



North East Journal of Legal Studies

Volume 31 *Spring 2014*

Article 1

Spring 2014

Signs Of Things To Come: Inter-Agency Coordination, Shared Evidence, And Wiretaps In Prosecuting White-Collar Crime

Natalie Bordeaux

Follow this and additional works at: <https://digitalcommons.fairfield.edu/nealsb>

Recommended Citation

Bordeaux, Natalie (2014) "Signs Of Things To Come: Inter-Agency Coordination, Shared Evidence, And Wiretaps In Prosecuting White-Collar Crime," *North East Journal of Legal Studies*: Vol. 31 , Article 1. Available at: <https://digitalcommons.fairfield.edu/nealsb/vol31/iss1/1>

This item has been accepted for inclusion in DigitalCommons@Fairfield by an authorized administrator of DigitalCommons@Fairfield. It is brought to you by DigitalCommons@Fairfield with permission from the rights-holder(s) and is protected by copyright and/or related rights. **You are free to use this item in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses, you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/or on the work itself.** For more information, please contact digitalcommons@fairfield.edu.

**SIGNS OF THINGS TO COME: INTER-AGENCY
COORDINATION, SHARED EVIDENCE, AND
WIRETAPS IN PROSECUTING WHITE-COLLAR
CRIME**

by

Natalie Bordeaux*

INTRODUCTION

Although wiretapping suspects and coordinated investigations by law enforcement to prosecute wrongdoers are tactics commonly used for so-called blue-collar crimes, the economic collapse of 2008 spurred a new wave of ingenuity on the part of the federal government in deterring and punishing white-collar crime, particularly fraud. It wasn't that any of the investigative techniques used were novel, as all of the methods had already existed. Rather, law enforcement's approach was fresh because its fact-gathering tools were rarely used for white-collar crime before, and never employed as successfully as in the parallel civil and criminal actions against Raj Rajaratnam and others within his circle for insider trading. Through inter-agency collaboration and wiretapping¹, the United States Department of Justice ("DOJ") and the Securities and Exchange

Commission ("SEC") prosecuted and fined perpetrators of

*Natalie Bordeaux, Adjunct Professor, Pace University

what had been described as the “largest hedge fund insider trading case in history”.²

The “largest hedge fund insider trading case” was actually two cases: *United States v. Rajaratnam*,³ and *SEC v. Galleon Management, LP*.⁴ Both cases resulted from an organized investigation by the DOJ and the SEC that uncovered a ring of powerful, wealthy members of the financial industry engaged in insider trading.⁵ Raj Rajaratnam, Manager of Galleon Management LP (hereinafter, “Galleon”), a hedge-fund advisory firm, was convicted of fourteen counts of conspiracy to commit and actual commission of insider trading.⁶ In the criminal action, Rajaratnam was sentenced to 11 years in prison, ordered to forfeit \$53.8 million, and was fined an additional \$10 million in criminal penalties.⁷ At the time, Rajaratnam’s sentence was the longest ever imposed in an insider trading case.⁸ In the civil action commenced by the SEC, District Court Judge Jed Rakoff imposed a civil penalty of \$92,805,705 on Raj Rajaratnam.⁹

In both the criminal and civil cases, defense counsel raised numerous challenges, including the government’s ability to wiretap the defendants’ telephones, and utilize intercepted calls as evidence of wrongdoing. Nevertheless, the DOJ and SEC prevailed in their actions against the defendants for conspiring to engage in insider trading and committing insider trading. Their success was founded largely upon the use of wiretapped conversations between the defendants, and cooperation between the SEC and the United States Attorney’s Office (“USAO”)¹⁰.

This article will provide an overview of the Rajaratnam cases, and explain key procedural and substantive issues it presented, including the fundamental requirements for lawfully obtaining wiretaps, the investigative and enforcement process

for securities violations, and the increasing communication between federal agencies regarding white-collar criminal investigations. The article concludes that the efficiencies afforded by wiretapping and the pooling of administrative resources in fact-gathering will lead to an increase in enforcement actions and penalties.

UNITED STATES V. RAJARATNAM¹¹ AND SEC V. GALLEON MANAGEMENT, LP¹²

On October 16, 2009, the USAO and the SEC filed criminal and civil complaints, respectively, against Raj Rajaratnam and other defendants¹³ for insider trading.¹⁴ The USAO unsealed criminal complaints charging Raj Rajaratnam and other defendants with conspiracy and insider trading under Section 10(b) of the Securities Exchange Act of 1934¹⁵, and Rule 10b-5¹⁶.

Both complaints involved the same conduct,¹⁷ and a significant portion of evidence introduced in each case was obtained from wiretapping the communications of several defendants.¹⁸ Members of Rajaratnam's ring included personal friends Rajiv Goel and Anil Kumar, and a former employee, Roomy Khan.¹⁹ At the outset, many of the facts surrounding trades made by Rajaratnam on Galleon's behalf appeared remarkably fortuitous. However, upon closer inspection, the trades served as strong evidence establishing the commission of both civil and criminal violations involving the unlawful use of material, non-public information.

