Pace Law Review

Volume 33
Issue 2 *Spring 2013*

Article 5

April 2013

New Methods of Financial White-Collar Criminal Investigation and Prosecution: The Spillover of Wiretaps to Civil Enforcement Proceedings

Andrew P. Atkins
Office of the Comptroller of the Currency

New Methods of Financial White-Collar Criminal Investigation and Prosecution: The Spillover of Wiretaps to Civil Enforcement Proceedings

Andrew P. Atkins*

I. Introduction

A new era of white-collar criminal enforcement has emerged from the 2008 to 2010 financial crisis.[1] Nowhere is this more evident than in the field of financial crimes.[2] In what has been described as "a tactical sea change in its pursuit of financial malefactors,"[3] new prosecutors and regulators are jumping into the sphere of financial crime enforcement,[4] and the federal government, primarily through the Department of Justice

* Andrew P. Atkins is an attorney at the Office of the Comptroller of the Currency ("OCC"). Before joining the OCC, he clerked for Justice Mark D. Martin of the Supreme Court of North Carolina. The author would like to thank Jennifer Peterson for her comments and edits. The opinions expressed in this article are solely those of the author and do not necessarily represent the opinions of the OCC. Any errors or omissions are solely those of the author.

1. Mei Lin Kwan-Gett, *Developing Effective Strategies in White Collar Cases*, *in* MANAGING WHITE COLLAR LEGAL ISSUES: LEADING LAWYERS ON UNDERSTANDING RECENT NOTABLE CASES, ESTABLISHING KEY DEFENSE STRATEGIES, AND DEVELOPING CLIENT RELATIONSHIPS (INSIDE THE MINDS) 91, 92 (Aspatore Books 2010) (stating there is "increased emphasis on white collar crime" and discussing increased attention by prosecutors and regulators); Robert G. Morvillo & Robert J. Anello, *Overview of Federal Wiretap Law in White-Collar Cases*, N.Y. L.J. (Feb. 1, 2011), http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202479830264&Overview_of_Federal_Wiretap_Law_in_WhiteCollar_Cases&slreturn=20130127181642 (discussing new investigative techniques used by the federal government to investigate financial crimes); *Economic Crisis and Market Upheavals*, NY TIMES, http://topics.nytimes.com/top/reference/timestopics/subjects/c/credit_crisis/index.html (last visited Nov. 13, 2012) (discussing the financial crisis and its timeline).

2. *See* Morvillo & Anello, *supra* note 1.

3. Abigail Field, *Sorry, Judge Rakoff: You Can't Give the SEC the* Galleon *Wiretaps . . . Yet*, DAILYFINANCE (Sept. 30, 2010, 3:30 PM), http://www.dailyfinance.com/story/investing/galleon-wiretaps-insider-trading-rakoff-overturned-sec-justice-trial/19655156/.

4. Kwan-Gett, *supra* note 1, at 92. These new prosecutors include state and local prosecutors, especially within the state of New York. *Id.*

("DOJ"), is using new investigative techniques.[5] Most notable among these new investigative techniques is the use of court-authorized wiretaps.[6] Traditionally used to prosecute organized crime, gangs, terrorists,[7] and drug cartels,[8] prosecutors are now aggressively using wiretaps to target insider trading.[9] The federal government is now truly going after the "Wall Street mob."[10]

While the use of wiretaps by the federal government to target insider trading rings is certainly interesting in its own right, perhaps the more interesting issue is how the use of wiretaps to investigate and prosecute financial crimes will affect parallel civil enforcement proceedings.[11] This Article will analyze if and how the contents of court-authorized wiretaps obtained for use in criminal proceedings may also be used by regulatory agencies in their civil enforcement proceedings. Presumably, any regulatory agency targeting civil enforcement of an offense with a parallel, or near parallel, criminal offense could take advantage of court-authorized wiretaps.[12] However, for simplicity, this Article will focus on the use of wiretaps by the Securities and Exchange Commission ("SEC") in its civil enforcement proceedings. In so doing, this Article will use the civil and criminal insider trading charges against Raj Rajaratnam, Galleon Management, and Danielle Chiesi as an illustrative example.[13] Although some of the issues presented by these

5. Morvillo & Anello, *supra* note 1.

6. Preet Bharara, U.S. Attorney for the S. Dist. of N.Y., Prepared Remarks for U.S. Attorney Preet Bharara: U.S. v. Raj Rajaratnam, et al.; U.S. v. Dainielle [sic] Chiesi, et al. Hedge Fund Insider Trading Takedown (Oct. 16, 2009).

7. Gail Shifman, *Wall Street Meets "The Wire,"* WHITE COLLAR CRIME PROF BLOG (Oct. 19, 2009), http://lawprofessors.typepad.com/whitecollarcrime_blog/2009/10/wall-street-meets-the-wire.html.

8. Bharara, *supra* note 6.

9. *Id.*

10. *See* The Truth Shall Set Ye Free, *Wall Street Mob Set to Pay Themselves $144 Billion*, DAILY KOS (Oct. 15, 2010, 9:12 AM), http://www.dailykos.com/story/2010/10/15/900441/-Wall-Street-mob-set-to-pay-themselves-144-BILLION (representing public sentiment that behavior by Wall Street firms and executives are comparable to that of the Mob).

11. *See* SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010). Here, the SEC sought the wiretaps used by the USAO in the parallel criminal proceeding for insider trading for its use in its civil enforcement proceeding. *Id.* at 164.

12. *See* Fleming v. United States, 547 F.2d 872 (5th Cir. 1977) (allowing the IRS to introduce wiretap recordings obtained in a criminal investigation in a parallel civil enforcement proceeding); Kwan-Gett, *supra* note 1, at 97 (mentioning the SEC and the CFTC). It is also likely that other agencies could take advantage of wiretap recordings in their enforcement actions.

13. SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010) (civil case); United States v.

two cases have been somewhat mooted by the ruling in the *Rajaratnam* criminal case, where the wiretaps were found to be lawfully intercepted,[14] Chiesi's subsequent guilty plea,[15] the Second Circuit Court of Appeals' ruling that the SEC does have an interest in discovering the wiretap recordings,[16] and Rajaratnam's ultimate conviction,[17] the questions the cases initially raised are worth examining. Continued examination is especially necessary as these and other wiretap recordings are likely to be used in future criminal and civil cases.[18] This analysis will help to more clearly illustrate how the contents of court-authorized wiretaps may be used in future civil enforcement proceedings by the SEC and other regulatory agencies with the power to bring civil enforcement actions.[19] Nonetheless, it is important to note at the outset that the jurisdictional questions raised by this case are outside the scope of this article.[20]

Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010) (criminal case).

14. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *1 (S.D.N.Y. Nov. 24, 2010) (ruling that the wiretaps were lawfully intercepted).

15. Patricia Hurtado et al., *Danielle Chiesi Pleads Guilty to Insider Trading in Galleon Investigation*, BLOOMBERG (Jan. 19, 2011, 5:55 PM), http://www.bloomberg.com/news/2011-01-19/danielle-chiesi-pleads-guilty-to-insider-trading-in-galleon-group-probe.html [hereinafter Hurtado et al.] (describing the circumstances of Chiesi's guilty plea).

16. SEC v. Rajaratnam, 622 F.3d 159, 180-82 (2d Cir. 2010).

17. Peter Lattman & Azam Ahmed, *Hedge Fund Billionaire is Guilty of Insider Trading*, NY TIMES (May 11, 2011, 10:50 AM), http://dealbook.nytimes.com/2011/05/11/rajaratnam-found-guilty/ [hereinafter *Hedge Fund Billionaire*].

18. *See* Peter Lattman & Azam Ahmed, *Rajat Gupta Convicted of Insider Trading*, NY TIMES (Jun. 15, 2012, 12:05 PM), http://dealbook.nytimes.com/2012/06/15/rajat-gupta-convicted-of-insider-trading/ [hereinafter *Rajat Gupta*] (discussing the criminal case against Rajat Gupta, who was convicted of insider trading for tipping Rajaratnam, using wiretap recordings of conversations between the two of them). Gupta made similar arguments to Rajaratnam as he sought to suppress the wiretap communications at his trial. *See* United States v. Gupta, No. 11 Cr. 907(JSR), 2012 WL 1066817 (S.D.N.Y. Mar. 27, 2012).

19. While it is possible that some of these principles could be used by private civil litigants to obtain wiretaps, it is far less likely due to the privacy interests at stake. *See* Nat'l Broad. Co. v. U.S. Dep't of Justice, 735 F.2d 51, 54 (2d Cir. 1984) ("[T]urning Title III into a general civil discovery mechanism would simply ignore the privacy rights of those whose conversations are overheard."); *see also* SEC v. Rajaratnam, 622 F.3d 159, 176-79 (2d Cir. 2010) (discussing the balancing of right of access against privacy interests and indicating that the fact that the SEC is a government agency, not a private civil litigant, is important to the balancing).

