Journal of Technology Law & Policy

Volume XIII – Spring 2013

ISSN 1087-6995 (print)

DOI 10.5195/tlp.2013.122

http://tlp.law.pitt.edu

Drawing the Line: The Legality of Using Wiretaps to Investigate Insider Trading

Shane Miller

Drawing the Line: The Legality of Using Wiretaps to Investigate Insider Trading

Shane Miller*

The critically acclaimed television series *The Wire* ran for five seasons on HBO before going off the airwaves in 2008.[1] The show depicted how Baltimore police officers used wiretaps to eavesdrop on city drug lords.[2] Although *The Wire*'s plot was compelling, its storyline could be taken in an entirely new direction if the series aired today. In the past, wiretaps were used almost exclusively to investigate drug offenses and homicides.[3] *The Wire* accurately portrayed this reality.[4] In recent years, however, law enforcement has employed wiretaps to investigate an entirely different kind of crime: insider trading.[5]

Although wiretaps have been extremely effective in taking down insider trading rings, the precise scope of the government's power to use a wiretap for this purpose remains unclear.[6] This article examines this issue in the following manner. Part I describes how the government used wiretaps in the past, how its use of wiretaps has changed in recent years, and why any expansion of wiretap privileges could have privacy implications for millions of citizens. Part II examines Title III, the federal statute that governs the use of wiretaps. Part III defines insider trading, discusses how it is regulated, and explains why law enforcement recently started using wiretaps to fight insider trading. Part IV analyzes the landmark case of

---

* J.D. Candidate, University of Pittsburgh School of Law, May 2014; B.A., Business, Emory University.

[1] *About the Show*, HBO THE WIRE, http://www.hbo.com/the-wire/index.html#/the-wire/about/index.html.

[2] *Id.*

[3] Thomas Hogan, *Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications*, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS (June 2012), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/2011WireTap.pdf.

[4] *About the Show*, *supra* note 1.

[5] *See* James O'Toole, *Perfect Hedge: 56 Found Guilty of Insider Trading*, CNN MONEY (Jan. 31, 2012, 11:29 AM), http://money.cnn.com/2012/01/24/news/economy/insider_trading/index.htm.

[6] Howard J. Kaplan, Joseph A. Matteo & Richard Sillett, *The History and Law of Wiretapping* (Apr. 2012), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

United States v. Rajaratnam and determines whether the court's ruling is consistent with Title III. Finally, Part V offers recommendations and conclusions.

I. WIRETAPS & CELL PHONES

A wiretap is the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[7] Wiretaps are usually used to investigate drug crimes, as evidenced by the fact that narcotics investigations accounted for 85% of all wiretap applications in 2011.[8] Homicide investigations are the second most prevalent use for wiretaps.[9] In 2011, judges authorized 2,732 wiretaps nationwide, with telephone wiretaps constituting 96% of this total.[10]

Wiretaps on landline phones have sharply decreased in recent years due to the proliferation of mobile devices such as cell phones and smart phones.[11] The prevalence of mobile devices is quite startling, as nearly nine out of ten American adults now have a cell phone.[12] Amazingly, given that some individuals own multiple phones, there are now more cell phones than people in the United States.[13] Given the rapid growth of mobile devices, it is not surprising that nearly all wiretaps are now placed on cell phones and pagers.[14]

The scope of the government's eavesdropping power has privacy implications for all Americans. If the government is granted ever-greater wiretap authority, an individual's next private phone call could be monitored even if she is not suspected of unlawful activity. In one recent investigation, for example, investigators intercepted 18,150 separate phone calls among 550 different individuals.[15] Such broad eavesdropping power requires close scrutiny by the public.

---

[7] 18 U.S.C. § 2510 (2006).

[8] Hogan, *supra* note 3, at 10.

[9] *Id.* at 8.

[10] *Id.* at 9.

[11] *Id.* at 7.

[12] Joanna Brenner, *Pew Internet: Mobile*, PEW RESEARCH CENTER (Jan. 31, 2013), http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx.

[13] Cecilia Kang, *Number of Cellphones Exceeds U.S. Population: CTIA Trade Group*, WASH. POST BUS. (Oct. 11, 2011, 7:54 AM), http://www.washingtonpost.com/blogs/post-tech/post/number-of-cell-phones-exceeds-us-population-ctia-trade-group/2011/10/11/gIQARNcEcL_blog.html.

[14] Hogan, *supra* note 3, at 7.