Rajaratnam had enlisted the aid of Roomy Khan to obtain "material, non-public information" regarding earnings, acquisitions and business agreements of numerous publicly-traded corporations, including Google, Hilton Hotels Corporation, Intel and Sprint Nextel Corporation.²⁰ As

Rajaratnam's criminal conduct continued, law enforcement and the SEC were able to identify a large quantity of information to corroborate suspicions surrounding Galleon's financial success. For instance, Khan (who provided Rajaratnam with confidential information regarding Polycom,²¹ the sale of Kronos²² to a private equity firm,²³ the acquisition of Hilton by the Blackstone Group, and Google's earnings reports), traded on the information herself before the information became public, and very close in time to Rajaratnam's subsequent activity on the stock, personally, and on Galleon's behalf.²⁴ Additionally, Rajaratnam purchased Hilton shares to capitalize on the information that Khan had provided regarding an upcoming acquisition of Hilton by the Blackstone Group²⁵ on behalf of the Galleon Tech Funds, an unusual investment for funds whose objective is to invest in the technology sector.²⁶

Yet there was still more information to establish Rajaratnam's illegal activities. After Rajiv Goel provided Rajaratnam with insider information concerning Intel's earnings, and a business endeavor involving Sprint Nextel Corporation and Clearwire Corporation,²⁷ Rajaratnam rewarded Goel by trading on Goel's account, using insider information concerning the imminent Hilton takeover, and other companies' information.²⁸

Danielle Chiesi, portfolio manager at New Castle, used several tips she received to trade on New Castle's behalf, and shared the information with other individuals, including Rajaratnam.²⁹ Chiesi traded on material nonpublic information obtained from an Akamai Technologies, Inc. executive, and shared this information with Mark Kurland, and Rajaratnam, who traded on behalf of himself and Galleon using this information.³⁰

Chiesi also received several tips from Robert Moffat, a senior executive of IBM, which she used in trading on behalf of New Castle. Moffat provided Chiesi with material nonpublic information regarding the earnings of IBM and Sun Microsystems, Inc., along with negotiations between AMD³¹ and two companies based in Abu Dhabi.³²

Additionally, communications between several of the defendants were ongoing, and/or extremely close in time with changes in investments. For instance, Rajaratnam contacted Goel on January 8, 2007, about one week before Intel's earnings information regarding the fourth quarter of 2006 was to be released.³³ On January 9, 2007, Rajaratnam began buying Intel shares on his own behalf and that of Galleon.³⁴ Over the course of the Martin Luther King Day weekend, Rajaratnam and Goel were in repeated communication.³⁵ When the markets reopened on Tuesday, January 16, 2007, both defendants suddenly altered their investment strategies regarding Intel, with Galleon selling its entire long position in Intel.³⁶ In its complaint, the SEC cites numerous examples of continued communication coinciding with very pointed changes in investing by defendants Rajaratnam, Galleon, Chiesi, Kurland, New Castle, and Goel.³⁷

AUTHORIZATION OF WIRETAPS PURSUANT TO TITLE III OF THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968

An Overview on the Use of Wiretaps

Today, the term "wiretapping" refers to electronic or mechanical eavesdropping³⁸, a sweeping description that includes the surveillance of voice, e-mail, fax, and internet communications.³⁹ Other than certain enumerated exceptions

described below, wiretapping is illegal and yields inadmissible evidence.

In 1967, the Supreme Court issued two landmark decisions regarding law enforcement's use of wiretapped conversations. Although several earlier cases had ruled upon the permissibility of intercepted conversations,⁴⁰ the Supreme Court's decisions in *Berger v. New York*⁴¹ and *Katz v. United States*⁴² confirmed that the Fourth Amendment protection against unreasonable search and seizures⁴³ applied to intercepted communications in places where an individual has a reasonable expectation of privacy.⁴⁴

In *Berger*, the petitioner's conviction for conspiring to bribe the Chairman of the New York State Liquor Authority was based solely on recorded conversations using a planted "bug" in the office of an attorney allegedly involved in the bribery scheme.⁴⁵ The Court held that law enforcement must abide by the Fourth Amendment requirement of a warrant based upon probable cause before recording conversations in an individual's home or office.⁴⁶

The holding in *Katz* went a step further than *Berger*, extending Fourth Amendment protection to any location where an individual may "justifiably" expect to have a private conversation.⁴⁷ In *Katz*, the petitioner's conviction for interstate gambling by wire communication was based, in part, upon evidence submitted by the Government of the petitioner's portion of conversations recorded using a device attached to the outside of the public telephone booth where the petitioner had placed his bets. The Supreme Court confirmed that the determination as to the admissibility of oral evidence required the same analysis as conducted for physical evidence.⁴⁸ Additionally, the Court dismissed the notion that physical intrusion of a recording device was required for resulting

recordings to be in violation of the Fourth Amendment.⁴⁹ After *Berger* and *Katz*, law enforcement needed rules for permissible electronic surveillance.

*Added Guidance: Title III of the Omnibus Crime Control and Safe Streets Act of 1968*⁵⁰

In response to these holdings, Congress undertook its own efforts to define a clearer standard for law enforcement. Congressional research found that unauthorized and nonconsensual wiretapped communications were being used as evidence in courts and administrative agencies by both governmental and private parties, in violation of individuals' privacy rights.⁵¹

As a result of these findings, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the "Wiretap Act".⁵² At its inception, the Wiretap Act sought to balance the privacy interests of private persons with the needs of law enforcement in intercepting communications to prosecute individuals engaged in criminal activity.⁵³ This legislation made unauthorized or nonconsensual interceptions of wire or oral communications illegal.⁵⁴ Additionally, it delineated specific requirements for government officials to satisfy to obtain wiretap authorizations, and regulated the use of such interceptions.

Statutory Requirements for Lawful Wiretapping

Permissible use of wiretaps by government agents is comparable to any other governmental search and seizure under the Fourth Amendment, as law enforcement must obtain authorization to intercept communications in places where an individual has a reasonable expectation of privacy.⁵⁵

There are several ways in which law enforcement may legally intercept wire, oral or electronic communications. For instance, a “person acting under color of law” may utilize a wiretap if a party to the communication or where prior consent has been given by one of the parties engaged in the communication.⁵⁶

The Wiretap Act also permits application by both federal and state law enforcement agencies to the appropriate judges for authorization of a wiretap.⁵⁷ Such application requires great detail in order to avoid granting unfettered discretion to law enforcement in its use of wiretaps. Supporting information required for any wiretap authorization is similar to that of a regular warrant application in that the application must be made under oath,⁵⁸ with a specific description of the facts and circumstances upon which the applicant relies⁵⁹ as showing probable cause to believe that specific offenses have or are being committed.⁶⁰ The application must describe the type of communication which authorities seek to intercept,⁶¹ and the identity of the person, when known, whose communications are to be wiretapped.⁶²