20. These jurisdictional issues include whether there is interlocutory jurisdiction for discovery rulings, whether mandamus review is appropriate, and what constitutes abuse

To have a proper understanding of the questions presented by the Rajaratnam cases, a basic understanding of the criminal and civil cases is necessary. Accordingly, Part II will briefly discuss the facts of the two cases, the investigation, and relevant court rulings. Part III will briefly discuss the history and relevant provisions of Title III of the Omnibus Crime Control and Safe Streets Act ("Title III"),[21] the "comprehensive scheme" for regulating the authorization and disclosure of wiretaps.[22] Part IV will discuss the primary theories the SEC could have used to obtain wiretap recordings for use in its civil enforcement proceeding, namely disclosure from the U.S. Attorney's Office ("USAO") and from the civil defendant. This Part will also discuss timing as a factor for disclosure. Finally, in Part V, I will conclude with policy recommendations regarding how the issue can be more clearly resolved by congressional action and what the SEC can do to increase the likelihood of disclosure during discovery or otherwise.

The use of wiretaps is currently being analyzed under two sets of rules, one within Title III and one outside Title III.[23] Congress could simplify this area of the law, protect privacy, and strengthen civil enforcement efforts by reexamining and amending Title III. Specifically, Congress should address the concerns represented by the many balancing tests developed by the courts since enactment of Title III and more clearly allow regulatory agencies with civil enforcement power to receive wiretap recordings by deeming certain actors within these agencies investigative officers.[24] These amendments could fully return the regulation of wiretaps and disclosure of wiretap recordings to the Title III framework, thus avoiding judicial balancing outside the statutory confines. If Congress does not address these issues, civil enforcement agencies should take steps on their own to simplify their path to obtaining wiretap materials, such as conditioning investigative aid on full disclosure.

of discretion under these circumstances. *See generally* SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010).

21. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522 (2006) (while the statute is often referred to as the "Wiretap Act," this Article will refer to the statute as "Title III"–the name commonly used in federal criminal practice).

22. Gelbard v. United States, 408 U.S. 41, 46 (1972).

23. *See infra* Part III (discussing Title III and the balancing framework that has developed outside of Title III).

24. Under my proposal, regulatory agencies with civil enforcement power would not be given authority to petition courts to authorize wiretaps.

II. *United States v. Rajaratnam* and *SEC v. Rajaratnam*

At the time, *United States v. Rajaratnam*,[25] along with the related cases, was the largest hedge fund insider trading case ever brought criminally,[26] and was arguably the largest insider trading case of any kind.[27] When first announced, illicit profits were thought to be around $20 million;[28] however, more recent estimates by the SEC have increased that number to more than $52 million.[29] The insider-trading scheme was far-reaching and deep. In addition to hedge fund managers and employees like Raj Rajaratnam and Danielle Chiesi, the scheme included directors and executives of many well-known corporations including Intel Capital, IBM, McKinsey and Company, and Goldman Sachs.[30] In total, approximately twenty-one people were charged, many of whom have already pleaded guilty or been convicted.[31] The issues presented by these two parallel proceedings require a basic understanding of the facts of the insider-trading scheme, the USAO's and SEC's investigations, and preliminary court decisions, which will be discussed in Part II.

A. *Facts Surrounding the Galleon Insider-Trading Scheme*

The Galleon insider-trading scheme involved "widespread and repeated insider trading" at two major hedge funds: Galleon Management, managed by Raj Rajaratnam, and New Castle LLC, where Danielle Chiesi was a portfolio manager.[32] The scheme was allegedly led by Rajaratnam and Chiesi and involved trading on material, non-public information of at least fourteen public companies,[33] including companies

25. No. 09 Cr. 1184(RJH), 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010).

26. Bharara, *supra* note 6.

27. Kwan-Gett, *supra* note 1, at 93.

28. Bharara, *supra* note 6.

29. Patricia Hurtado, *SEC Seeks Wiretaps from Rajaratnam for Civil Case After Judge Admits Them*, BLOOMBERG (Dec. 20, 2010, 3:02 PM), http://www.bloomberg.com/news/2010-12-20/sec-seeks-wiretaps-from-rajaratnam-for-civil-case-after-judge-admits-them.html.

30. Bharara, *supra* note 6; *see also Rajat Gupta*, *supra* note 18.

31. Kwan-Gett, *supra* note 1, at 93; *Hedge Fund Billionaire*, *supra* note 17 ("Mr. Bharara noted that over the last 18 months, his office had charged 47 people with insider trading; Mr. Rajaratnam is the 35th to be convicted.").

32. Complaint at 2, SEC v. Galleon Mgmt., LP, No. 1:09-CV-08811 (S.D.N.Y. Oct. 16, 2009), 2009 WL 3329053 [hereinafter Galleon Complaint].

33. Brief of the Securities and Exchange Commission at 2, SEC v. Rajaratnam, Nos. 10-462-cv(L), 10-464-cv(Con) (2d Cir. May 24, 2010), 2010 WL 2584232

such as Google, Hilton Hotels Corporation, and Intel.[34] The inside information originated from high-level executives and consultants at prominent companies[35] and concerned "market moving events such as quarterly earnings announcements, takeovers, and material contracts."[36] Rajaratnam received the tips from multiple tippers, who themselves anticipated getting reciprocal inside tips from Rajaratnam and Chiesi in the future, employment by Galleon Management, or substantial kickbacks.[37] The USAO and the SEC alleged that Rajaratnam "exploited [this] corrupt network"[38] of tippers and tippees since 2003 to realize significant monetary gains.[39] The USAO unsealed criminal complaints charging Rajaratnam, Chiesi, and other defendants with securities fraud and conspiracy on October 16, 2009, the same day the SEC filed its civil complaint based on the same alleged activities.[40] Ultimately, many of the defendants, including Danielle Chiesi, pleaded guilty to both civil and criminal charges.[41] Rajaratnam was convicted of the criminal charges against him and, as part of the civil enforcement proceeding, ordered to pay a record $92.8 million in penalties.[42]

[hereinafter SEC Brief].

34. Galleon Complaint, *supra* note 32, at 2.

35. *See id.*

36. SEC Brief, *supra* note 33, at 7.

37. Galleon Complaint, *supra* note 32, at 10 (alleging a tipper provided Rajaratnam insider information with the hopes of being employed by Galleon and in anticipation of future inside tips); Associated Press, *Gov't Witness: Galleon Founder Paid for Tips*, CBS MONEYWATCH (Mar. 14, 2011, 12:45 PM), http://www.cbsnews.com/stories/2011/03/14/business/main20042916.shtml?tag=mncol;1st;1 (alleging that one tipper, Anil Kumar, was promised payments of $500,000 per year as well as a $1 million kickback in exchange for inside information).

38. Bob Van Voris, et al., *Rajaratnam Exploited 'Corrupt Network' For Trades, Prosecutor Tells Jurors*, BLOOMBERG (Mar. 10, 2011, 12:01 AM), http://www.bloomberg.com/news/2011-03-09/rajaratnam-exploited-a-corrupt-network-of-people-prosecutor-tells-jury.html.

39. Associated Press, *supra* note 37.

40. SEC v. Rajaratnam, 622 F.3d 159, 164-65 (2d Cir. 2010).

41. Hurtado et al., *supra* note 15; *SEC Reaches Settlement with Insider Trading Convict Danielle Chiesi*, CBS NEW YORK (July 14, 2011, 7:30 AM), http://newyork.cbslocal.com/2011/07/14/sec-reaches-settlement-with-insider-trading-convict/.

42. SEC v. Rajaratnam, 822 F. Supp. 2d 432, 436 (S.D.N.Y 2011); Chad Bray, *Rajaratnam Ordered to Pay Record SEC Penalty*, WALL ST. J., Nov. 9, 2011, http://online.wsj.com/article/SB10001424052970204554204577026372138523912.html.

B. *USAO and SEC Investigations*

When Preet Bharara, the United States Attorney for the Southern District of New York, announced that the USAO had unsealed criminal complaints against Rajaratnam, Chiesi, and four other defendants, he was flanked by Joe Demarest, the Assistant Director-in-Charge of the New York Division of the FBI, and Robert Khuzami, the Director of Enforcement for the SEC.[43] Mr. Bharara called them "our two law enforcement partners in this case,"[44] signaling how intertwined their investigative efforts had been.[45]

The USAO's investigation spanned over two years and included the use of informants, cooperating witnesses, consensual monitoring, and court-authorized wiretaps.[46] Nonetheless, the USAO relied heavily on the SEC's investigation, which used more traditional techniques to track the insider-trading scheme.[47] In fact, before the wiretaps were made, the SEC's investigation "was the bedrock of the prosecutor's own criminal investigation,"[48] as the USAO and the FBI had access to all the SEC's files.[49] The USAO's investigation of Rajaratnam and Chiesi began in 2007 and 2008, respectively.[50] However, it did not seek to use wiretaps targeting either Rajaratnam or Chiesi until March 2008.[51] Much of the evidence the USAO gathered before applying for wiretaps was gathered through the use of a confidential informant, Roomy Kahn, who had been cooperating with the FBI in the investigation of Rajaratnam, after she was investigated for insider trading violations of her own, including

43. Bharara, *supra* note 6.

44. *See id.*

45. *See* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *15-23 (S.D.N.Y. Nov. 24, 2010).

