Unconventional Investigative Techniques in White Collar Cases: Wiretaps, Search Warrants, and Sting Operations.

Robert H. Hotz, Jr. and Harry Sandick[1]

I. Introduction

The federal government has resorted to unconventional investigative techniques previously reserved for combating narcotics traffickers and organized crime figures in several recent high profile white collar cases. For example, last year, the United States Attorney for the Southern District of New York spoke out publicly in favor of the increased use of wiretaps by the federal government in insider trading investigations. Describing "inside information" as a "financial steroid," he said "every legitimate tool" at law enforcement's disposal was needed to combat it, including wiretaps.[2] In a speech to the Practising Law Institute, the Assistant Attorney General of the Criminal Division said that the Department of Justice ("DOJ") had hired more attorneys to review and approve wiretap applications.[3] In addition, in November 2010, FBI agents executed coordinated search warrants at a number of hedge funds in connection with an insider trading investigation into the use of so-called "expert network[s]."[4] Further, in January 2010, 22 individuals were charged with violations of the Foreign Corrupt Practice Act ("FCPA") in

---

[1] The authors gratefully thank Dan Fisher of Akin Gump Strauss Hauer & Feld LLP and Frank Cavanagh of Patterson Belknap Webb & Tyler LLP for their significant contributions to the preparation of this paper.

[2] Mark DeCambre, *Taped Crusader*, NEW YORK POST, Oct. 22, 2010, http://www.nypost.com/p/news/business/taped_crusader_IjhonU7UjaE5vH7C8koS2M. ("In some respects, inside information is a form of financial steroid. It is unfair; it is offensive; it is unlawful; and it puts a black mark on the entire enterprise," the 42-year-old lawman noted). Perhaps underscoring the limits of the steroid analogy, thankfully the use of inside information does not appear to cause the same harmful side effects as steroid use. *See Barry Bonds' former mistress testifies to changes in his body and temperament*, NEW YORK POST, March 28, 2011, http://www.nypost.com/p/news/national/barry_bonds_former_mistress_testifies_N5cWDyYWoTijqHPQPhdpWK (reporting that Bonds' former mistress testified that "between 1999 and 2001, Bonds' body went through a transformation. She said he got much bigger overall during that time, which was noticed by many. What was not so visible, she said, was that he developed acne on his back and shoulders and his testicles shrank.").

[3] *See DOJ Strengthening Its Fraud Section, Wiretap Unit*, WALL ST. J., Nov. 4, 2010, http://blogs.wsj.com/corruption-currents/2010/11/04/doj-strengthening-its-fraud-section-wiretap-unit/tab/. For a complete copy of the speech see DOJ, "Assistant Attorney General Lanny A. Breuer Speaks at Practising Law Institute" (Nov. 4, 2010), *available at* http://www.justice.gov/criminal/pr/speeches/2010/crm-speech-101104.html. ("[W]e have begun increasingly to rely, in white collar cases, on undercover investigative techniques that have perhaps been more commonly associated with the investigation of organized and violent crime. As part of this effort, we have significantly strengthened the Criminal Division's Office of Enforcement Operations (known as OEO), which is the office in the Justice Department that reviews and approves all applications for federal wiretaps from across the country . . . . and we've substantially increased the number of attorneys at OEO who review these wiretap applications . . . .").

[4] *See* Matthew Goldstein and Jonathan Stempel, *FBI raids 3 hedge funds in insider trading case*, REUTERS, Nov. 22, 2010, http://www.reuters.com/article/2010/11/22/us-hedgefunds-fbi-idUSTRE6AL4DT20101122. ("The FBI raided three hedge funds as part of a widening probe into suspected insider trading in the $1.7 trillion hedge fund industry.").

a massive undercover sting operation conducted by the FBI in which federal agents posed as corrupt foreign officials seeking bribes in return for lucrative defense contracts.[5]

At the risk of stating the obvious, these techniques can be devastating both to individuals and businesses. A defendant's voice on a wiretap engaged in criminal activity when he thought no one was listening is extremely powerful evidence, as there are "[f]ew things jurors find more persuasive than the defendant's own voice."[6] The strength of such surveillance is magnified when accompanied by visual evidence. Consider, for example, the effect of a video-tape of the defendant caught red-handed as part of a sting operation making a bribe to an undercover agent. As for businesses, it is hard to imagine a more damaging blow to a business enterprise than having all of its documents and computers taken away by a team of federal agents. Particularly if the business is small, a search warrant may kill the business before any indictments are returned. For defense counsel, representing white collar clients in this new era of enforcement poses unique and daunting challenges.