[15] Kaplan et al., *supra* note 6, at 5.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

II. THE FEDERAL WIRETAP STATUTE

The government's wiretap and electronic surveillance authority is regulated primarily by a federal statute, Title III.[16] Evidence gathered from a wiretap can be suppressed in court if the government fails to comply with the statute's strict requirements.[17]

Title III requires the government to obtain judicial approval before using electronic devices to intercept a "wire, oral or electronic communication."[18] Therefore, when seeking a wiretap the government must first provide probable cause that an individual is engaging or about to engage in criminal activity.[19] The government then must prove that the communications dealing with the particular offense will likely be intercepted by a wiretap.[20] Moreover, the issuing judge must be convinced (1) that normal investigative procedures have been exhausted and failed, (2) that the normal investigative procedures, if reasonably tried, will be unlikely to succeed, or (3) that they would be too dangerous if carried out.[21]

This three-step process is known as the "necessity" requirement.[22] Given that wiretaps create a tremendous intrusion into personal privacy, Congress included the "necessity" provision to ensure that law enforcement try less invasive investigative techniques before resorting to a wiretap.[23]

Furthermore, Title III states that a wiretap cannot be used to investigate every type of unlawful activity. Instead, the statute authorizes the interception of communications only when certain crimes are under investigation.[24] These so-called "predicate offenses" are enumerated in § 2516 of Title III.[25] The extensive list of predicate offenses includes many serious crimes such as terrorism,

---

[16] 18 U.S.C. §§ 2510–2522 (2006); Kenneth M. Breen & Sean T. Haran, *The Rise of Wiretaps and Government Eavesdropping in Securities Fraud Cases*, 35 CHAMPION 43, 43 (May 2011).

[17] *Id.* at 44.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Peter J. Henning, *Judging if Wiretaps Are Necessary*, N.Y. TIMES (Oct. 25, 2012), http://dealbook.nytimes.com/2012/10/25/judging-if-wiretaps-are-necessary/.

[23] United States v. Lilla, 699 F.2d 99, 102–03 (2d Cir. 1983).

[24] Gelbard v. United States, 408 U.S. 41, 46 (1972).

[25] 18 U.S.C. § 2516 (2006).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

assassination, murder for hire, money laundering, and racketeering.[26] Congress has expanded the list over the years when it determines that law enforcement needs broader wiretap power.[27]

Notably, although wire fraud is included, neither insider trading nor securities fraud is listed as a predicate offense in § 2516.[28] Under Title III's "plain-view" exception, however, law enforcement can still use a wiretap to investigate a non-predicate offense, such as insider trading, in certain situations.[29] This exception allows the government to gather evidence about a non-predicate offense with a wiretap if the information is obtained while lawfully investigating a predicate offense listed in § 2516.[30] The plain-view exception ensures that law enforcement is not forced to ignore illegal activity that is uncovered during the course of another lawful investigation.[31]

Finally, Title III requires the government to make a reasonable effort to minimize the interception of communications that are unrelated to the crime being investigated.[32] Thus, while monitoring calls, law enforcement must stop listening when the conversation concerns topics unrelated to the investigation.[33]

III. INSIDER TRADING

In general, an individual is guilty of insider trading if she purchases or sells securities while in possession of material, non-public information in a manner that breaches a fiduciary duty owed to shareholders or the information source.[34] Courts have expanded this definition, holding that insider trading occurs when an individual:

[26] *Id.*; Breen & Haran, *supra* note 16, at 43–44.

[27] Kaplan et al., *supra* note 6, at 6.

[28] Breen & Haran, *supra* note 16, at 43.

[29] Kaplan et al., *supra* note 6, at 6.

[30] *Id.*

[31] Breen & Haran, *supra* note 16, at 44.

[32] 18 U.S.C. § 2518(5) (2006).

[33] JOHN C. HUESTON, NEW DEVELOPMENTS IN INSIDER TRADING INVESTIGATIONS AND HOW TO RESPOND 1, 5 (Thomson Reuters/Aspatore 2012).

