of wiretap evidence to bring the crime to life before the jury. As the recent trials of Mr. Rajaratnam, Zvi Goffer, and expert networking consultant Winifred Jiau have unfolded, the full scope of the government's wiretapping has been revealed. The government's recordings have ensnared not just traders and financiers but also officers and directors of public companies, lawyers, and consultants. As a result, Wall Street may now be wondering "is law enforcement listening?" whenever they pick up the phone, as U.S. Attorney Preet Bharara warned in announcing the arrest of Mr. Rajaratnam.

Indeed, many commentators have suggested that the newly aggressive use of wiretaps will have a profound chilling effect on the practices of the financial services sector. Following the revelations about the Rajaratnam wiretaps, hedge-fund managers wondered whether even legitimate exchanges caught on tape would draw scrutiny.[3] One hedge fund executive has reportedly "instructed his colleagues to be extra careful about what they say on the phone, not because they are breaking the law, but because they are fearful that any conversation about stocks could be misconstrued."[4]

Others may choose to meet in person instead of picking up the phone.[5] But whether the success of the Galleon case will open a floodgate of white collar prosecutions based on wiretap evidence remains an open question. Similarly, the extent to which companies will need to change their internal controls and procedures may not be as significant as feared.

### Wiretaps and Financial Crimes

Historically, law enforcement has used wiretaps primarily to aid in the investigation of narcotics trafficking and organized crime.[6] Wiretaps and other means of electronic surveillance are particularly suited for this purpose because organized criminal groups are by nature tightly knit and they rarely create a paper trail that can be used as evidence.[7] Electronic surveillance, therefore, is often the best way—and sometimes the only way—to obtain incriminating evidence against the members of the group. By contrast, financial crimes typically involve false statements in financial statements, prospectuses, disclosures and other written material, and the wrongdoers either leave behind documents, or they communicate by e-mail, instant message and other means that leave an electronic "paper" trail of incriminating evidence.

> It seems unlikely that the government will be given carte blanche to expand the reach of the wiretap statute.

The use of electronic surveillance evidence in white collar cases, however, is not as unprecedented as some commentators have suggested. While the Galleon case marked the first use of wiretaps in an insider trading case, federal and state law enforcement agencies have used wiretaps and undercover agents in past white collar criminal cases, including investigations of mail and bank fraud conspiracies,[8] trafficking in counterfeit goods,[9] and telemarketing "boiler rooms."

Nevertheless, the Galleon case reflects a recent coordinated effort by law enforcement to use electronic surveillance and "organized crime" style approaches more frequently in white collar cases. For example, in 2009, the FBI created the National Mortgage Fraud Team and began using "sophisticated investigative techniques, such as undercover operations and wiretaps" with the goal of "apprehend[ing] criminals in the commission of their crimes…."[10] The 2010 prosecution of Trevor Cook in Minnesota for running a fraudulent investment scheme,[11] as well as the ongoing prosecution of 22 military and law enforcement equipment suppliers for allegedly engaging in a scheme to bribe foreign government officials, relied heavily on the aggressive use of undercover law enforcement tactics.[12]

As technology advances faster than the speed of light, criminals continue to get more sophisticated in their methods, forcing law enforcement to try and keep up. While electronic surveillance, and particularly wiretaps, are a useful and compelling tool in building a case, there are legal and practical limitations that will likely prevent this tool from becoming as ubiquitous in white collar criminal prosecutions as some have predicted.

### Limitations

The legal limitations on the use of wiretaps in white collar criminal investigations stem primarily from the language of the statute itself. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (codified in 18 U.S.C. §2510, et seq.)