The use of these techniques in white collar cases raises many interesting legal and factual issues that this panel will explore. Before delving into these topics, a basic familiarity with the applicable legal standards for wiretaps, search warrants, and undercover operations is required.[7]

II. Wiretaps

Although currently in vogue, wiretapping was once controversial and viewed by some as an enormous invasion of individual liberty and privacy. Justice Brandeis observed more than 80-years ago, "[a]s a means of espionage, writs of assistance and general warrants[8] are but puny instruments of tyranny and oppression when compared with wiretapping." *Olmstead v. United States*, 277 U.S. 438, 476 (1928) (Brandeis, J. dissenting).[9] The Supreme Court subsequently noted, "[f]ew threats to liberty exist

---

[5] *See* DOJ, Office of Public Affairs, "*Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme*" (Jan. 19, 2010), *available at* http://www.justice.gov/opa/pr/2010/January/10-crm-048.html. At the time this paper went to print, the jury had not returned a verdict in a case brought against four of these individuals. The remaining individuals are either awaiting trial or have pleaded guilty.

[6] John W. Schoen, *Rajaratnam verdict may mean more Wall St. crackdowns*, MSNBC.COM, May 11, 2011, *available at*, http://www.msnbc.msn.com/id/42991824/ns/business-us_business/t/rajaratnam-verdict-may-mean-more-wall-st-crackdowns/.

[7] For a detailed discussion of the use of wiretapping, search warrants and undercover operations in federal investigations *see* Diana Parker et al., Defending Federal Criminal Cases § 1A.01[3] (2010).

[8] Writs of assistance and general warrants were used by the British in colonial America in the years preceding the Revolutionary War to conduct searches without probable cause. The evils of these practices were a cause of the American Revolution and the subsequent creation of the Fourth Amendment which prohibited such practices by the federal government. *See* Black's Law Dictionary 1723, 1748-49 (9th ed. 2009).

[9] In his dissent in *Olmstead*, Justice Brandeis eloquently expressed concern about law enforcement use of wiretapping. He wrote that "it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the government's purposes are

which are greater than that posed by the use of eavesdropping devices." *Berger v. New York*, 388 U.S. 41, 63 (1967).

"Mindful of this potential danger, Congress, in enacting Title III of the Omnibus Crime Control Act and Safe Streets Act of 1968, prescribed specific and detailed procedures to ensure careful judicial scrutiny of the conduct of electronic surveillance and the integrity of its fruits." *United States v. Gigante*, 538 F.2d 502, 503 (2d Cir. 1976) (internal citation omitted). This section provides a summary of the federal wiretap statute which is commonly referred to as Title III. *See* 18 U.S.C. § 2516 *et seq*.

A. Federal Statutory Authority for Wiretapping

1. How Wiretaps are Obtained

Title III allows the government to obtain a wiretap *ex parte* from a United States district judge for certain offenses specifically enumerated in the statute. *See* 18 U.S.C. § 2516 (1)(a)-(s).[10] Title III permits a wiretap for an initial period of 30 days; the wiretap can be extended by the reviewing court for subsequent, additional 30-day periods. 18 U.S.C. § 2518(5). Title III does not answer the question of how many such extensions the government may obtain. The statute states only that "[n]o order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objection of the authorization." *Id*. In practice, wiretaps can be extended for many months. According to published statistics for 2010, one wiretap in the Southern District of California was extended six times to complete a 210-day wiretap and another in the District of Alaska was extended for 330 days. *See* AO Wiretap Report 2011 at 7.[11] Those figures pale in comparison to state wiretaps in New York that were in use for 559 and 540 days respectively. *Id*. Although the extraordinary length of these extensions is unusual,[12] the number of extensions granted in a typical wiretap instance is plainly on the rise, as 2010 saw 1,925 extensions requested and authorized, an increase of 18% over 2009. *Id*. at 7.

While many of the offenses specified in Title III evoke images of La Cosa Nostra – murder, racketeering, narcotics trafficking, prostitution, extortion and interstate

---

beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding." *Id*. at 479.