[34] *Id.* at 7.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

> (1) breaches a fiduciary duty or other relationship of trust and confidence by purchasing or selling a security while in possession of material, non-public information;
> (2) "tips" others to material, non-public information;
> (3) trades securities after receiving a "tip"; or
> (4) trades securities after "misappropriating" material, non-public information.[35]

The Securities and Exchange Commission's ("SEC") Enforcement Division and the Department of Justice's ("DOJ") Fraud Section prosecute insider trading through Section 10(b) of the Securities Exchange Act and its corresponding regulation, Rule 10b-5.[36] Both agencies have vigorously pursued insider trading investigations in recent years, possibly in response to their failure to sufficiently regulate financial institutions in previous years.[37] In fact, the SEC has filed more insider trading actions in the last three years than it has during any other three-year period in the agency's history.[38] These cases have targeted a wide variety of powerful corporate executives, including chief executive officers, financial professionals, hedge fund managers, corporate insiders, and attorneys.[39]

An insider trading investigation is normally triggered by the occurrence of suspicious trading activity, such as when a large stock purchase or sale occurs right before a major corporate announcement.[40] The government then typically tries to make its case by using circumstantial evidence such as telephone calls, e-mails, and meetings to tie the suspect to a corporate insider.[41] After establishing this link, the prosecution then asks the fact finder to infer that the suspect engaged in insider trading by pointing to subsequent trading activity in which the suspect achieved significant financial gains or avoided sizable losses.[42]

---

[35] Patrick Craine & Lashon Kell, *Prosecuting Insider Trading: Recent Developments and Novel Approaches*, 59 THE ADVOC. (TEXAS) 45, 45 (Summer 2012).

[36] *Id.*; 17 C.F.R. § 240.10b-5.

[37] Breen & Haran, *supra* note 16, at 43.

[38] *Id.*

[39] *Id.*

[40] HUESTON, *supra* note 33, at 2.

[41] *Id.*

[42] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

Law enforcement is well aware that insider trading is pervasive at some financial institutions.[43] Past investigations revealed the existence of so-called "expert-network firms."[44] These firms are designed to connect finance professionals with corporate insiders willing to provide nonpublic information for a generous fee.[45] In other cases, investigators learned that inside traders covered their illegal activity with mafia-like tactics, such as secrets meetings, disposable cell phones, and cash kickbacks.[46]

The government turned to wiretaps after concluding that traditional methods of investigation were inadequate to fight the insider trading epidemic.[47] According to law enforcement, the finance industry is a tightly knit circle, thus making it difficult for undercover sources or informants to infiltrate insider trading networks.[48] Moreover, potential informants have little incentive to cooperate, knowing that their business careers will be finished if their identity is uncovered.[49]

The government also favors wiretaps because recorded conversations can provide direct evidence of insider trading.[50] Sophisticated investors buy and sell stocks quite frequently, making it difficult for law enforcement to differentiate between normal everyday trading and illegal insider trading.[51] Without direct evidence obtained from wiretaps, prosecutors may struggle to gather enough circumstantial evidence to secure an insider trading conviction.[52]

---

[43] Ailsa Chang, *Wall Street Wiretaps: Investigators Use Insiders' Own Words to Convict Them*, NPR (Dec. 26, 2012, 3:25 AM), http://www.npr.org/2012/12/26/168021457/wall-street-wiretaps-investigators-use-insiders-own-words-to-convict-them.

[44] Katherine Burton, Paul M. Barrett & Saijel Kishan, *The Rajaratnam Conviction: How Big a Victory?*, BLOOMBERG BUS. WEEK MAG. (2011), http://www.businessweek.com/magazine/content/11_21/b4229006268073.htm.

[45] *Id.*

[46] *SEC Charges 14 in Wall Street Insider Trading Case*, REUTERS (Mar. 1, 2007, 5:03 PM), http://uk.reuters.com/article/2007/03/01/sec-insidertrading-idUKN01350020070301.

[47] Chang, *supra* note 43.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

IV. *UNITED STATES V. RAJARATNAM*—DID THE COURT GET IT RIGHT?

A. Background

In 2008, law enforcement took the gloves off and elected to use a wiretap to investigate insider trading for the first time.[53] This momentous investigation targeted Raj Rajaratnam, the founder of Galleon Group, an enormously profitable hedge fund.[54] At the height of its prosperity in early 2008, Galleon controlled more than $7 billion in assets and produced staggering returns year after year.[55]

On March 7, 2008 the government submitted an application to tap Rajaratnam's cell phone in the Federal District Court for the Southern District of New York.[56] The court granted a 30-day wiretap, and the government began intercepting communications on Rajaratnam's cell phone shortly thereafter.[57] However, the government needed more evidence to build its case and subsequently received permission to tap nine more phones over the next sixteen months.[58] The authorities ultimately recorded 18,150 separate phone calls among 550 different individuals in the course of their investigation.[59]