JONATHAN B. NEW *is a partner in Baker Hostetler's white collar defense and corporate investigations practice in the New York office and a former assistant U.S. attorney.* SAMMI MALEK *is a litigation associate at the firm's New York office.*

specifies certain predicate offenses that the federal government must be investigating in order to apply for an electronic surveillance order.[13] Notably, neither securities fraud nor insider trading is one of those predicate offenses.[14] While the proverbial "catch-all" offenses of wire fraud and mail fraud can provide a basis for obtaining warrants to wiretap suspects being investigated for a variety of different activities, the decisions by Southern District of New York Judges Richard Holwell and Richard Sullivan in the Galleon-related cases remain the only legal precedent for allowing the use of wiretaps in an insider trading case, and those decisions will undoubtedly be appealed.[15]

If, as some have predicted, the government tries to capitalize on the Rajaratnam victory by applying more frequently for wiretaps to investigate financial crimes, it remains to be seen whether courts will follow the lead of these decisions, or if they will begin to recognize limits. The government can only seek a wiretap if there is probable cause to believe that a predicate offense is being committed, and a court may suppress a wiretap if the application fails to meet this standard or for government misconduct.

The number of crimes that may be investigated using wiretaps has expanded over time, but still does not include securities fraud. Since 1986, Congress has repeatedly added to the list of predicate offenses to include access device fraud, bank fraud, computer fraud and criminal violations of the Sherman Act.[16] Similarly, in March 2011, the Obama administration proposed legislation granting law enforcement the authority to seek wiretaps in investigations of criminal copyright and trademark offenses.[17] Thus, the government recognizes that prosecutors may not always be able to bootstrap non-predicate white collar offenses to wire fraud and mail fraud in order to get around the limitations of the statute.

The proposed legislation, notably, was received with some skepticism,[18] and privacy advocates have raised concerns about attempts by the government to further monitor people's communications.[19] It, therefore, seems unlikely that the government will be given carte blanche to expand the reach of the wiretap statute.

The second legal hurdle the government faces in obtaining wiretap authorization in white collar criminal cases is the requirement to show "necessity": the government must set forth facts to support a finding that "other investigative procedures have been tried and failed" or that "they reasonably appear to be unlikely to succeed if tried" or are "too dangerous."[20] Additionally, a wiretap application has to be renewed after 30 days and the government is required to justify the continued necessity of the wiretaps. Most financial crimes can be detected using conventional investigative techniques, making it difficult for the government to be able to routinely show necessity when applying for electronic surveillance. While the government is not required to exhaust all other techniques before turning to wiretaps, electronic surveillance is not intended to be "a routine initial step" in an investigation.[21]

There are also practical limitations to the routine use of wiretaps in insider trading cases. Wiretaps are an invaluable tool for investigating ongoing crimes involving large groups of individuals where the government is able to build a foundation over an extended period of time. White collar cases do not often follow this model. Investigations of financial crimes are typically historical in nature, and often start after the fraudulent act or insider trading has already taken place.

Unlike the Rajaratnam investigation, which spanned nearly a decade and involved a large network of individuals that included hedge fund managers, consultants, corporate insiders and even attorneys, the garden variety insider trading cases ordinarily involve a handful of suspects accused of making a discreet number of illicit trades. In such instances involving few individuals and relatively small losses, the considerable time and expense required to conduct electronic surveillance makes its routine use impractical.[22]

> While electronic surveillance, and particularly wiretaps, are a useful and compelling tool in building a case, there are legal and practical limitations that will likely prevent this tool from becoming as ubiquitous in white collar criminal prosecutions as some have predicted.

### Implications

Although electronic surveillance of the financial sector may not become routine, its dramatic use in the Galleon and expert networking investigations has highlighted the need for effective and comprehensive compliance programs to identify and address questionable practices before they become widespread. With the government having publicly declared its policy of aggressively pursuing cases of financial fraud, companies are well-advised to take this opportunity to review and update their internal policies and procedures currently in place, to retrain their employees on best practices, and establish a culture in which employees seek advice on actions that may be close to the line.

Similarly, the recordings played at the recent insider trading trials highlight the challenges that public companies and their investment relations officers (IROs) face in managing disclosure risks. Some commentators have called it "an opportunity for IROs to reinforce their disclosure policies internally to insiders who might be tempted to provide sensitive information either via expert networks or directly to analysts."[23] Compliance officers and IROs who seize this opportunity stand a greater chance of preventing or detecting early even an inadvertent improper disclosure of material nonpublic information, which not only protects the company and its insiders from criminal prosecution, but also benefits the investing public.