[10] Forty-four states, the District of Columbia and the Virgin Islands also have laws that authorize wiretaps. *See* Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications at 6 (June 2011) (hereinafter "AO Wiretap Report 2011"). New York's electronic surveillance laws are codified in CPL article 700. Those laws are beyond the scope of these materials.

[11] There were similar lengthy wiretap extensions in 2009, with one wiretap in the Southern District of New York extended for 330 days and another in the Eastern District of Michigan extended for 300 days. *See* Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications at 6 (April 2010) at 7-8.

[12] The average length of a wiretap extension in 2010 was 29 days. AO Wiretap Report 2011 at 7.

gambling – there are a number of white collar offenses listed in Title III including, among others, wire fraud, bank fraud, mail fraud, computer fraud, and embezzlement from pension and welfare funds. 18 U.S.C. § 2516(1)(c). Of note, securities fraud (of which insider trading is a subset) is not enumerated as a specified offense, although the Southern District of New York has held that wiretapping for insider trading is permitted under Title III. *See United States v. Rajaratnam*, No. 09-CR-1184, 2010 WL 4867402, at *1 (S.D.N.Y. Nov. 24, 2010). Furthermore, Title III allows the federal government to utilize evidence of crimes other than those specified in the order of authorization or approval obtained through the wiretap, so long as a "judge finds on subsequent application [made as soon as practicable] that the contents were otherwise intercepted in accordance with" Title III. 18 U.S.C. § 2517(5).

2. The Approvals Needed to Obtain Wiretapping Authorization

Title III requires all requests for wiretaps be reviewed and approved by the Department of Justice before they are submitted to the court. *See* U.S. DOJ, U.S. Attorney's Manual § 9-7.100 ("One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval . . . ."); *see also* 18 U.S.C. § 2516(1). The initial review of any such application is conducted by the DOJ's Electronic Surveillance Unit of the Office of Enforcement Operations ("OEO"). U.S. DOJ, U.S. Attorney's Manual § 9-7.110. After the initial review is completed, the application must be reviewed and authorized by a senior official in the DOJ, usually a Deputy Assistant Attorney General. These approvals can be time consuming. The failure to obtain the required approvals within the DOJ requires suppression of the wiretap. *See United States v. Giordano*, 416 U.S. 505, 528 (1974) ("We are confident that the provision for pre-application approval was intended to play a central role in the statutory scheme and that suppression must follow when it is shown that this requirement has been ignored."); *see also* Gordon Mehler et al., Federal Criminal Practice: A Second Circuit Handbook § 16-3 at p. 268 (11th ed. 2011).

3. The Standards for Obtaining a Wiretap: Probable Cause

Under Title III, the government must provide a district court judge with "a full and complete statement of the facts and circumstances relied upon" to establish probable cause that a specified offense has been committed and that the phone that is the subject of the wiretap application has been or will be used to commit that offense. 18 U.S.C. § 2518(1)(b); *see id.* § 3(a) & (b).

Probable cause is a flexible common-sense standard. Probable cause exists when, given the totality of the circumstances, a person of reasonable caution would conclude that a crime is being committed and that the phone in question is being used in furtherance of the crime. *See Rajaratnam*, 2010 WL 4867402, at *6; *see also* Hon. James Cissell, *Federal Criminal Trials* § 2-4[b] (7th ed. 2008) (for discussions of probable cause generally). The probable cause standard does not require the government to establish a *prima facie* case of each element of the crime, but instead requires only a

showing of probability of criminal activity. *United States v. Fea*, No. 10-CR-708, 2011 WL 1346981, at *4 (S.D.N.Y. Apr. 5, 2011); *see United States v. Martin*, 426 F.3d 68, 76 (2d Cir. 2005). In determining whether probable cause exists to authorize wiretapping, a court may consider hearsay statements, including those of a criminal informant. *See United States v. Fiorella*, 468 F.2d 688, 691-92 (2d Cir. 1972); *see generally United States v. Garcia*, No. 04-CR-603, 2005 WL 589627, at *5 (S.D.N.Y. Mar. 14, 2005), *aff'd by summary order*, *United States v. Vazquez*, 223 Fed. App'x 43 (2d Cir. 2007).