46. Shifman, *supra* note 7.

47. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *1 (S.D.N.Y. Nov. 24, 2010). This became an issue during the wiretap suppression hearing, since the USAO failed to include the extent of the SEC's investigation, and their reliance, on the wiretap application. *See generally id.*

48. *Id.* at *1.

49. *Id.* at *15.

50. *Id.* at *2.

51. *Id.* The USAO also used wiretaps against defendants named in separate actions, even though they were involved in the same underlying insider-trading scheme. *See* Brief for the United States of America as Amicus Curiae in Support of the Securities and Exchange Commission at 6, SEC v. Rajaratnam, Nos. 10-462-cv(L), 10-464-cv(CON) (2d Cir. June 1, 2010), 2010 WL2584233.

providing tips to Rajaratnam.[52] The wiretaps provided substantially more information over the sixteen-month period.[53] They netted 18,150 communications involving over 550 people.[54] Those communications were intercepted from ten separate telephones, including home, office, and mobile lines.[55]

On the other hand, the SEC's investigation relied entirely on conventional investigative techniques.[56] Though the SEC's investigation was relatively successful, "[it] had . . . failed to fully uncover the scope of Rajaratnam's alleged insider trading ring . . . ."[57] The SEC had compiled a plethora of information through its investigation.[58] The information consisted of millions of documents and witness interviews that SEC employees had gathered through the use of the SEC's regulatory subpoena power.[59] These documents included trading records, investor lists, emails, and Rajaratnam's contact lists, hard drive, bank records, and calendar.[60] The SEC even deposed Rajaratnam at least once.[61] Furthermore, the SEC issued 221 subpoenas to various banks, clearing houses, telephone companies, and securities issuers.[62] An analysis of these documents strongly implied that Rajaratnam was receiving or giving inside information by telephone.[63]

The SEC and the USAO were "'partners' in the investigation."[64] Besides having access to the SEC's files, the USAO, the FBI, and the SEC had "numerous meetings" to "discuss the course of [the] investigation."[65] The SEC regularly "kept the criminal authorities up to speed" and provided particularly important documents and chronologies

52. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *9-12 (S.D.N.Y. Nov. 24, 2010).

53. *See* SEC v. Rajaratnam, 622 F.3d 159, 165 (2d Cir. 2010).

54. *Id*. Most of these communications are still non-public and have not been released to the SEC or used in non-redacted court documents. *Id*. at 166.

55. *Id*. at 165.

56. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *1 (S.D.N.Y. Nov. 24, 2010).

57. *Id.*

58. *See id*. at *15.

59. *See id*. at *16.

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

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

65. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *15 (S.D.N.Y. Nov. 24, 2010).

outlining trading patterns and conversations.[66] "[T]he USAO and FBI either knew about or had access to 'the best of what the SEC could produce.'"[67] Despite the fact that the SEC, the USAO, and the FBI cooperated throughout the investigation,[68] the SEC never received the wiretap recordings during the course of that investigative cooperation.[69]

C. *Court Decisions*

Because issues of timing can become relevant to the Title III analysis,[70] a brief discussion of the civil and criminal cases against Rajaratnam and Chiesi is necessary. However, this section will not attempt to provide a detailed analysis of either case, but instead will focus on a general overview of the rulings in each case and the timing of the rulings in relation to each other.

As previously stated, the SEC filed its civil complaint against Rajaratnam and Chiesi the same day the USAO unsealed its criminal complaints charging them with securities fraud and conspiracy.[71] The SEC's civil complaint was assigned to Judge Jed Rakoff and the criminal case to Judge Richard Holwell.[72] Both the civil complaint and the criminal charges were based on the same allegedly illegal conduct.[73]

Issues of timing often arise in white-collar cases, as they did here, because civil suits commonly get to court more quickly than the parallel criminal proceedings, though the criminal case will often be resolved more quickly than the civil case once it gets to court.[74] Shortly after the criminal complaints were unsealed, and before indictment, the USAO disclosed wiretap communications to Rajaratnam and Chiesi according to

66. *Id.* (internal citations omitted).

67. *Id.* (internal citations omitted).

68. *Id.* at *16.

69. SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316, 317 (S.D.N.Y. 2010). The USAO did inadvertently disclose a small set of tapes to the SEC, though they were returned without being used. *Id.* at 319 n.2.

70. For instance, wiretapped communications not related to an offense specified in the wiretap authorization cannot be disclosed pursuant to subsections (1), (2), or (3) without a ruling of legality by a judge of competent jurisdiction. 18 U.S.C. § 2517(5) (2006).

71. SEC v. Rajaratnam, 622 F.3d 159, 164-65 (2d Cir. 2010).

72. *Id.* at 165. It is also important to note that another criminal case, based on the same allegations, was assigned to Judge Richard Sullivan. United States v. Goffer, 756 F. Supp. 2d 588 (S.D.N.Y. 2011).

73. SEC v. Rajaratnam, 622 F.3d 159, 165 (2d Cir. 2010).

74. Kwan-Gett, *supra* note 1, at 5.

criminal discovery rules, and did so without a protective order.[75] Because the USAO had not disclosed the contents of the wiretaps to the SEC during the investigation, the SEC sought production of the wiretaps through civil discovery.[76] Rajaratnam and Chiesi, however, opposed the discovery request arguing that Title III precluded the disclosure of the contents to anyone but co-defendants.[77] In his February 9, 2010 order, Judge Rakoff compelled discovery of the recordings subject to a protective order, stating that the recordings were "highly relevant" and that any privacy interest protected by Title III could be adequately protected through the protective order preventing further disclosure.[78] Judge Rakoff declined to rule on the legality of the wiretaps.[79] He also appeared resolute about the fact that the civil case would move forward despite any delay in the criminal case.[80]

Rajaratnam and Chiesi appealed Judge Rakoff's order to the Second Circuit Court of Appeals, which granted a stay in the discovery order pending appeal.[81] The Second Circuit concluded that it had "no interlocutory jurisdiction to review the order,"[82] but did find they had the power to review a "novel and significant question of law . . . whose resolution will aid in the administration of justice" through a writ of mandamus.[83] More importantly, the Second Circuit held that the SEC did have a right to discover the wiretap recordings, but that Judge Rakoff would be unable to properly balance the public interest in discovery

75. SEC v. Rajaratnam, 622 F.3d 159, 165 (2d Cir. 2010); SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316, 317-18 (S.D.N.Y. 2010).

76. *Galleon Mgmt., LP*, 683 F. Supp. 2d at 317.

77. *Id*. at 317-18. While the defendants claimed Title III prohibited them from disclosing the communications to the SEC, it is unclear why they believed it permitted disclosure to the co-defendants. *Id.* at 318 ("[Defendants] proved unable to cite any statutory authority for this restriction.").

78. *Id*. at 318-19.

79. *Id*. at 319.

80. *See id*. (explaining that "the trial of this action is firmly set for August 2, 2010"); SEC v. Rajaratnam, 622 F.3d 159, 166 (2d Cir. 2010) (affirming that "because of the strong public interest in having cases of this kind move forward promptly" an adjournment would not be granted until after the criminal case was resolved).

81. SEC v. Rajaratnam, 622 F.3d 159, 166 (2d Cir. 2010). At that point, Judge Rakoff concluded that resolution of wiretap issues was unlikely to occur before the civil trial, and granted an adjournment. *Id.*

82. *Id*. at 168.

83. *Id*. at 177. (quoting *In re* City of New York, 607 F.3d 923, 939 (2d Cir. 2010) (internal citations omitted)). Whether the Second Circuit's use of mandamus review is appropriate is certainly debatable, as it required the court to find that Judge Rakoff abused his discretion in ordering disclosure. *Id*. at 171. However, the jurisdictional issues are outside the scope of this paper.

against the relevant privacy interests before the legality of the wiretaps was determined by Judge Holwell.[84] In so doing, the Second Circuit discussed Title III in depth and reaffirmed that "Title III does not prohibit all disclosures of legally intercepted wire communications that it does not expressly permit . . . ."[85] Accordingly, the SEC would have to wait for the suppression hearings in the criminal case before they could renew their motion to discover the recordings.[86]

Judge Holwell did not issue the suppression decision until November 24, 2010.[87] In that order, he stated that the wiretaps of both Rajaratnam and Chiesi were legally obtained.[88] More specifically, Judge Holwell decided that because Title III permitted wiretaps to investigate wire fraud,[89] the government could use wiretaps to investigate insider-trading schemes using telephones as long as the interceptions were "incidental."[90] In addressing legality, Judge Holwell had to determine whether there was probable cause to issue the wiretap order.[91] This issue was complicated by the fact that the USAO had not given an accurate and complete description of their informant's credibility and reliability, but ultimately Judge Holwell decided that there was sufficient evidence to establish probable cause with regard to both Rajaratnam and Chiesi.[92] Judge Holwell also had to address whether wiretaps were necessary or whether traditional methods of investigation would suffice.[93] Again, the issue was complicated because the USAO failed to disclose the extent of the SEC's investigation and their cooperation with the USAO's investigation.[94] Nonetheless, he decided that the government did meet its burden of necessity, since it need not exhaust every investigative technique[95] and the facts were "minimally adequate" to justify the

84. *Id.* at 180.