However, the applicant must also provide a “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”.⁶³ As any wiretapping authorization is to be as narrow in scope as possible, authorizations must describe the type of communications to be intercepted,⁶⁴ the location where the authority to intercept is given,⁶⁵ the agency possessing the authority to conduct such interceptions,⁶⁶ and the period of time for which interception is permissible by the order.⁶⁷ Additionally, the order must include a provision requiring the interception to “be conducted in such a way as to minimize the

interception of communications not otherwise subject to interception” pursuant to the Wiretap Act.⁶⁸

Despite the utmost precision with which wiretapping authority is given, and a lengthy list of offenses for which interception is authorized, the Wiretap Act enables law enforcement to use information obtained from otherwise lawful intercepts regarding offenses for which authorization was not granted or those offenses that are not specifically listed in the Wiretap Act as lawful grounds upon which wiretapping is permissible.⁶⁹ As will be discussed below, the United States Attorneys’ Office procured a lawful intercept for an investigation of wire fraud (an enumerated offense in the Wiretap Act), and obtained admissible evidence establishing charges of insider trading in the *Rajaratnam* case.

Furthermore, the Wiretap Act permits law enforcement to share the information obtained from authorized interceptions with other members of law enforcement.⁷⁰ Cooperation is now increasingly likely between several federal enforcement agencies, including the United States Department of the Treasury, the DOJ and the United States Department of Housing and Urban Development, as will be discussed below.

Issues Presented by the Rajaratnam Cases

Unlisted Offenses:

In the criminal action brought against Raj Rajaratnam and others, Rajaratnam and Danielle Chiesi moved to suppress the recorded conversations obtained by the DOJ pursuant to Title III on several grounds. First, Rajaratnam and Chiesi sought exclusion of the wiretapped calls from evidence because insider trading was not an offense enumerated in Title III for which a wiretap was permissible.⁷¹ In its application, the

government requested wiretap authorization for investigation of wire fraud, an enumerated offense for which recording conversations is authorized.⁷² District Court Judge Richard Holwell rejected this contention, noting that although Title III only authorizes the use of wiretaps for offenses listed in 18 U.S.C. § 2516, it does not bar evidence obtained during the course of a lawful wiretap for unlisted offenses, so long as wiretap applications were obtained in good faith and “not as a subterfuge for gathering evidence of other offenses.”⁷³ Judge Holwell found the DOJ’s applications to be very transparent, detailing the insider trading plot, and setting forth the evidence they had obtained that established probable cause to believe that wire fraud and money laundering had been committed.⁷⁴ Thus, the government’s investigation was conducted in good faith, and evidence obtained by the wiretapped conversations which established securities fraud was a “by-product” of lawfully procuring evidence of wire fraud.⁷⁵

Probable Cause:

Rajaratnam and Chiesi also argued that the government’s applications and supporting affidavits failed to show probable cause as to the necessity of the wiretaps.⁷⁶ Rajaratnam argued that the wiretap application and supporting documentation falsely characterized co-defendant Roomy Khan as a credible source, and misconstrued other evidence in the application.⁷⁷ Judge Holwell rejected this challenge, noting that the government’s application provided information that corroborated Ms. Khan’s allegations that she had given Rajaratnam insider information on Polycom, Hilton, Google and Kronos.⁷⁸ Specifically, Khan’s claims were validated by Rajaratnam’s own statements to Khan in conversations she had recorded at the request of the FBI.⁷⁹

Full Statement of Other Attempted Investigative Procedures:

Rajaratnam and Chiesi both sought suppression of the recordings on the grounds that the wiretap applications did not comply with Title III's requirement of 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."⁸⁰ This argument also failed, as Judge Holwell noted that the requirement was not one of exhaustion of all other investigative methods, but rather, communication with the authorizing judge about the investigation's progress and difficulties corresponding with employing regular law enforcement tactics.⁸¹ Where an application shows that less invasive methods are unlikely to succeed or are impractical, such facts will satisfy the requirements of Section 2518(1)(c).⁸²

Minimization Requirement:

Both Rajaratnam and Chiesi also challenged the introduction of several wiretaps, arguing that the government failed to minimize conversations that were not relevant to the investigation, as required by 18 U.S.C. § 2518(5).⁸³ Judge Holwell noted that the wiretap authorizations properly included the minimization order, and that the law enforcement agents worked to reasonably minimize the interception of irrelevant conversations.⁸⁴ Furthermore, the Court recognized that an investigation involving a large-scale conspiracy requiring "more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise."⁸⁵

Rajaratnam's Motions for Acquittal:

Subsequent to these challenges, Rajaratnam sought acquittal on all 14 charges against him at three different points in the trial: (1) at the close of the prosecution's case; (2) after all evidence had been presented; and (3) after a jury verdict

found him guilty of all 14 charges (five counts of conspiracy to commit securities fraud, and nine counts of securities fraud).⁸⁶ Amidst multiple arguments submitted regarding Rajaratnam's conviction, Rajaratnam's attorneys contended that his conviction on several conspiracy counts was based solely upon indirect evidence from the wiretapped conversations and that such conversations were inadmissible hearsay evidence.⁸⁷ Both arguments were rejected. Pursuant to the Federal Rules of Evidence, a co-conspirator's statements made "during the course and in furtherance of the conspiracy" are not considered hearsay.⁸⁸ Furthermore, the government was able to provide additional evidence corroborating statements made, notably, changes in Rajaratnam's investment positions within very short time periods subsequent to calls made and information he obtained therefrom.⁸⁹

The SEC's Discovery Demands for Wiretapped Conversations from Rajaratnam and Chiesi:

In the course of the criminal proceedings commenced against the defendants, the USAO had given Rajaratnam and Chiesi the wiretap recordings that they intended to use at trial; however, the prosecutors had not shared these recordings with the SEC.⁹⁰ Since certain recordings were in the possession of Rajaratnam and Chiesi, the SEC sought to obtain production of the recordings through discovery demands, which both Rajaratnam and Chiesi opposed.⁹¹ Although there was no dispute that such recordings would normally be discoverable, Rajaratnam and Chiesi challenged the requests. They claimed that they were unable to provide the SEC with the recordings because Title III prohibited disclosure of interceptions not explicitly permitted by statute, stemming from Congress' privacy concerns in enacting Title III.⁹²

Judge Rakoff of the Southern District of New York noted that 18 U.S.C. § 2517 had been amended in 1970 to enable anyone who had lawfully obtained wiretap recordings to disclose the contents of such recordings “while giving testimony in any proceeding held under the authority of the United States or of any State or political subdivision thereof.”⁹³ In granting the SEC’s demand for production of the recordings, Judge Rakoff observed:

[T]he notion that only one party to a litigation should have access to some of the most important non-privileged evidence bearing directly on the case runs counter to basic principles of civil discovery in an adversary system and therefore should not readily be inferred, at least not when the party otherwise left in ignorance is a government agency charged with civilly enforcing the very same provisions that are the subject of the parallel criminal cases arising from the same transactions.⁹⁴

Privacy concerns were addressed by the court’s issuance of a protective order barring disclosure of the recordings to any non-party to the case until a court of competent jurisdiction ruled on a suppression motion regarding such disclosure.⁹⁵

INTER-AGENCY COORDINATION OF INVESTIGATIVE AND ENFORCEMENT EFFORTS IN WHITE-COLLAR CRIME CASES

The SEC is authorized to investigate potential securities violations using administrative, civil, and/or criminal remedies.⁹⁶ The SEC may employ civil and/or administrative actions to enforce the relevant federal laws.⁹⁷ However, only the DOJ may pursue a criminal action for these violations.⁹⁸

The investigation surrounding Rajaratnam and his co-defendants showed that the ultimate success in prosecuting Rajaratnam and others resulted from the complimentary investigative approaches of the SEC and DOJ. The SEC had employed conventional investigational tools to expose Rajaratnam's insider trading circle and was unable to unearth the scheme to its fullest extent because the suspects had carried out their violations by telephone.⁹⁹ It was through the DOJ's efforts that wiretaps were authorized,¹⁰⁰ and resulting recorded conversations served as key evidence against the defendants.¹⁰¹

The Authority of the SEC

The Securities Exchange Acts of 1933 and 1934 prohibit a number of securities-related activities.¹⁰² Congress has given the SEC the authority to promulgate rules and regulations pertaining to such activities.¹⁰³

After monitoring suspicious market activity, receiving a complaint, or a referral from other SEC divisions or other sources, the SEC's Enforcement Division may commence an informal investigation of possible securities violations.¹⁰⁴ Upon completion of the initial review and identifying violations, the Enforcement Division prepares a "formal investigative order", which requires only a non-adherence to securities laws.¹⁰⁵ The Enforcement Division is able to issue subpoenas, and order production of documents.¹⁰⁶ At the conclusion of the Enforcement Division's investigative presentation, the Commission may authorize the Enforcement Division to file a claim in federal district court or seek administrative action.¹⁰⁷

Administrative proceedings are conducted before an Administrative Law Judge or the SEC.¹⁰⁸ Where a successful showing of securities violations is made by a preponderance of

the evidence, the SEC may seek to enjoin wrongdoers from continuing to engage in wrongful conduct,¹⁰⁹ impose fines,¹¹⁰ and/or order disgorgement.¹¹¹

The Role of the United States Attorney's Office in Securities-Based Crimes

As mentioned above, the SEC lacks the authority to impose criminal sanctions on violators. Such proceedings must be commenced by the United States Attorney's Office within the Department of Justice.¹¹² The SEC rules enable the USAO to access its investigation files, preventing bureaucratic inefficiency from hampering an investigation.¹¹³

A securities-based criminal action has stronger investigative techniques at its disposal, including the use of search warrants,¹¹⁴ and the USAO's ability to determine the scope of discovery, without interference of the defendants.¹¹⁵ Although the USAO's actions are generally initiated after a referral from the SEC,¹¹⁶ the DOJ is not bound by, or reliant solely upon, information from the SEC.¹¹⁷ Thus, the USAO may commence criminal actions in situations where the SEC has either declined to pursue civil or administrative remedies, or where violations, while related to securities, are not within the purview of the SEC's enforcement efforts.¹¹⁸

The Financial Fraud Enforcement Task Force

On the heels of the cooperation between the SEC and the DOJ in investigating Rajaratnam and numerous others allegedly involved in his insider trading ring, the government sent a strong message to would-be violators that joint investigative and enforcement efforts were the new normal. By Executive Order dated November 17, 2009, President Barack Obama established the Financial Fraud Enforcement Task

Force (the “Task Force”).¹¹⁹ The Task Force, led by the Department of Justice, includes senior-level members of numerous federal agencies, and departments, including the SEC, the Department of Treasury, the Criminal Investigation Division of the IRS, the Federal Deposit Insurance Corporation (“FDIC”), and the Department of Housing and Urban Development (“HUD”).¹²⁰

The Task Force’s main purpose is to advise the Attorney General on investigating and prosecuting a variety of fraud cases.¹²¹ Additionally, the Task Force is expected to “coordinate law enforcement operations” with state and local law enforcement.¹²² As SEC Chairman Mary Schapiro explained, “Many financial frauds are complicated puzzles that require painstaking efforts to piece together. By formally coordinating our efforts, we will be able to better identify the pieces, assemble the puzzle, and put an end to the fraud.”¹²³

CONCLUSION

The accomplishments of the SEC and DOJ in unraveling Raj Rajaratnam’s insider trading ring sounded a loud and clear warning to white-collar criminals – federal agencies are now working together, sharing their information, and using new investigative methods to build and bolster their cases. While some may characterize the use of recorded conversations in the Rajaratnam cases as historically insignificant, it is clear that neither the DOJ nor the SEC would have triumphed in the actions commenced against Rajaratnam and others without those communications. Given the number of defendants that were fined and/or sentenced because of the admissible wiretapped evidence, it is highly probable that enforcement agencies will seek to intercept communications in future investigations. If anything, the decisions in the Rajaratnam

cases have refined the wiretapping standards propounded by Title III.