There are any number of ways that probable cause can be established linking a specific phone to criminal activity. Federal agents often review all outgoing telephone calls that are dialed from a phone. The method for obtaining outgoing calls is through a "pen register." Federal agents also often review all incoming calls received by a phone. The method for obtaining incoming calls is through a "trap and trace device." These methods identify the outgoing or incoming phone numbers themselves rather than the content of the communications.[13]

The federal government can obtain an order authorizing a pen register or a trap and trace device by an *ex parte* application to a federal magistrate. The application need not establish probable cause; all that is required is that "the attorney for the Government" certify "that the information likely to be obtained . . . is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123 (a)(1). Federal agents can also establish the nexus of the phone to the criminal activity through what is commonly referred to by federal agents as "a dirty call" – that is a recent call on the phone in question in which criminal activity is discussed. Typically, a cooperating witness or confidential informant will supply the evidence of such a call. A common tactic is for a cooperating witness to make a consensually recorded call to the targeted phone number to help establish probable cause.

4. The Standard for Obtaining a Wiretap: Necessity

In addition to establishing probable cause, the government must also provide the district court with 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." *See* 18 U.S.C. § 2518(1)(c). This requirement, which is commonly referred to as the "necessity" requirement, prevents the government from resorting to wiretapping "in situations where traditional investigative techniques would suffice to expose the crime." *United States v. Kahn*, 415 U.S. 143, 153 n.12 (1974). The necessity requirement is not merely a rubber stamp. "[G]eneralized and conclusory statements that other investigative procedures would prove unsuccessful" do not suffice to establish necessity for a wiretap. *United States v. Lilla*, 699 F.2d 99, 104 (2d Cir. 1983). The wiretap affidavit "must provide some basis for concluding that less intrusive investigative procedures are not feasible." *Id*. at 103. The government is not, however, "required to exhaust all conceivable investigative techniques before resorting to electronic surveillance." *United States v. Concepcion*, 579 F.3d 214, 218 (2d Cir. 2009);

[13] The law permits a pen register or a trap and trace device for an initial period of 60 days, and either can be extended by the reviewing court for subsequent additional 60-day period. *See* 18 U.S.C. § 3123(c).

see also Rajaratnam, 2010 WL 4867402, at *22. The failure of the government to establish necessity can result in suppression of the wire as explained below.

5. Minimization

Once a wiretap authorization is obtained for a particular phone, the federal government is not entitled to eavesdrop on each and every conversation. The calls intercepted must be relevant to the investigation. Title III requires that the eavesdropping "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception . . . ." 18 U.S.C. § 2518(5). Accordingly, conversations that have nothing to do with the criminal activity should not be intercepted. The Supreme Court has articulated an "objective reasonableness" standard for determining whether monitoring agents acted in compliance with Title III's minimization requirement, and stressed the fact-intensive nature of such an inquiry. *Scott v. United States*, 436 U.S. 128, 136-40 (1978) ("Whether the agents have in fact conducted the wiretap in such a manner [of minimizing intercepted calls] will depend on the facts and circumstances of each case.").

6. The Sealing of Title III Material

Title III requires that the recordings made pursuant to a wiretap order and the applications for any order be sealed by the district court. *See* 18 U.S.C. § 2518(8)(a) & (b). The government must follow these procedures or it cannot use the intercepted communications in a criminal trial. To use wiretap evidence, the government must (1) seal the tapes immediately or (2) provide a satisfactory explanation for the delay in obtaining a seal. *See Gigante*, 538 F.2d at 505-06.

7. How Federal Agents Can Use Title III Materials

Title III has express provisions governing how law enforcement officers can use the fruits of a wiretap. *See* 18 U.S.C. § 2517. One question that has arisen in recent cases is whether federal agents or Assistant U.S. Attorneys ("AUSAs") may share the fruits of the wiretap with the United States Securities and Exchange Commission ("SEC") in connection with a parallel civil proceeding. In the Galleon insider trading case, the U.S. Attorney's Office ("USAO") for the Southern District initially took the position before the district court that it could share Title III materials with the SEC, but then changed its position before the Second Circuit and contended that it lacked authority to do so. *See SEC v. Rajaratnam*, 622 F.3d 159, 165 n.1, *see also id*. at 174 n.12 (2d Cir. 2010). Of note, the Second Circuit did not rule on whether the USAO's was correct. *Id*. at 174.