85. *Id.* at 176. The circuit split on this part of the decision will be discussed in greater depth in Part III.B.

86. *See* Field, *supra* note 3.

87. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010).

88. *See generally id. See also* Part III *infra* (discussing the Title III issues raised in Judge Holwell's opinion).

89. 18 U.S.C. § 2516(1)(c) (2006).

90. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *3-6 (S.D.N.Y. Nov. 24, 2010).

91. *Id.* at *6.

92. *Id.* at *13.

93. *Id.* at *14.

94. *Id.* at *15-18.

95. *Id.* at *14.

conclusion that traditional techniques would not be fully effective.[96] Finally, Judge Holwell had to determine whether the government properly minimized the interception of non-relevant recordings, which could lead to suppression if not properly done.[97] Judge Holwell quickly found that the government was "objectively reasonabl[e] under the circumstances," despite the fact that some non-relevant recordings were intercepted.[98] Accordingly, he denied the motions to suppress, finding that the wiretaps were legally intercepted.[99]

Chiesi and certain other defendants pleaded guilty to their criminal charges shortly after the suppression motion was dismissed.[100] Rajaratnam and Chiesi's civil trial had been delayed, though Judge Rakoff had again ordered them to turn over relevant wiretap recordings to the SEC.[101] Rajaratnam was subsequently convicted of all criminal charges against him.[102] Ultimately, Rajaratnam agreed that the underlying criminal convictions estopped him from contesting civil liability for insider trading.[103] As a result, the issues addressed during the civil enforcement proceeding were limited to the calculation of damages, thus rendering the discoverability and admissibility of wiretap recordings irrelevant.[104] Chiesi settled her civil suit with the SEC for $540,000,[105] again mooting the wiretap issue in that case. Nevertheless, the question remains as to whether discovery and introduction of the wiretap recordings would be permissible if a civil defendant had not yet been criminally convicted or acquitted.

96. *Id.* at *26.

97. *Id.*

98. *Id.* at *28.

99. *Id.*

100. *Judge: Rajaratnam Must Turn Over Wiretaps to SEC*, FINALTERNATIVES (Feb. 2, 2011 10:35 AM), http://www.finalternatives.com/node/15397.

101. *Id.*

102. United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2012 WL 362031, at *1 (S.D.N.Y Jan. 31, 2012).

103. SEC v. Rajaratnam, 822 F. Supp. 2d 432, 433 (S.D.N.Y 2011).

104. *See generally id.*

105. SEC v. Galleon Mgmt., LP, 09 Civ. 8811(JSR), 2011 WL 2695431 (S.D.N.Y. July 11, 2011); Danielle Chiesi, Investment Advisers Act Release No. 3251, 2011 WL 2956680 (July 22, 2011).

III. Title III of the Omnibus Crime Control and Safe Streets Act

A. *Background*

Title III[106] is a "comprehensive statute" with which Congress attempted to regulate the "interception and disclosure of wire and oral communications."[107] It has a "dual purpose."[108] First, it seeks to protect the privacy rights of individuals and their Fourth Amendment rights.[109] Second, it seeks to provide "a uniform basis" for the authorization of the interception of wiretap communications.[110] Title III was adopted following the Supreme Court decision *Katz v. United States*,[111] which subjected electronic eavesdropping to Fourth Amendment protections.[112] The primary purpose of Title III was to "combat organized crime."[113] Accordingly, it attempted to "preserve as much as could be preserved of the privacy of communications, consistent with the legitimate law enforcement needs that the statute also sought to effectuate."[114] It is important to note at the outset that Title III does not regulate the disclosure of information that is publicly available, because "one cannot 'disclose' what is already in the public domain."[115]

B. *Court Decisions*

The comprehensiveness of Title III is somewhat debatable in light of the many court decisions that introduced balancing tests to qualify its reach.[116] Title III clearly forbids disclosure of wiretap evidence gained in

106. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522 (2006).

107. United States v. Cianfrani, 573 F.2d 835, 855 (3d Cir. 1978).

108. United States v. Torres, 751 F.2d 875, 881 (7th Cir. 1984).

109. United States v. Masciarelli, 558 F.2d 1064, 1066 (2d Cir. 1977).

110. *Torres*, 751 F.2d at 881 (quoting S. REP. NO. 1097, at 66 (1968)).

111. 389 U.S. 347 (1967).

112. *Torres*, 751 F.2d at 881.

113. *Id.* (quoting S. REP. NO. 1097, at 70 (1968) (internal quotations omitted)).

114. United States v. Cianfrani, 573 F.2d 835, 856 (3d Cir. 1978).

115. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 546 (2001) (Rehnquist, C.J., dissenting).

116. *See, e.g.*, Gardner v. Newsday, Inc., 895 F.2d 74, 75 (2d Cir. 1990); *In re* N.Y. Times Co. (*New York Times I*), 828 F.2d 110, 113 (2d Cir. 1987); *In re* Globe Newspaper Co., 729 F.2d 47, 56-58 (1st Cir. 1984).

violation of the Act.[117] Some circuit court decisions have gone on to say that it "implies that what is not permitted is forbidden . . . ."[118] However, other circuits have ruled that that view "is not a helpful guide to statutory interpretation"[119] and does not apply to Title III.[120] The Supreme Court has not yet ruled on this circuit split. But this debate on the maxims of statutory interpretation is paramount in determining what is permitted and prohibited by Title III and whether it truly is a comprehensive statutory framework governing wiretaps and wiretap recordings.[121]

Also relevant to the debate of comprehensibility is the extent to which other interests have limited the goals of Title III. One such interest is the qualified right of access.[122] This right of access is based on the First Amendment and the common law.[123] Courts have held that this right of access must be balanced against privacy rights.[124] This balancing test has been used in the context of court documents containing Title III evidence,[125] as well as court proceedings where Title III evidence would be introduced.[126] As a result, the public, often media entities, has been able to obtain Title III materials when Title III would otherwise appear to

117. 18 U.S.C. § 2511(1)(c) (2006).

> (1) Except as otherwise specifically provided in this chapter any person who-- . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Id. See also Fultz v. Gilliam, 942 F.2d 396, 401 (6th Cir. 1991).

118. United States v. Dorfman, 690 F.2d 1230, 1232 (7th Cir. 1982); *see Fultz*, 942 F.2d at 402.

119. United States v. Torres, 751 F.2d 875, 880 (7th Cir. 1984).

120. *See Gardner*, 895 F.2d at 77. The Second Circuit continued to rely on its precedent in *SEC v. Rajaratnam*, 622 F.3d 159, 176 (2d Cir. 2010).

121. Courts have reached very different results depending on their decision as to what Title III implies. *Compare Dorfman*, 690 F.2d at 1230-35, *with Gardner*, 895 F.2d at 74-79.

122. *Gardner*, 895 F.2d at 75; *In re* N.Y. Times Co. (*New York Times I*), 828 F.2d 110, 113 (2d Cir. 1987); *In re* Globe Newspaper Co., 729 F.2d 47, 56-58 (1st Cir. 1984).

123. *Gardner*, 895 F.2d at 78.

124. *Id.* at 74; United States v. Cianfrani, 573 F.2d 835, 851 (3d Cir. 1978).

125. *See, e.g.*, *Gardner*, 895 F.2d at 75-76.

126. *See, e.g.*, *In re Globe Newspaper Co.*, 729 F.2d at 56-58.

prohibit disclosure of those materials.[127] Since this balancing only takes account of the privacy interests addressed in Title III, not the prohibitions themselves, and balances them against other interests, it appears that the decision of whether disclosure is permissible lies outside the Title III framework.[128]

The First Amendment was also implicated in *Bartnicki v. Vopper*,[129] where a party broadcasted illegal wiretap recordings over the radio.[130] In *Bartnicki*, the Supreme Court held that in cases that "implicate[] the core purposes of the First Amendment . . . privacy concerns give way when balanced against the interest in publishing matters of public importance."[131] While the application of the balancing of the public interest against privacy interests does not necessarily lead to the conclusion that Title III wiretap evidence will always or frequently be disclosed to the public,[132] it does raise the question of whether Congress actually "performed all of the balancing necessary of the public interest in law enforcement against the privacy interests of citizens."[133] It is apparent that the court system is still doing some balancing with Title III, including balancing it against Constitutional Amendments, as well as with common law rights. The question, then, is to what extent do other interests implicate the same balancing test of the public interest versus privacy rights? This balancing seems to fall outside of the Title III framework.