The SEC's and DOJ's combined resources and pooled efforts in the Rajaratnam cases are also significant. The agencies' coordination in these cases exemplified the aims of the Financial Fraud Enforcement Task Force – to aggressively and efficiently prosecute white-collar crime. The image presented by the Task Force is that of a unified movement to protect the public, and punish fraud. If this Task Force succeeds, this is the dawn of a new era, one with strong enforcement, and without red tape.

ENDNOTES

¹ Before the Rajaratnam investigation, wiretapping was a rarity in white-collar criminal investigations. However, this tool had been used before. In *United States v. Zolp*, 659 F.Supp. 692 (D.N.J.) (1987), a case alleging conspiracy to defraud, and actual securities fraud committed by some of the defendants, the United States Attorney's Office obtained authorizations to intercept calls in various locations, including a defendant's home, and corporate offices.

² Press Release, United States Attorney's Office, Manhattan U.S. Attorney Charges Hedge Fund Managers, Fortune 500 Executives, and Management Consulting Director in \$20 Million Insider Trading Case (Oct. 16, 2009) (available at <http://www.fbi.gov/newyork/press-releases/2009/nyfo101609.htm>); *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 70385, *5 (S.D.N.Y. 2010).

³ *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Oct. 16, 2009).

⁴ *SEC v. Galleon Mgmt., LP.*, No. 09 Civ. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009).

⁵ According to SEC Enforcement Director Robert Khuzami, “[Rajaratnam] cultivated a network of high-ranking corporate executives and insiders, and then tapped into this ring to obtain confidential details about quarterly earnings and takeover activity.” Press Release, SEC (Oct. 16, 2009) (available at <http://www.sec.gov/news/press/2009/2009-221.htm>).

⁶ See *United States v. Rajaratnam*, 802 F.Supp.2d 491 (S.D.N.Y. Aug. 16, 2011) (referring to May 11, 2011 jury verdict that found Rajaratnam guilty of five counts of conspiracy to commit insider trading, and nine counts of engaging in insider trading).

⁷ *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Oct. 16, 2009). According to evidence proffered by the DOJ, Rajaratnam was believed to have amassed unlawful gains totaling \$72,071,219, resulting from insider trading activities. *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2012 U.S. Dist. LEXIS 14961, at *3-4 (S.D.N.Y. Feb. 6, 2012).

⁸ Aaron Smith, *Raj Rajaratnam Checks into Prison*, CNN MONEY (Dec. 5, 2011), http://money.cnn.com/2011/12/05/news/companies/rajaratnam_prison/index.htm.

⁹ Before reaching this determination, the parties asked Judge Rakoff to review excerpts from the Pre-Sentence Report in the corresponding criminal case. In describing the criminal penalties imposed, he observed that such penalties were far less than Rajaratnam’s net worth. *SEC v. Rajaratnam*, 822 F.Supp.2d 432, 434 (S.D.N.Y. 2011).

“When to this is added the huge and brazen nature of Rajaratnam’s insider trading scheme, which, even by his own estimate, netted tens of millions of dollars and continued for years, this case cries out for the kind of civil penalty that will deprive this defendant of a material part of his fortune.” *Id.*

¹⁰ “Our law enforcement agencies are together much more than the sum of our parts. That is why coordination, of which today’s actions are a prime example, is critically important to the goal of rooting out fraud and misconduct in our markets. The investing public deserves no less, and we will deliver.” Robert Khuzami, Remarks at Press Conference Regarding Rajaratnam Case (Oct. 16, 2009) (available at <http://www.sec.gov/news/speech/2009/spch101609rk.htm>).

¹¹ *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Oct. 16, 2009).

¹² *SEC v. Galleon Mgmt., LP*, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009).

¹³ The other defendants in these cases were: (1) Galleon Management, LP (the hedge fund management firm that was managed by Rajaratnam); (2) Rajiv Goel (Rajaratnam's friend, and Managing Director at Intel Corp.); (3) Anil Kumar (Rajaratnam's friend, investor in several Galleon funds, and a director at McKinsey & Co.); (4) Danielle Chiesi (a portfolio manager at New Castle Funds LLC); (5) Mark Kurland (Senior Managing Director and General Partner at New Castle Funds, LLC); (6) Robert Moffat (a senior executive at IBM); (7) New Castle Funds, LLC (an investment adviser to hedge funds which was previously a part of Bear Stearns Asset Management); (8) Roomy Khan (a hedge fund consultant); (9) Deep Shah (a former Moody's analyst); (10) Ali Hariri (Vice President of Broadband Carrier Networking at Atheros, a "developer of semiconductor systems for network communication products"); (11) Schottenfeld Group LLC (a New York-based registered broker-dealer); (12) Zvi Goffer (a registered representative and proprietary trader at Schottenfeld during the period investigated); (13) David Plate (a registered representative and proprietary trader at Schottenfeld); (14) Gautham Shankar (registered representative and proprietary trader at Schottenfeld); (15) S2 Capital Management, LP (a New York-based unregistered hedge fund investment adviser); (16) Steven Fortuna (principal and founder of S2 Capital Management, LP); (17) Ali T. Far (Managing Member of Spherix Capital and Far & Lee, LLC, and previously worked for Galleon as a Managing Director, portfolio manager, and analyst.); (18) Choo-Beng Lee (Managing Member of Far & Lee, LLC., and co-founder of Spherix Capital) (19) Spherix Capital (a California-based, unregistered hedge-fund investment adviser established by Far and Lee); and (20) Far & Lee (trading entity created by Lee and Far before establishing Spherix Capital, LLC. SEC Complaint, SEC v. Galleon Mgmt., LP (No. 09-CV-0811-JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010). Excluding Rajaratnam and Galleon Management, LP, all of the defendants served as sources of material, non-public information to Rajaratnam who, in turn, traded on behalf of Galleon based upon such information. *Id.* All named individuals were defendants in criminal actions commenced by the USAO. *See, e.g.,* United States v. Rajaratnam, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Oct. 16, 2009); United States v. Moffat, No. 10 Cr. 270 (DAB) (S.D.N.Y. Oct. 16, 2009); United States v. Goel, No. 10 Cr. 90 (BSJ) (S.D.N.Y. Oct. 16, 2009); United States v. Hariri, No. 09