•••••••••••••●●●•••••••••••••

1. Peter Lattman and Azam Ahmed, Galleon's Rajaratnam Found Guilty, Dealb%k (May 11, 2011 10:50 AM), http://dealbook.nytimes.com/2011/05/11/rajaratnam-found-guilty/.
2. Stephen A. Miller, Will There Be a 'CSI Effect' for Wiretapping?, The National Law Journal (May 23, 2011), http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202494773565&slreturn=1&hbxlogin=1.
3. Katherine Burton and David Glovin, Galleon Wiretaps Rattle Hedge Funds, Bloomberg (Oct. 26, 2009), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=as8seXJpbDUY.
4. Id.
5. Id.
6. In 2009, 86 percent of all applications for wiretaps involved drug-related offenses. See 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), available at http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/2009Wiretaptext.pdf.
7. Corporate Counsel's Guide to White collar Crime (2009), available at Westlaw CCGWHCOLL §9:1.
8. 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, 12 (2006), available at http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2006/2006WT.pdf.
9. Nicholas Schmidle, "Inside the Knockoff-Tennis-Shoe Factory," N.Y. Times, Aug. 8, 2010, at MM38.
10. James Vicini, "FBI Sets Up Mortgage Fraud Team, Uses Wiretaps," Reuters (May 20, 2009, 2:48 PM) (quoting remarks by FBI Director Robert Mueller), http://www.reuters.com/article/2009/05/20/us-fbi-mortgage-fraud-idUSTRE54J5RO20090520.
11. Dan Browning and Sarah Gorvin, "Minneapolis Money Manager Trevor Cook Admits to $190 Million Scam," Star Tribune (April 14, 2010, 12:20 PM), http://www.startribune.com/business/90751939.html.
12. Lanny A. Breuer, Assistant Attorney General, Dept. of Justice, Financial Crisis Fallout 2010: Emerging Enforcement Trends, Address Before the Practising Law Institute (Nov. 4, 2010) (transcript available at http://www.justice.gov/criminal/pr/speeches/2010/crm-speech-101104.html).
13. 18 U.S.C. §2516.
14. Id.
15. See *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 WL 4867402 at *1 (S.D.N.Y. Nov. 24, 2010) (Holwell, J.); *United States v. Goffer*, 756 F.Supp.2d 588 (S.D.N.Y. 2011) (Sullivan, J.).
16. *Rajaratnam*, 2010 WL 4867402 at *6, n.8.
17. Exec. Office of the President, Administration's White Paper On Intellectual Property Enforcement Legislative Recommendations (2011), available at http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf.
18. David Makarewicz, Do Obama's Proposed New Copyright Laws Go Too Far?, Sites and Blogs (March 16, 2011), http://www.sitesandblogs.com/2011/03/do-obamas-proposed-new-copyright-laws.html; David Makarewicz, New Proposal to Wiretap Suspected Infringers Raises Privacy Concerns, Infowars.com (Mar. 17 2011), http://www.infowars.com/new-proposal-to-wiretap-suspected-infringers-raises-privacy-concerns/.
19. Debra Cassens Weiss, "Privacy Advocates Decry Anti-Crime Proposals for Internet Wiretaps, Bank Disclosures," ABA Journal, (Sept. 27, 2010, 8:03 AM), http://www.abajournal.com/news/article/privacy_advocates_decry_anticrime_proposals_for_internet_wiretaps_bank_dis/.
20. 18 U.S.C. §2518(1)(c).
21. *United States v. Lilla*, 699 F.2d 99, 104 (2d Cir. 1983) (internal quotations and citations omitted).
22. According to the Report of the Director of the Administrative Office of the United States Courts, the average cost for federal wiretaps in 2009 was $62,552.
23. Brad Allen, Galleon Verdict Bolsters Role of IR, Business Insider (May 12, 2011), http://www.businessinsider.com/galleon-verdict-bolsters-role-of-ir-2011-5.