C. *Relevant Provisions of Title III*

Title III is a "complex"[134] statute with "conflicting implications from different sections of [the Act]."[135] Even so, an examination of only a few relevant provisions of Title III is essential to determine the various methods that would allow for the use of court-authorized wiretap recordings in civil enforcement proceedings such as the SEC's case against Rajaratnam.

127. *See, e.g.*, *Gardner*, 895 F.2d at 79-80.

128. *See id.*

129. 532 U.S. 514, 517 (2001).

130. *Id.* at 519.

131. *Id.* at 533-34.

132. *See, e.g.*, *In re* New York Times Co. (*New York Times II*), 577 F.3d 401 (2d Cir. 2009).

133. *In re* Grand Jury, 111 F.3d 1066, 1078-79 (3d Cir. 1997).

134. United States v. Cianfrani, 573 F.2d 835, 855 (3d Cir. 1978).

135. Gelbard v. United States, 408 U.S. 41, 71 (1972) (Rehnquist, J., dissenting).

1. Section 2511—The General Prohibition

Section 2511 of Title III provides a general prohibition against the intentional interception, or the attempted interception, of "wire, oral, or electronic communications,"[136] as well as the "use of electronic, mechanical, or other communications."[137] Nonetheless, section 2511 exempts certain acts from regulation under Title III, including recording of conversations where one party consents[138] and the use of a pen register.[139] Section 2518 also permits interception and disclosure by law enforcement according to a mandated statutory procedure.[140]

In addition to prohibiting interception, section 2511 also prohibits intentional disclosure in a number of circumstances.[141] First, subsection 2511(1)(c) prohibits the intentional disclosure of the "contents of any wire, oral, or electronic communication" when the person "know[s] or [has] reason to know that the information was obtained . . . in violation of [subsection 2511(1)]."[142] Rajaratnam pointed to this subsection claiming that it prohibited him from disclosing wiretaps to the SEC because he had reason to know the wiretaps were intercepted in violation of Title III, as evidenced by his motion to suppress.[143] Second, similarly to subsection 2511(1)(c), subsection 2511(1)(d) prohibits the use of the contents of wire, oral, or electronic communications when the person "know[s] or [has] reason to know" they were obtained through a violation of subsection 2511(1).[144] This subsection attempts to prevent acts such as blackmail, where disclosure may never actually occur.[145] Finally, subsection 2511(1)(e) prohibits disclosure of certain lawfully

136. 18 U.S.C. § 2511(1)(a) (2006).

137. § 2511(1)(b). Also note that this prohibition is qualified by five factors, at least one of which must be present. *Id.* These factors, however, are not important to this discussion.

138. § 2511(2)(c)-(d).

139. § 2511(2)(h)(i). Other acts by private individuals and law enforcement are also exempt under the Act, but they are not worth discussing for the purposes of this paper. *See* § 2511(2); *In re* High Fructose Corn Syrup Litig., 216 F.3d 621, 624-25 (7th Cir. 2000).

140. 18 U.S.C. § 2518 (2006). *See infra* Part III.C.4.

141. § 2511(1)(c)-(e).

142. § 2511(1)(c).

143. Brief for Defendants-Appellants Raj Rajaratnam and Danielle Chiesi at 35-36, SEC v. Rajaratnam, Nos. 10-462-cv(L), 10-464-cv(CON), (2d Cir. Apr. 26, 2010), 2010 WL 2584235 [hereinafter Rajaratnam Brief].

144. § 2511(1)(d).

145. *See In re* High Fructose Corn Syrup Litig., 216 F.3d 621, 626 (7th Cir. 2000).

intercepted communications when the person "know[s] or [has] reason to know that the information was obtained . . . in connection with a criminal investigation," the person "received the information in connection with a criminal investigation," and it is done "with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation."[146] It is important to note that this subsection applies only to communications intercepted pursuant to certain subsections of section 2511 and only when disclosed with the intent to "obstruct, impede, or interfere" with a criminal investigation.[147] Accordingly, it is not generally applicable to all intercepted communications, primarily those that were exempted from the Act.[148] Notably, a violation of Title III occurs at the time the interception is obtained, as well as with each subsequent disclosure to "a third party who has not yet heard [the recording]."[149] Disclosure is permitted by section 2517 under certain circumstances.[150]

2. Section 2515—Evidence

Section 2515 prohibits the use of the contents of an intercept or "evidence derived therefrom . . . [as] evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, [or] legislative committee . . . if the disclosure of that information would be in violation of [Title III]."[151] Nonetheless, many circuit courts have found that contents of communications obtained in violation of Title III may be used in order to impeach witnesses' oral testimony or to impeach evidence submitted via sworn affidavit.[152]

Important to the analysis of this section is what is considered evidence. Apparently, disclosure in violation of Title III would not prevent use of wiretap communications for purposes of impeachment, either in a civil or criminal case.[153] Furthermore, it is important to note

146. § 2511(1)(e).

147. *Id.*

148. *See generally* § 2511.

149. Fultz v. Gilliam, 942 F.2d 396, 402 (6th Cir. 1991).

150. 18 U.S.C. § 2517 (2006); *see infra* Part III.C.3.

151. 18 U.S.C. § 2515 (2006).

152. *See, e.g.*, United States v. Baftiri, 263 F.3d 856, 856-57 (8th Cir. 2001); Culbertson v. Culbertson, 143 F.3d 825, 828 (4th Cir. 1998) (civil case); United States v. Echavarria-Olarte, 904 F.2d 1391, 1397 (9th Cir. 1990); United States v. Vest, 813 F.2d 477, 484 (1st Cir. 1987); United States v. Caron, 474 F.2d 506, 508 (5th Cir. 1973).

153. *See, e.g.*, cases cited *supra* note 152.

that use of the wiretaps or derivative evidence is only prohibited when disclosure is in violation of Title III.[154] Based on the structure of this section, one could presume that Congress anticipated at least some situations where contents of wiretaps and derivative evidence could be used as evidence, including before regulatory bodies, agencies, and courts.[155] In fact, courts have indicated that use in civil proceedings, such as in civil tax proceedings,[156] may be appropriate. In dicta, the Second Circuit also insinuated that disclosure by the DOJ might be appropriate in civil RICO suits and "other situations where release would be compatible with the purposes of Title III."[157] Accordingly, Congress may not have intended the use of lawfully intercepted wiretap contents to be limited to criminal proceedings, especially when dealing with a civil enforcement proceeding predicated on the same acts charged criminally.[158]

3. Section 2517—Permitted Disclosure

Section 2517 describes situations under which lawfully intercepted wiretap contents may be disclosed.[159] Only four are relevant in the context of use in civil enforcement proceedings.[160] Subsection 2517(1) allows "any investigative or law enforcement officer" who legally obtained wiretap contents or derivative evidence to disclose them to another "investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making *or* receiving the disclosure."[161] This authorization is more broad than subsection 2517(2), which authorizes only the *use* of legally obtained intercepts or derivative evidence by an "investigative or law enforcement officer" when the use "is appropriate to the proper

154. § 2515.

155. *See id.*

156. Fleming v. United States, 547 F.2d 872, 875 (5th Cir. 1977).

157. Nat'l Broad. Co. v. U.S. Dep't of Justice, 735 F.2d 51, 55 (2d Cir. 1984).

158. *See* SEC v. Rajaratnam, 622 F.3d 159, 178-79 (2d Cir. 2010) (discussing the 1970 amendment to Title III to permit disclosure in civil and criminal proceedings).

159. 18 U.S.C. § 2517 (2006).

160. *See* § 2517(1), (2), (3), (5). The other provisions deal with various other instances allowing disclosure. § 2517(4) (retaining privilege); § 2517(6) (sharing information with foreign intelligence/counterintelligence) § 2517(7) (sharing information with foreign law enforcement officials); § 2517(8) (sharing information with any foreign or domestic official when the contents reveal a threat to the United States or foreign power).

161. § 2517(1) (emphasis added).

performance of *his* official duties."[162] Nonetheless, both subsections 2517(1) and 2517(2) are limited by the definition of "investigative or law enforcement officer," which must be a person "empowered by law to conduct investigations of or to make arrests for offenses enumerated in [section 2516], and any attorney authorized by law to prosecute or participate in the prosecution of such offenses."[163] Accordingly, under these subsections an investigative or law enforcement officer would only be permitted to turn over wiretap contents and derivative evidence to the extent doing so is "appropriate to the proper performance" of either that officer's or the other officer's duty,[164] or to the extent disclosure was considered proper use according to that officer's official duties.[165] The application of these two subsections to civil enforcement proceedings, primarily SEC enforcement proceedings, will be discussed in Part IV.