MAG. 2436 (S.D.N.Y. Nov. 4, 2009); and *United States v. Goffer*, No. 100 Cr. 56 (RJS) (S.D.N.Y. Nov. 5, 2009).

¹⁴ The USAO also indicted other defendants in a separate criminal action, as a result of information they obtained during the Rajaratnam investigation. *SEC v. Rajaratnam*, 622 F.3d 159, 164-65 (2d Cir. Sep 29, 2010). *See also* *United States v. Goffer*, 756 F.Supp.2d 588 (S.D.N.Y. 2011). The SEC filed a civil complaint against Rajaratnam and Rajat Gupta on October 26, 2011, separate from the complaint filed against Rajaratnam described above. This case was also based upon evidence obtained from wiretapped conversations, corroborated by investment changes. *SEC v. Gupta*, No. 11 Cv. 7566 (JSR) (S.D.N.Y. Oct. 26, 2011).

¹⁵ Pursuant to Section 10(b), it is “unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange – (b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange...any manipulative device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.” Securities Exchange Act of 1934 § 10(b) (2012), 15 U.S.C. § 78j(b) (2012).

¹⁶ Codified at 17 C.F.R. § 240.10b-5(a) (2012), which prohibits “any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange, (a) To employ any device, scheme or artifice to defraud...” Aside from insiders possessing a fiduciary duty, insider trading restrictions also apply to recipients of insider information from such insiders. *United States v. Rajaratnam*, 802 F.Supp.2d 491, 497-98 (S.D.N.Y. 2011) (citing *SEC v. Ballesteros Franco*, 253 F. Supp.2d 720, 726 (S.D.N.Y. 2003)).

¹⁷ Although both the civil and criminal complaints alleged violations of Section 10(b) of the Securities Exchange Act of 1934 (15 U.S.C. § 78j(b) (2012)), and Rule 10b-5 (codified at 17 C.F.R. § 240.10b-5(a) (2012)), the criminal complaint also alleged that the defendants had conspired to commit insider trading. *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Oct. 16, 2009).

¹⁸ SEC Complaint, *SEC v. Galleon Mgmt., LP* (No. 09-CV-0811-JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5,

2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010); United States v. Rajaratnam, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Oct. 16, 2009).

¹⁹ SEC Complaint, SEC v. Galleon Mgmt., LP (No. 09-CV-0811-JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²⁰ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²¹ Polycom is a corporation that “produces applications for voice, video and data networking”. SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²²Kronos is a “workforce management software company” that sells time tracking and payroll software to businesses. ABOUT KRONOS, <http://www.kronos.com/about/about-kronos.aspx> (last visited January 9, 2013); SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²³ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²⁴ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010). Khan also compensated Deep Shah, the Moody’s analyst who had provided this information, with \$10,000. Shah was reviewing Hilton’s creditworthiness in furtherance of the takeover. *Id.*

²⁵ As described by Shah, the contemplated Hilton takeover by the Blackstone Group would remove Hilton’s stock from the New York Stock Exchange, resulting in it becoming a private company. This tip was accurate. The Blackstone Group bought back all of Hilton’s stock at a premium. *Id.*

²⁶ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²⁷ Clearwire constructs and operates wireless and broadband networks worldwide. SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²⁸ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

²⁹ *Id.*

³⁰ *Id.*

³¹ “AMD is a global semiconductor company offering microprocessor, embedded processor, chipset and graphics products.” SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

³² *Id.*

³³ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

³⁴ *Id.*

³⁵ *Id.*

³⁶ SEC Complaint, SEC v. Galleon Mgmt., LP, No. 09 Cv. 8811 (JSR) (S.D.N.Y. Oct. 16, 2009), amended by First Amended Complaint (S.D.N.Y. Nov. 5, 2009), amended by Second Amended Complaint (S.D.N.Y. Jan. 29, 2010).

³⁷ The SEC filed a civil complaint against Rajaratnam and Rajat Gupta on October 26, 2011, separate from the complaint filed against Rajaratnam described above. This case was also based upon evidence obtained from wiretapped conversations, corroborated by investment changes. Gupta, a former Board Member of Procter & Gamble, and Goldman Sachs, as well as a former Director of McKinsey, was found to have provided Rajaratnam with material nonpublic information concerning Goldman Sachs and Procter & Gamble. SEC v. Gupta, No. 11 Cv. 7566 (JSR) (S.D.N.Y. Oct. 26, 2011). Gupta was found guilty of insider trading in the criminal action commenced by the USAO, and sentenced to 24 months’ imprisonment, and fined \$5 million. United States v. Gupta, No. 11 Cr. 907 (JSR), 2012 U.S. Dist. LEXIS 45610 (S.D.N.Y. March 26, 2012), *sentence imposed by* United States v. Gupta, No. 11 Cr. 907 (JSR), 2012 U.S. Dist. LEXIS 154226 (S.D.N.Y. Oct. 24, 2012).

³⁸ BLACK'S LAW DICTIONARY 769 (9th ed. 2009).