The government's painstaking and extensive investigation finally paid off on October 16, 2009, when Rajaratnam and more than twenty associates were arrested and charged with multiple counts of conspiracy and securities fraud.[60] A jury convicted Rajaratnam of fourteen counts of insider trading and conspiracy after a lengthy trial on May 11, 2011.[61] He received eleven years in prison, the longest sentence ever imposed for an insider trading case.[62] He was also required to pay a $10 million fine, give back $53 million in profits, and pay $92 million to the SEC

---

[53] *Analysis—Insider Trading Wire Taps Sign of Things to Come*, REUTERS (Oct. 20, 2009, 5:28 PM), http://news.alibaba.com/article/detail/technology/100186869-1-analysis-insider-trading-wire-taps-sign.html.

[54] HUESTON, *supra* note 33, at 1.

[55] *Id.* at 2.

[56] United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 WL 4867402 at *2 (S.D.N.Y. Nov. 24, 2010).

[57] *Id.*

[58] Kaplan et al., *supra* note 6, at 5.

[59] *Id.*

[60] *Rajaratnam*, 2010 WL 4867402, at 2.

[61] Breen & Haran, *supra* note 16, at 1.

[62] Kaplan et al., *supra* note 6, at 1.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

as part of a civil suit.[63] Ultimately, Rajaratnam's own words sealed his fate, as the wiretapped conversations between Rajaratnam and his associates provided the crucial evidence the prosecution needed to secure a conviction.[64]

B. The Suppression Hearing

At a suppression hearing before his trial, Rajaratnam vigorously argued that the wiretapped conversations were not authorized under Title III and thus should be excluded at trial.[65] He advanced four main arguments.[66] First, he asserted that the government could not use wiretaps to investigate insider trading because securities fraud is not listed as a predicate offense under § 2516 of Title III.[67] Second, the government had failed to establish the probable cause necessary to receive wiretap authority.[68] Third, the government had not proven that the wiretaps were "necessary" because it had failed to show that conventional investigative techniques were inadequate.[69] Finally, Rajaratnam argued that the conversations should be suppressed because the government failed to minimize its interception of phone conversations that were unrelated to insider trading.[70]

C. The Importance of Rajaratnam

Given that *Rajaratnam* is the first case in which wiretaps were used to investigate insider trading, the court's decision may guide other courts in future cases. Thus, the ruling requires careful analysis to ensure that the court properly interpreted the scope the government's wiretap authority under Title III. As this article argues, the *Rajaratnam* decision is controversial and may exceed the boundaries of Title III.

D. Did the Court Get It Right?

Rajaratnam's first argument—that the wiretaps were illegal because securities fraud or insider trading are not listed as predicate offenses under Title III—deserves closer examination. As stated earlier, a wiretap may only be used when

---

[63] *Id.*

[64] Breen & Haran, *supra* note 16, at 1.

[65] *Rajaratnam*, 2010 WL 4867402, at *1.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

certain crimes—known as predicate offenses—are under investigation.[71] However, under the plain view exception, the government may gather evidence of a non-predicate offense, such as insider trading, if the information is obtained by a wiretap that is lawfully being used to investigate a predicate offense.[72]

At the suppression hearing, Federal District Court judge Richard J. Howell soundly rejected Rajaratnam's argument that the wiretapped conversations should be suppressed because insider trading is not listed as a predicate offense.[73] According to the court, the government can use wiretap evidence of crimes not specified in § 2516 if it can show that "the original wiretap order was lawfully obtained, that it was sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order."[74] The court ruled that the government acted in good faith because it candidly revealed its intention to use the wiretap to investigate securities fraud.[75] Furthermore, it held that communications concerning insider trading were intercepted "incidentally" because they were a mere "by-product" of the of the government's lawful investigation into the predicate offense of wire fraud.[76]

However, the court acknowledged that *Rajaratnam* differed from a typical plain-view exception case.[77] Normally, the exception applies when government receives authorization to investigate a predicate offense with a wiretap and then "happens upon" an entirely different crime.[78] In *Rajaratnam*, however, the government clearly expected the wiretap to yield evidence of a non-predicate offense, insider trading.[79]

The court's ruling is troubling in several respects. First, the government appears to have used wire fraud as a pretext to investigate insider trading. This conclusion is supported by the fact that the government never charged Rajaratnam with wire fraud.[80] Judge Howell held that the issuance of a wiretap is not

---

[71] Gelbard v. United States, 408 U.S. 41, 46 (1972).