Subsection 2517(3) provides that "any person" who has lawfully received contents of intercepted communications or derivative evidence can "disclose the contents . . . while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State . . . ."[166] Accordingly, it is possible that an investigative or law enforcement officer could disclose the contents of lawfully intercepted communications if called to testify in a civil enforcement proceeding.[167] Furthermore, as Judge Rakoff noted, if the civil attorney could elicit the contents through testimony in court, "it would be absurd for the civil attorneys preparing the witness not to have access to the wiretap recordings beforehand."[168] This subsection will be discussed in greater detail in Part IV.

Finally, subsection 2517(5) allows intercepted communications related to crimes not listed in the wiretap authorization or approval to be used according to subsection 2517(1) and 2517(2) without change, as

162. § 2517(2) (emphasis added).

163. § 2510(7).

164. § 2517(1).

165. § 2517(2). Presumably this is what was done when the USAO disclosed the wiretap recordings to Rajaratnam and Chiesi as part of criminal discovery. *See* SEC v. Rajaratnam, 622 F.3d 159, 165-66 (2d Cir. 2010).

166. § 2517(3).

167. *See, e.g.*, Fleming v. United States, 547 F.2d 872, 875 (5th Cir. 1977) (stating that FBI agents would have been able to disclose contents of wiretaps while testifying in a civil tax proceeding).

168. SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316, 318 (S.D.N.Y. 2010). *But cf. In re* High Fructose Corn Syrup Litig., 46 F. Supp. 2d 819, 831 (C.D. Ill. 1999) (stating that while the provision allows disclosure during testimony, it did not extend to pre-trial discovery).

well as subsection 2517(3) "when authorized or approved by a judge of competent jurisdiction."[169] This subsection would become relevant in instances where evidence of other crimes were "incidentally" intercepted, as would have been the case in the *Rajaratnam* case if insider trading had not been listed on the order.[170]

4. Section 2518—Procedure for Interception

Finally, section 2518 sets forth the procedure for which an "investigative or law enforcement officer" can apply "for an order authorizing or approving the interception of wire, oral, or electronic communication[s]."[171] While a discussion of all the requirements and intricacies of the section is beyond the scope of this paper, a basic understanding of the requirements is useful for further analysis of whether the intercepts may be used in civil enforcement proceedings.

Each application must be made under oath or affirmation[172] and contain the identity of the officer making the application.[173] Furthermore, it must contain a "complete statement of the facts and circumstances relied upon by the applicant" as to the offense, location of the proposed intercept, the "type of communications sought," and, if available, the identity of the target.[174] It must also give "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."[175] This has been termed the necessity requirement, though complete exhaustion of alternatives is not required.[176] Finally, there must be a set period of time for interception,[177] a maximum of thirty days unless an extension is granted,[178] and a recitation of the facts of any previous interception regarding the person or place targeted.[179]

169. § 2517(5).

170. *See* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *4-5 (S.D.N.Y. Nov. 24, 2010).

171. 18 U.S.C. § 2518 (2006).

172. § 2518(1).

173. § 2518(1)(a).

174. § 2518(1)(b).

175. § 2518(1)(c).

176. *See* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *14 (S.D.N.Y. Nov. 24, 2010).

177. § 2518(1)(d).

178. § 2518(5).

179. § 2518(1)(e).

Upon application, a judge may issue the order when "there is probable cause for [the] belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 . . . ,"[180] there is probable cause that communications concerning the offense will be obtained through the interception,[181] the judge finds that normal procedures have been tried or failed or are unlikely to succeed,[182] and there is probable cause that the target location is being used in connection with the offense.[183] The requirements for the application and order ensure that it is "'sought in good faith and not as a subterfuge search . . .'" to gain evidence for a crime for which there is no probable cause.[184]

Section 2518 goes further to impose a minimization requirement, to avoid interception of non-targeted communications,[185] as well as a procedure for handling treatment of wiretaps and wiretap orders after recording.[186] The details of these procedures need not be discussed in this paper.

IV. Obtaining Wiretaps in Civil Enforcement Proceedings

The parallel proceedings of *SEC v. Rajaratnam*[187] and *United States v. Rajaratnam*[188] raised the question of whether wiretaps, lawfully or unlawfully obtained in a criminal investigation, could be used in a parallel civil enforcement proceeding. These cases also presented the issue of timing, since the Second Circuit ruled that the judge in the civil case could not properly balance privacy interests against the need for disclosure until the suppression hearing challenging the wiretaps occurred.[189] Presumably, the SEC could have attempted to obtain the wiretaps from two sources. First, it could have sought them from the USAO. Second, it could have sought them from the defendants, which it

180. § 2518(3)(a).
181. § 2518(3)(b).
182. § 2518(3)(c).
183. § 2518(3)(d).
184. *See* United States v. Barnes, 47 F.3d 963, 965 (8th Cir. 1995) (quoting United States v. Sedovic, 679 F.2d 1233, 1237 n.4 (8th Cir. 1982)).
185. § 2518(5).
186. § 2518(8)-(12).
187. 622 F.3d 159 (2d Cir. 2010).
188. No. 09 Cr. 1184(RJH), 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010).
189. SEC v. Rajaratnam, 622 F.3d 159, 185 (2d Cir. 2010).

did in this case, as part of civil discovery.[190] Both of these methods will be analyzed in this section. The analysis will also take into account the issue of timing discussed above.

A. *From the USAO*

The SEC could have attempted to obtain the wiretap recordings from the USAO according to section 2517, either under subsection (1), (2), or (3).[191] Each of these subsections present separate circumstances under which disclosure would be proper. Accordingly, each will be analyzed separately.

Subsection 2517(1) authorizes the USAO to disclose the contents of the wiretaps obtained pursuant to Title III to an investigative or law enforcement officer if it is "appropriate to the proper performance" of either its or the receiving officer's "official duties."[192] The United States Attorney for the Southern District of New York referred to the SEC as the USAO's "law enforcement partner[]."[193] If SEC attorneys are in fact investigative or law enforcement officers, this subsection would seem to allow disclosure, as the SEC is authorized to investigate violations of the Securities and Exchange Act of 1934.[194] However, because Title III's definition of "[i]nvestigative or law enforcement officer" is limited to those who are "empowered by law" to investigate or make arrests for offenses enumerated in section 2516,[195] the analysis becomes much more attenuated. Criminal wire fraud is an enumerated offense,[196] however civil and criminal securities fraud are not.[197] Nonetheless, the SEC is authorized to refer cases to the U.S. Attorney General for criminal prosecution.[198] But this is unlikely to qualify the SEC as "empowered by law"[199] to investigate wire fraud, even though practically, its employees will often investigate wire fraud as part of their insider trading

190. *See* SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316 (S.D.N.Y. 2010).
191. 18 U.S.C. § 2517(1)-(3) (2006).
192. § 2517(1).
193. Bharara, *supra* note 6.
194. Securities Exchange Act of 1934 § 21(a)(1), 15 U.S.C. § 78u(a)(1) (2006).
195. 18 U.S.C. § 2510(7) (2006).
196. 18 U.S.C. § 2516(1)(c) (2006).
197. *See* § 2516.
198. Securities Act of 1933, § 20(b), 15 U.S.C. § 77t(b) (2006); 15 U.S.C. § 78u(d)(1).
199. § 2510(7).

investigations[200] and share that information with the U.S. Attorney General and USAO.[201] Accordingly, it is unlikely that any circumstances exist in which any employee of the SEC could be considered an investigative or law enforcement officer under the Act and be permitted to receive wiretap recordings under this subsection.

Subsection 2517(2) is broader in the sense that disclosure is not limited to an investigative or law enforcement officer.[202] Instead, the USAO could disclose the wiretaps whenever it is "appropriate to the proper performance of [its] official duties."[203] Though the USAO initially took the position that it had authority to disclose the wiretaps to the SEC pursuant to this section,[204] it later claimed that it could not disclose the recordings "to the SEC without any law enforcement purpose solely to assist the SEC in a civil case."[205] On its face, this statement is correct; the USAO may not disclose wiretap communications to the SEC unless appropriate to its duties.[206] Nevertheless, if aiding civil enforcement branches like the SEC in their investigations was considered part of the USAO's duties, disclosure would be appropriate. Instead, the USAO took the position that it could only disclose the recordings to the SEC pursuant to this section if disclosure was done to gain assistance from the SEC in its criminal investigation.[207] Under that theory, disclosure would have been most appropriate when the SEC, FBI, and USAO were acting as partners in the investigation of Rajaratnam and Chiesi.[208]

It appears that the USAO could take a more liberal approach to when disclosure is necessary to "obtain assistance in preventing, investigating, or prosecuting a crime . . ."[209] and, thus, increase instances

200. *See* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *4 (S.D.N.Y. Nov. 24, 2010).