³⁹ 18 U.S.C. §§ 2510 (1), (2), (5), (12), (14), & (17) (2012).

⁴⁰ See, e.g. *Wong Sun v. United States*, 371 U.S. 471 (1963) (holding that oral evidence obtained from an unwarranted intrusion may be inadmissible as the result of an impermissible search).

⁴¹ *Berger v. New York*, 388 U.S. 41 (1967).

⁴² *Katz v. United States*, 389 U.S. 374 (1967).

⁴³ "The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized." U.S. CONST. amend. IV.

⁴⁴ *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967).

⁴⁵ *Berger v. New York*, 388 U.S. 41, 44-45 (1967).

⁴⁶ *Berger v. New York*, 388 U.S. 63-64 (1967).

⁴⁷ *Katz v. United States*, 389 U.S. 347, 353 (1967).

⁴⁸ *Katz v. United States*, 389 U.S. 347, 353 (1967).

⁴⁹ *Katz v. United States*, 389 U.S. 347, 352 (1967) (noting "[W]hat [petitioner] sought to exclude when he entered the booth was not the intruding eye – it was the uninvited ear").

⁵⁰ Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-22, Pub. L. 90-351 (1968), as amended by Electronic Communications Privacy Act, Pub. L. 99-508 (1986), Communications Assistance to Law Enforcement Act, Pub. L. 103-414 (1994), Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132 (1996), USA PATRIOT Act, Pub. L. 107-56 (2001), USA PATRIOT Additional Reauthorization Amendments Act of 2006, Pub. L. 109-178 (2006), Foreign Intelligence Surveillance Act ("FISA") Amendments Act of 2008, Pub. L. 110-261 (2008), FISA Sunsets Extension Act, Pub. L. 112-3 (2011), PATRIOT Sunsets Extension Act of 2011, Pub. L. 112-14 (2011).

⁵¹ Pub. L. 90-351 (1968).

⁵² *Id.*

⁵³ *Id.*

⁵⁴ The Electronic Communications Privacy Act, enacted in 1986, amended the Wiretap Act to include interception of electronic communications. Pub. L. 99-508 (1986).

⁵⁵ Notwithstanding the overall similarities between wiretap authorizations and conventional warrants, the Supreme Court in *Katz v. United States* noted that “a conventional warrant ordinarily serves to notify the suspect of an intended search” and that advance notice to a suspect of governmental intent to record his conversations would render such recordings useless. *Katz v. United States*, 389 U.S. 347, 355 (1967).

⁵⁶ 18 U.S.C. § 2511(2)(c) (2012).

⁵⁷ 18 U.S.C. § 2516 (2012).

⁵⁸ 18 U.S.C. § 2518(1) (2012).

⁵⁹ 18 U.S.C. § 2518(1)(b) (2012).

⁶⁰ 18 U.S.C. § 2518(1)(d); 18 U.S.C. § 2518(3).

⁶¹ 18 U.S.C. § 2518(1)(b)(iii).

⁶² 18 U.S.C. § 2518(1)(a).

⁶³ 18 U.S.C. § 2518(1)(c).

⁶⁴ 18 U.S.C. § 2518(4)(c) (2012).

⁶⁵ 18 U.S.C. § 2518(4)(b).

⁶⁶ 18 U.S.C. § 2518(4)(d).

⁶⁷ 18 U.S.C. § 2518(4)(e).

⁶⁸ 18 U.S.C. § 2518(5) (2012).

⁶⁹ 18 U.S.C. § 2517(5) (2012).

⁷⁰ 18 U.S.C. § 2517(1) (2012).

⁷¹ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *1-2 (S.D.N.Y. Nov. 29, 2010).

⁷² *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *8-23 (S.D.N.Y. Nov. 29, 2010); 18 U.S.C. § 2516(c) (2012).

⁷³ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *9-11 (S.D.N.Y. Nov. 29, 2010).

⁷⁴ *Id.* at *11-19.

⁷⁵ *Id.* at *17-19.

⁷⁶ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *23 (S.D.N.Y. Nov. 29, 2010).

⁷⁷ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *27-28 (S.D.N.Y. Nov. 29, 2010).

⁷⁸ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *35 (S.D.N.Y. Nov. 29, 2010).

⁷⁹ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *35 (S.D.N.Y. Nov. 29, 2010). Since the government established probable cause in furtherance of its wiretap application to wiretap Chiesi solely on recorded

conversations from the Rajaratnam wiretap, Chiesi's challenge that the wiretap authorization lacked probable cause failed. *Id.* at *52-53.

⁸⁰ 18 U.S.C. § 2518(1)(c) (2012); *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *52-53 (S.D.N.Y. Nov. 29, 2010).

⁸¹ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *53-54 (S.D.N.Y. Nov. 29, 2010) (citing *United States v. Concepcion*, 579 F.3d 214, 218 (2d Cir. 2009)).

⁸² *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *53-54 (S.D.N.Y. Nov. 29, 2010).

⁸³ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *98 -102 (S.D.N.Y. Nov. 29, 2010).

⁸⁴ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *98-100 (S.D.N.Y. Nov. 29, 2010).

⁸⁵ *United States v. Rajaratnam*, 2010 U.S. Dist. 143175, at *99-100 (S.D.N.Y. Nov. 29, 2010) (citing *United States v. Scott*, 436 U.S. 128 (1978)). Judge Holwell also rendered the minimization requirement inapplicable to calls that do not exceed two minutes in duration. *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *100 (S.D.N.Y. Nov. 29, 2010) (citing *United States v. Salas*, 07 Cr. 557 (JGK), 2008 U.S. Dist. LEXIS 92560, at *6 (S.D.N.Y. Nov 5, 2008). Danielle Chiesi independently challenged the minimization efforts on grounds that 155 wiretapped calls related only to personal issues; however, Judge Holwell rejected this argument, and noted that the minimization requirement does not limit lawful interception to only those conversations dealing only with criminal topics. *United States v. Rajaratnam*, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *101-102 (S.D.N.Y. Nov. 29, 2010).