[72] Kaplan et al., *supra* note 6, at 6.

[73] *Rajaratnam*, 2010 WL 4867402, at *1.

[74] *Id.* at 3.

[75] *Id.* at 4.

[76] *Id.* at 5.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] Craine & Kell, *supra* note 35, at 47.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

contingent upon a specific charge actually being levied against a defendant because a judge issuing a wiretap is unable to foresee which charges will ultimately be brought against the defendant.[81] Nevertheless, the fact that authorities charged Rajaratnam with fourteen different counts of conspiracy and securities fraud—and zero counts of wire fraud—surely suggests that wire fraud served as a pretext to get a wiretap to investigate insider trading. Moreover, the SEC had been investigating Rajaratnam for insider trading as early as 1999, suggesting that insider trading—not wire fraud—had long been the target of the investigation.[82]

The court also erred in holding that the insider trading communications were intercepted "incidentally" by the wiretap. Judge Howell distinguishes between "incidental" and "inadvertent" interceptions.[83] He states that the communications were not intercepted "inadvertently" but holds that they were intercepted "incidentally" and thus lawfully.[84]

Judge Howell draws a false distinction between "incidental" and "inadvertent" interceptions. First, it is hard to believe that these communications could have been intercepted "incidentally" but not "inadvertently" because the two words essentially mean the same thing. "Incidental" is defined as "being likely to ensue as a chance or minor consequence" or "occurring merely by chance or without intention or calculation."[85] "Inadvertent" means "unintentional."[86] Taken together, both words mean "unintentional," "without intention," or "by chance." Furthermore, Judge Howell admits that the Second Circuit has used both words interchangeably in prior decisions, further supporting this article's contention that they mean the same thing.[87] Therefore, given that the two words carry the same meaning and have been used interchangeably by the courts, it is hard to support Judge Howell's conclusion that the communications could somehow be intercepted "incidentally" but not "inadvertently." In short, given that he held that the wiretapped conversations were not intercepted inadvertently, he also should have concluded that they were not intercepted incidentally and thus were unlawful. In

---

[81] United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 WL 4867402, at *4 n.5 (S.D.N.Y. Nov. 24, 2010).

[82] *Id.* at 9.

[83] *Id.* at 5.

[84] *Id.*

[85] *Incidental Definition*, M-W.COM, http://www.merriam-webster.com/dictionary/incidental (last visited Apr. 4, 2013).

[86] *Inadvertent Definition*, M-W.COM, http://www.merriam-webster.com/dictionary/inadvertent (last visited Apr. 4, 2013).

[87] *Rajaratnam*, 2010 WL 4867402, at *5.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

reality, the communications concerning insider trading were intercepted intentionally, not incidentally or inadvertently, because the government had been investigating Rajaratnam for years and tapped his phone with the specific purpose of discovering evidence of insider trading.[88]

More importantly, the court's ruling is at odds with the policy behind Title III. The statute grants the government limited, not absolute, wiretap authority.[89] Congress feared that if Title III were construed too broadly and wiretap authority were granted too freely, the statute may essentially become "the electronic equivalent of a general search warrant," thereby allowing the government to eavesdrop on almost any conversation it desired.[90] "The purpose of the legislation . . . was effectively to prohibit . . . all interceptions of oral and wire communications, except those specifically provided for in the Act. . . ."[91] "Although Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern."[92] "It was recognized that unless stringent detail were required the government might obtain an overly broad wiretap authorization for one offense as a pretext for gaining information with respect to offenses . . . for which wiretap authorization would be unavailable."[93] Given that the legality of wiretaps for insider trading investigations is unclear at best, and that Congress clearly intended to limit the government's wiretap authority, the *Rajaratnam* court errs by giving the benefit of the doubt to the government and not the defendant.

Moreover, the absence of securities fraud or insider trading from the list of predicate offenses is not a mere oversight by Congress. Congress has amended Title III in the past when it concludes that law enforcement needs greater wiretap authority.[94] For example, the list of predicate offenses was expanded to include bank fraud in 1990, aircraft parts fraud in 2000, and computer fraud in 2001.[95] Thus, until securities fraud or insider trading expressly appear on the list of

[88] Kaplan et al., *supra* note 6, at 9.

[89] United States v. Brodson, 528 F.2d 214, 216 (7th Cir. 1975).