201. *See* 15 U.S.C. § 77t(b); 15 U.S.C. § 78u(d)(1).

202. § 2517(2).

203. *Id.*

204. SEC v. Rajaratnam, 622 F.3d 159, 165 n.1 (2d Cir. 2010).

205. Brief for the United States of America as Amicus Curiae in Support of the Securities and Exchange Commission at *9 n.*, SEC v. Rajaratnam, Nos. 10-462-cv(L), 10-464-cv(CON) (2d Cir. June 1, 2010) (first footnote).

206. § 2517(2).

207. Brief for the United States of America as Amicus Curiae in Support of the Securities and Exchange Commission at *9 n.*, SEC v. Rajaratnam, Nos. 10-462-cv(L), 10-464-cv(CON) (2d Cir. June 1, 2010) (first footnote).

208. *See* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *15-18 (S.D.N.Y. Nov. 24, 2010) (describing the investigation).

209. Sharing Title III Electronic Surveillance Material with the Intelligence Community, 2000 WL 33716983 (O.L.C.), at *1 (Oct. 17, 2010), *available at* http://www.justice.gov/olc/titleIIIfinal.htm.

of disclosure and cooperation, though policy in the past has been to construe this power narrowly.[210] However, it is uncontested that disclosure to the SEC could be appropriate in some circumstances. Accordingly, if the SEC were more adamant about receiving recordings in the initial phases of the investigation, one would assume the USAO would be more likely to comply and accept greater assistance from the SEC, especially since the SEC has discretion as to whether or not they will transmit evidence of criminal violations to criminal authorities and assist in USAO investigations.[211] SEC policy conditioning assistance on full disclosure of relevant evidence would likely go a long way in encouraging more complete cooperation, as well as to strengthen the USAO's argument that disclosure was necessary "to the proper performance of [its] official duties."[212]

Finally, the SEC could receive the wiretap recordings from the USAO (or the FBI) as testimony in the civil trial by calling a person with knowledge of the contents to the stand.[213] Under this subsection "a judge of competent jurisdiction" may have to find that the wiretaps were lawfully intercepted,[214] since securities fraud is not an enumerated offense.[215] Nonetheless, it is possible that a ruling on legality is not required since securities fraud was listed on the wiretap application and order.[216] The question then becomes whether the SEC would be able to discover the materials before the officer testifies, which is the subject of some controversy.[217] While the literal reading of subsection 2517(3) seems to limit disclosure to testimony, it seems absurd[218] to force the civil trial to "be carried on in the dark."[219] This seems to be one of those instances in which the court must balance privacy interests with the

210. *See id.*

211. *See* Securities Act of 1933, § 20(b), 15 U.S.C. § 77t(b) (2006); Securities Exchange Act of 1934, § 21(d), 15 U.S.C. § 78u(d) (2006).

212. 18 U.S.C. § 2517(2) (2006).

213. § 2517(3).

214. § 2517(5).

215. 18 U.S.C. § 2516 (2006).

216. *See* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *4 (S.D.N.Y. Nov. 24, 2010).

217. *Compare* SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316, 318 (S.D.N.Y. 2010), *with In re* High Fructose Corn Syrup Litig., 46 F. Supp. 2d 819, 831 (C.D. Ill. 1999).

218. *In re High Fructose Corn Syrup Litig.*, 46 F. Supp. 2d at 831.

219. Hickman v. Taylor, 329 U.S. 495, 501 (1947) (discussing the purpose of the newly adopted Federal Rules of Civil Procedure).

public interest of full discovery in civil enforcement proceedings.[220] Though not a common law or constitutional interest, the broad, liberal application of the Federal Rules of Civil Procedure ("Rules") is a well-recognized aspect of modern civil litigation and is worthy of protection against narrow interpretation without specific prohibitions narrowing the Rules' application.[221]

All three of these subsections seem to assume that disclosure may be made without a determination as to the legality of the interception,[222] except as to disclosure through testimony about offenses not listed in the order.[223] This makes sense since a judge has already made a preliminary determination that the interceptions are legal when he or she issued the wiretap order.[224] Nevertheless, whenever the contents of the recordings are being introduced into evidence at the civil trial, the judge will be able to decide whether they are relevant and admissible.[225] The judge may also have to make a determination of whether the interception was authorized pursuant to Title III to determine whether the contents or derivative evidence are admissible.[226] Any "judge of competent jurisdiction" likely could make this determination, either in the criminal trial or in the civil trial.[227]

220. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 533-34 (2001) (balancing privacy interests with the public interest in publishing matters of public importance); Gardner v. Newsday, Inc., 895 F.2d 74, 75 (2d Cir. 1990) (balancing privacy interests with the right of access).

221. *See generally Hickman*, 329 U.S. at 501-06 ("[S]ince the discovery provisions are to be applied as broadly and liberally as possible, the privilege limitation must be restricted to its narrowest bounds.").

222. 18 U.S.C. § 2517(1)-(3) (2006).

223. § 2517(5).

224. 18 U.S.C. § 2518 (2006). It is still possible that the wiretaps may be suppressed because of a failure to minimize or if the application was not "full and complete." *Id.* It is unclear whether suppression is a result of the 4th Amendment's exclusionary rule or because the intercepts were illegal and, thus, unable to be disclosed. *See Bartnicki*, 532 U.S. at 550-51; United States v. Caceres, 440 U.S. 741, 754-56 (1979).

225. *See* FED. R. EVID. 401, 403 (relevancy and exclusion of relevant evidence).

226. 18 U.S.C. § 2515 (2006).

227. *See* § 2517(5).

B. *From the Defendant*

As they did in *SEC v. Rajaratnam*, the SEC could seek to get the wiretap recordings from the defendant as part of civil discovery.[228] Obviously, this would require that the USAO have turned over the recordings to the defendants, as it did in *SEC v. Rajaratnam*, as part of criminal discovery.[229] It may also require that they be disclosed to the defendants not subject to a protective order.[230] Because Title III does not permit disclosure in this fashion, the court would have to accept "that Title III does not prohibit all disclosures of legally intercepted wire communications that it does not expressly permit."[231] If the court were to accept that interpretation, it would have to balance the privacy interests against the broad notion of liberally construed discovery rules,[232] just as the courts have done with other constitutional and common law interests.[233] This balancing, while acknowledging Title III interests, falls outside the regulatory bounds of the Act.[234]

The Federal Rules of Civil Procedure are designed to allow both "parties to obtain the fullest possible knowledge of the issues and facts before trial."[235] They are to be "broadly and liberally" construed to allow for the discovery of "true facts . . . wherever they may be found."[236] The broad notion of civil discovery is only limited by privilege, which "must be restricted to its narrowest bounds."[237] Broad civil discovery is clearly expressed in Rule 26: "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense . . . ."[238] Furthermore, "the court may order discovery" of any relevant matter, which "need not be admissible" if it will likely lead to "admissible evidence."[239]

228. *See generally* SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010).
229. *Id.* at 165.
230. *See* SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316, 317-18 (S.D.N.Y. 2010).
231. SEC v. Rajaratnam, 622 F.3d 159, 176 (2d Cir. 2010).
232. Hickman v. Taylor, 329 U.S. 495, 505-06 (1947).
233. *See, e.g.*, sources cited *supra* note 224.
234. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514 (2001).
235. *Hickman*, 329 U.S. at 501.
236. *Id.* at 506.
237. *Id.*
238. FED. R. CIV. P. 26(b)(1).
239. *Id.*

The Second Circuit stated that the privacy interest must be balanced against the right of access.[240] While that is certainly relevant, the court must also take account of the public interest in broad civil discovery rules—that "civil trials in the federal courts no longer need [to] be carried on in the dark."[241] The existence of Title III indicates the severity of the privacy interests at stake, even in lawfully obtained wiretap recordings.[242] This privacy interest is not just invaded upon by the initial recording, but also upon each subsequent disclosure.[243] Nonetheless, a party's interest in discovering relevant evidence is also strong.[244] As the Supreme Court has stated over and over, "[m]utual knowledge of all the relevant facts gathered by both parties is essential to proper litigation."[245] Here, however, mutual knowledge cannot be achieved without discovery of the wiretap materials.[246] Rajaratnam was in possession of the wiretaps and could use them in preparation for both his criminal and civil trials.[247] This "informational advantage" could not be remedied in any way other than disclosure.[248]

The informational gap between the two parties seems to hold true regardless of whether the intercepts were conducted lawfully or unlawfully. If they were intercepted in violation of Title III, however, the contents of the wiretap or any derivative evidence could not be introduced into evidence according to the plain language of Title III.[249] That may be an instance where Congress has truly done "all of the balancing necessary";[250] the informational imbalance is acceptable because of the privacy interests at stake. Nonetheless, disclosure through discovery may still be required since the SEC may be able to use the materials for purposes of impeachment.[251] If a determination of legality is necessary, it seems that "any judge of competent jurisdiction" could

240. SEC v. Rajaratnam, 622 F.3d 159, 176-77 (2d Cir. 2010).

241. *See Hickman*, 329 U.S. at 501.