⁸⁶ *United States v. Rajaratnam*, 802 F.Supp.2d 491, 495-96 (S.D.N.Y. Aug 16, 2011).

⁸⁷ *Id.* at 499-512.

⁸⁸ *United States v. Rajaratnam*, 802 F.Supp.2d 491, 511 (S.D.N.Y. Aug. 16, 2011); FED. R. EVID. 801(d)(2)(E).

⁸⁹ As Judge Holwell noted, Section 801(d)(2) of the Federal Rules of Evidence permits consideration of co-conspirator's statements; however, such statements alone will not establish "the existence of the conspiracy and the participation therein of the declarant and the party against whom the statement is offered." *United States v. Rajaratnam*, 802 F.Supp.2d 491, 511 (S.D.N.Y. Aug. 16, 2011); FED. R. EVID. 801(d)(2).

⁹⁰ *SEC v. Galleon Mgmt., LP*, 683 F.Supp.2d 316, 317 (S.D.N.Y. Feb. 9, 2010).

⁹¹ *Id.*

⁹² SEC v. Galleon Mgmt., LP, 683 F.Supp.2d 316, 318 (S.D.N.Y. Feb. 9, 2010).

⁹³ SEC v. Galleon Mgmt., LP, 683 F.Supp.2d 316, 318 (S.D.N.Y. Feb. 9, 2010) (referencing 18 U.S.C. § 2517(3)).

⁹⁴ SEC v. Galleon Mgmt., LP, 683 F.Supp.2d 316, 318 (S.D.N.Y. Feb. 9, 2010).

⁹⁵ *Id.* at 319.

⁹⁶ Securities Exchange Act of 1934 § 21(a)(1) (2012), 15 U.S.C. § 78u(a)(1) (2012). *See also* SEC News Room, Office of Public Affairs, *How*

Investigations Work,

www.sec.gov/new/newsroom/howinvestigationswork.html (last visited December 1, 2012).

⁹⁷ Securities Act of 1933, § 20(b) (2012), 15 U.S.C. § 77t(b) (2012); Securities Exchange Act of 1934 § 21(a)(1) (2012), 15 U.S.C. §§ 78u(c) – (e) (2012).

⁹⁸ Securities Act of 1933, § 20(b) (2012), 15 U.S.C. § 77t(b) (2012); Securities Exchange Act of 1934 § 21(d)(1) (2012), 15 U.S.C. § 78u(d)(1) (2012).

⁹⁹ United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 143175, at *3-4 (S.D.N.Y. Nov. 29, 2010).

¹⁰⁰ The efforts of both the USAO and the FBI in criminally investigating Rajaratnam resulted in his indictment. Indictment, United States v. Rajaratnam, No. 09 Cr. 1184 (RJH) (S.D.N.Y. Dec. 15, 2009).

¹⁰¹ *Id.*

¹⁰² *See, e.g.*, Securities Act of 1933 §§ 5, 11, 12, 15, 17 (2012); Securities Exchange Act of 1934 §§ 5, 9, 10, 18, 20, 20A, 21A (2012).

¹⁰³ Securities Exchange Act of 1934 § 23(a) (2012), 15 U.S.C. § 78j(b) (2012).

¹⁰⁴ Securities Exchange Act of 1934 §21(a)(1) (2012); Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1266 (2012).

¹⁰⁵ Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1266 (2012).

¹⁰⁶ *Id.* at 1267.

¹⁰⁷ Securities Exchange Act of 1934 §21(b) (2012), 15 U.S.C. § 78u(b) (2012).

¹⁰⁸ Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1267 (2012).

¹⁰⁹ Securities Exchange Act of 1934 § 21(e) (2012), 15 U.S.C. § 78u(e) (2012).

¹¹⁰ Securities Exchange Act of 1934 § 21(d)(3) (2012), 15 U.S.C. § 78u(d)(3) (2012).

¹¹¹ Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1268 (2012). Civil actions commenced by the SEC may seek the same remedies. *Id.* at 1269-72.

¹¹² Securities Exchange Act of 1934 §21(d)(1) (2012), 15 U.S.C. § 77t(b) (2012), 15 U.S.C. § 78u(d)(1) (2012).

¹¹³ Securities Exchange Act of 1934 §21(d)(1) (2012), 15 U.S.C. §78u(d)(1) (2012) (“The Commission may transmit such evidence as may be available concerning such acts or practices as may constitute a violation of any provision of this chapter or the rules or regulations thereunder to the Attorney General, who may, in his discretion, institute the necessary criminal proceedings under this chapter.”). Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1276 (2012); Scott Colesanti, Article, *Wall Street as Yossarian: The Other Effects of the Rajaratnam Insider Trading Conviction*, 40 HOFSTRA L. REV. 411, 424 & n.97 (2011).

¹¹⁴ Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1276 (2012).

¹¹⁵ *Id.*

¹¹⁶ Securities Exchange Act of 1934 §21(d)(1) (2012), 15 U.S.C. §78u(d)(1) (2012).

¹¹⁷ USAO Criminal Resource Manual, USAM, Title 9 – USAM 9, 2001, available at www.justice.gov/usao/eousa/a_reading_room/usam/title9/2mcrm.htm.

¹¹⁸ Rebecca Gross, Lauren Britsch, Kirk Goza & Jaclyn Epstein, Article, *Securities Fraud*, 49 AM. CRIM. L. REV. 1213, 1276 (2012).

¹¹⁹ Exec. Order No. 13519, Nov. 17, 2009, “Establishment of the Financial Fraud Enforcement Task Force”.

¹²⁰ *Id.*

¹²¹ *Id.*

¹²² *Id.*

¹²³ Exec. Order No. 13519, Nov. 17, 2009, “Establishment of the Financial Fraud Enforcement Task Force”.