[90] *Id.* at 215.

[91] United States v. Giordano, 416 U.S. 505, 514 (1974).

[92] Gelbard v. United States, 408 U.S. 41, 48 (1972).

[93] United States v. Masciarelli, 558 F.2d 1064, 1067 (2d Cir. 1977).

[94] United States v. Rajaratnam, No. 09 Cr. 1184 (RJH), 2010 WL 4867402 n.8 (S.D.N.Y. Nov. 24, 2010).

[95] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

predicate offenses, it should be concluded that Congress does not wish to grant law enforcement wiretap authority for these crimes.[96]

Finally, although the *Rajaratnam* court does not hold that the securities fraud is a predicate offense, its ruling ultimately has this effect.[97] In the court's view, as long as the government can create a good faith case of wire fraud, it can prove that an investigation into securities fraud or insider trading was not a subterfuge search.[98] Since the court has set an extremely low bar for demonstrating a good faith case of wire fraud—all the government must do is candidly reveal how it intends to use the wiretap—insider trading has effectively been transformed into a predicate offense.

Subsequent cases have justified this concern. In *United States v. Gupta*, a case involving the prosecution of Rajaratnam's associate, the court interpreted Judge Howell's opinion in *Rajaratnam* as follows: "[so] long as the Government acts in good faith with respect to informing the Court of the crimes it is investigating and learning of in connection with the wiretap . . . the Government is free to use evidence obtained from an authorized wiretap in the prosecution of a non-predicate crime. . . ."[99]

The *Rajaratnam* court also ruled that it made little sense to distinguish between wire fraud and securities fraud, noting, "unlikely is the insider trading scheme that uses no interstate wires."[100] Because it concluded that the two crimes are essentially one and the same, the court held that government did not use wire fraud as a pretext to investigate insider trading.[101] However, securities fraud and wire fraud are comprised of different elements, a fact Judge Howell ultimately acknowledges.[102] Simply put, wire fraud and securities fraud are two separate crimes, and only wire fraud is listed as a predicate offense under § 2516 of Title III.[103]

---

[96] *Id.*

[97] *Id.* at 6.

[98] *Id.*

[99] United States v. Gupta, No. 11 Cr. 907 (JSR), 2012 WL 1066817 at *1 (S.D.N.Y. 2012).

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

[101] *Id.*

[102] *Id.*

[103] 18 U.S.C. § 2516 (2006).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu

V. RECOMMENDATIONS AND CONCLUSION

Given the *Rajaratnam* court's dubious reasoning, the government's authority to investigate insider trading with a wiretap is questionable at best and illegal at worst. However, insider trading is a crime worth fighting, for it undermines public confidence in the financial markets, increases risk for average investors, and creates an unfair advantage for corporate insiders.[104]

As it stands, the law does not permit the government's use of wiretaps to investigate insider trading in a case like *Rajaratnam*. To be sure, other factual circumstances may lead to a different conclusion, such as when evidence of insider trading is truly uncovered "incidentally" or "inadvertently" during a lawful wiretap investigation. Nonetheless, Congress should add securities fraud to the list of predicate offenses in § 2516 of Title III. This would give law enforcement clear authority to investigate insider trading with a wiretap. As Judge Jed Rakoff wrote in *United States v. Gupta*: "The simple truth is that . . . insider trading cannot often be detected, let alone successfully prosecuted, without the aid of wiretaps."[105] If Congress determines that the benefits of prosecuting insider trading rings exceeds the privacy concerns raised by wiretaps, then insider trading should be added as a predicate offense under § 2516.

Such a decision could have privacy implications for millions of Americans. With more cell phones being used and more wiretaps being placed on those cell phones than ever before, one can reasonably wonder whether the benefits of increased government surveillance outweighs the potential violations of individual privacy. Rather than having the courts struggle to set the boundaries on the government's wiretap power in insider trading investigations, Congress should give law enforcement express authority. Until then, however, courts should abide by the clear language of the statute.

[104] *Why Insider Trading is Hard to Define, Prove, and Prevent*, KNOWLEDGE @ WHARTON, http://www.knowledgeatwharton.com.cn/index.cfm?fa=printArticle&articleID=2140&languageid=1 (last visited Apr. 6, 2013).

[105] United States v. Gupta, No. 11 Cr. 907 (JSR), 2012 WL 1066817 at *3 (S.D.N.Y. 2012).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.122 ● http://tlp.law.pitt.edu