242. *See* Gelbard v. United States, 408 U.S. 41, 48 (1972) (asserting that "the protection of privacy was an overriding congressional concern").

243. *See id.* at 51-52.

244. SEC v. Rajaratnam, 622 F.3d 159, 182 (2d Cir. 2010).

245. *Hickman*, 329 U.S. at 507.

246. *See* SEC Brief, *supra* note 33, at 3.

247. *See id.*

248. *Id.* at 42.

249. 18 U.S.C. § 2515 (2006).

250. *In re* Grand Jury, 111 F.3d 1066, 1078-79 (3d Cir. 1997).

251. *See, e.g.*, sources cited *supra* note 152.

make the determination,[252] even though the judge in the criminal case or the authorizing judge may initially have more information to do so as a result of the judge's prior involvement.

While the privacy interests are strong, the Federal Rules of Civil Procedure already contain a method to protect privacy interests—the protective order.[253] The protective order allows a judge great leniency in deciding the method of discovery, as well as subsequent disclosure.[254] A protective order should be sufficient to protect the privacy interests at stake, especially when dealing with legally intercepted communications.[255] While the privacy interests are admittedly greater when dealing with illegally intercepted communications, a protective order may still be sufficient to allow discovery for purposes of impeachment. Furthermore, the judge should consider privacy interests of third parties when setting terms of discovery and disclosure.[256]

Congress did not intend Title III to act as a "general civil discovery mechanism," as it would "ignore the privacy rights of those whose conversations are overheard."[257] However, Title III would arguably not have this effect if allowed in civil enforcement proceedings. Intercept materials would not be "broadly available to all civil litigants . . . ."[258] Rather, it would be available to civil enforcement branches of government agencies "charged" with enforcing the civil law.[259] It appears that the invasion of privacy interests is less severe in this context, especially when the USAO does not oppose disclosure.[260] And again, even if discoverable, a judge may still rule that the wiretap contents are inadmissible at the civil proceeding or limit questioning because the contents are irrelevant, unfairly prejudicial, or embarrassing.[261]

252. *See* 18 U.S.C. § 2517(5) (2006).

253. FED. R. CIV. P. 26(c).

254. *Id.*

255. *See In re* High Fructose Corn Syrup Litig., 216 F.3d 621, 624 (7th Cir. 2000).

256. *New York Times I*, 828 F.2d 110, 112 (2d Cir. 1987).

257. Nat'l Broad. Co. v. U.S. Dep't of Justice, 735 F.2d 51, 54 (2d Cir. 1984).

258. *Id.*

259. *See* SEC v. Galleon Mgmt., LP, 683 F. Supp. 2d 316, 318 (S.D.N.Y. 2010); SEC v. Mgmt. Dynamics, 515 F.2d 801, 808 (2d Cir. 1975) (describing the SEC as a "statutory guardian" rather than an "ordinary litigant").

260. *See* Gardner v. Newsday, Inc., 895 F.2d 74, 79 (2d Cir. 1990).

261. FED. R. EVID. 401, 403, 611(a).

Rajaratnam and Chiesi claimed that disclosure by them would be a violation of Title III.[262] That was likely not an accurate statement of the law. First, it would be peculiar for a party to the recording to be held liable for disclosure, especially since the recording would be exempted from Title III if they had recorded it themselves or given consent.[263] Second, nothing in Title III actually forbids disclosure unless it was not intercepted according to Title III.[264] Finally, even if it were a violation, reliance on a court order would be a complete defense against civil or criminal liability.[265] Accordingly, after balancing privacy interests against the interest of broad civil discovery, disclosure was likely proper. While the legality of the wiretaps may play a role in that balancing analysis, there is no reason to assume that a particular judge must make the determination.[266] This is especially true if there is a "strong public interest in cases of this kind moving forward promptly," apart from the criminal trial, as Judge Rakoff suggests.[267]

V. Conclusion

It appears that there is an "all-out assault on white collar crime" by the DOJ and that the use of wiretaps in white-collar criminal investigations will only increase.[268] Attempts to use wiretap recordings in parallel civil enforcement proceedings are also likely to increase, especially now that the Second Circuit seems likely to permit discovery

262. Rajaratnam Brief, *supra* note 143, at 35.

263. *See* 18 U.S.C. § 2511(2)(c), (d) (2006). Accordingly, intentional disclosure or intentional use may act as "constructive" consent.

264. *See* 18 U.S.C. §§ 2511, 2517 (2006).

265. 18 U.S.C. § 2520(d) (2006).

266. This is especially true when multiple criminal cases are ongoing, as was the case here. The civil case need not wait for a determination by the trial court, which may never come if the case were to settle before a suppression hearing occurs. *See* Plaintiff's Memorandum of Law in Support of its Renewed Motion to Compel Production of Relevant, Legally Obtained Wiretapped Communications, SEC v. Galleon Mgmt., LP, No. 09 Civ. 8811(JSR) 2010 WL5191710, at *3 n.1 (S.D.N.Y. Dec. 17, 2010) (discussing additional wiretaps that had not undergone a suppression hearing).

267. SEC v. Rajaratnam, 622 F.3d 159, 166 (2d Cir. 2010) (quoting Judge Rakoff) (explaining why the district court reserved judgment on the suppression motion).

268. Hillary Russ, *DOJ Promises More Wiretaps in White Collar Cases*, LAW360 (Nov. 4, 2010, 3:24 PM), http://www.law360.com/topnews/articles/206673/doj-promises-more-wiretaps-in-white-collar-cases; *see also* Peter J. Henning, *The Winning Record of Prosecutors on Insider Trading*, N.Y. TIMES (Aug. 21, 2012, 11:49 AM), http://dealbook.nytimes.com/2012/08/21/the-winning-record-of-prosecutors-of-insider-trading/.

after suppression hearings occur.[269] Accordingly, civil enforcement branches like the SEC can take actions that make it easier for them to obtain wiretap recordings. One such method would be to condition aid in USAO criminal investigations on forthright cooperation by the USAO, including disclosure of wiretap recordings. This gives the USAO a better argument that disclosure is proper under Title III[270] and would avoid the unnecessary controversy over when wiretap contents can be disclosed through testimony[271] and ordinary civil discovery.

At least some circuit court decisions are allowing disclosure outside Title III's confines, such as through civil discovery.[272] The balancing test employed allows for discovery when the privacy interest is not too severe as to outweigh the necessity for disclosure.[273] The Second Circuit held that this test can only occur after the legality of the wiretaps is tested.[274] Nonetheless, it is likely that the test could be employed if the civil judge made a ruling on the legality of the wiretaps, rather than waiting on a determination by the judge in the criminal trial. This is especially necessary when dealing with multiple criminal cases. However, the problem could be avoided altogether if the judge were to stay the civil trial until after the criminal trial, when legality has been tested and some wiretap contents have already become public. This would seem to be a wise approach if disclosure was not obtained through Title III mechanisms.

Title III is no longer a "comprehensive scheme" to regulate wiretaps.[275] The courts have broken it down through the use of various balancing tests.[276] Congress should consider incorporating these balancing tests into Title III by addressing these interests. Congress could also amend Title III to allow civil enforcement attorneys to receive wiretap contents as investigative officers.[277] This would avoid the current

269. SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010); *see also* Jonathan Stempel, *Analysis - Galleon Wiretaps Big for White Collar Crime Cases*, REUTERS (Jan. 27, 2010, 9:12 PM), http://in.reuters.com/article/2010/01/27/idINIndia-45739920100127.

270. *See* 18 U.S.C. § 2517(2) (2006).

271. *See* § 2517(3), (5).

272. *See, e.g.*, SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010).

273. *Id.* at 183.

274. *Id.* at 187.

275. Gelbard v. United States, 408 U.S. 41, 46 (1972).

276. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514 (2001); Gardner v. Newsday, Inc., 895 F.2d 74 (2d Cir. 1990); *New York Times I*, 828 F.2d 110 (2d Cir. 1987); *In re* Globe Newspaper Co., 729 F.2d 47 (1st Cir. 1984).

277. *See* 18 U.S.C. § 2517(1) (2006). This proposal would only cause civil enforcement attorneys to act as investigative officers for purposes of disclosure, not for

problems presented by the balancing tests because of timing with criminal cases.[278] As it stands, the courts are currently operating under two sets of rules, one within the bounds of Title III and the other a balancing of interests outside the Title III statutory framework. Congress could do much to simplify this area of the law, protect privacy, and ensure strong civil enforcement by bringing both these sets of rules back under the umbrella of Title III.

purposes of making wiretap applications.

278. A balancing test would still likely need to be employed before offering the contents as evidence in the civil trial.