Curiously, it appears that the SEC has the authority to obtain wiretaps through discovery of a defendant in parallel civil litigation even though it cannot get those same materials directly from the USAO. In the Galleon case, the Second Circuit concluded that there was nothing in Title III that prohibited the SEC in a parallel civil litigation from obtaining wiretap materials through conventional civil discovery from the defendants. The Court reasoned that "[w]hile the USAO may not be authorized to provide these

materials to the civil enforcement agency to help it investigate or prosecute a civil case, the civil discovery rules may well give the civil enforcement agency a right to these materials following their release to the defendants, to avoid an informational imbalance that would give the defendants an unfair advantage in the civil proceeding." *Id*. at 174; *see also SEC v. Galleon Mgmt.*, No. 09-CV-8811, 2011 WL 1770631 (S.D.N.Y. May 10, 2011) (ordering defendants to produce wiretapped communications to the SEC). Accordingly, a defendant contemplating the possibility of being subject to a SEC investigation might consider whether it is necessary to request discovery of Title III materials.

8. Challenging a Wiretap for Violation of Title III

Title III permits any "aggrieved person" to move to suppress a wiretap "before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof." 18 U.S.C. § 2518(10)(a). An aggrieved person is defined as "a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." 18 U.S.C. § 2510(11).

a. False Statements in the Application for Wiretap

When a wiretap application fails to satisfy the "full and complete statement" standard with respect to probable cause or necessity, the appropriate remedy is suppression of the intercepted communications. 18 U.S.C. § 2518(10)(a). The mechanism for challenging the wiretap usually takes the form of a *Franks* hearing named after the leading case of *Franks v. Delaware*, 438 U.S. 154 (1978) (Of note, *Franks* did not involve a challenge to a wiretap). "Where a defendant makes a preliminary showing that the government's affidavit misstated or omitted material information," the reviewing court holds "a hearing to determine if the misstatements or omissions were made intentionally or with reckless disregard, and if so, determines *de novo* whether, 'after setting aside the falsehoods, what remains of the warrant affidavit is insufficient.'" *Rajaratnam*, 2010 WL 4867402, at *7 (quoting *United States v. Coreas*, 419 F.3d 151, 155 (2d Cir. 2005)); *see also United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). "[A]llegations of negligence or innocent mistake are insufficient" to satisfy this standard. *Rajaratnam*, 2010 WL 4867402, at *8 (quoting *Franks*, 430 U.S. at 171). Reckless disregard, however, "may be inferred where the omitted information was 'clearly critical' to the probable cause determination." *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991). What constitutes reckless disregard or an intentional falsehood is a question of fact for the court to decide.

The omission of the success of traditional investigative methods may "create the illusion of necessity for the wiretap," and therefore may lead to suppression of the electronic interceptions. *United States v. Simpson*, 813 F.2d 1462, 1472 (9th Cir. 1987) (application misrepresented the extent to which the confidential informant had infiltrated a drug conspiracy); *see United States v. Ailemen*, 986 F. Supp. 1228, 1234-42 (N.D. Cal. 1997) (application misrepresented the usefulness of undercover agents and concealed unpursued leads).

b. Failure to Minimize

The government has the initial burden to show that it properly minimized intercepts. *United States v. Rizzo*, 491 F.2d 215, 217 n.7 (2d Cir. 1974). Once the government makes a *prima facie* showing of minimization, the burden shifts to the defendants to show that "a substantial number of nonpertinent conversations [have] been intercepted unreasonably." *United States v. Menendez*, No. 04-CR-219, 2005 WL 1384027, at *3 (S.D.N.Y. June 8, 2005) (internal quotation marks and citations omitted).

What remedies exist for violations of the minimization requirement under Title III depend on the facts and circumstances of the particular case focusing on the procedures employed by the government to ensure proper minimization and the number of irrelevant conversations intercepted. Generally, when minimization violations occur, the government will not seek to use the improperly intercepted conversations at trial. Therefore, suppression of these calls results in no harm to the government's case in chief because the calls are irrelevant. Such a lenient remedy, however, would seem to provide no deterrent against future minimization violations by the government. In a number of recent cases, defense counsel have argued (unsuccessfully) that the entire wiretap – including properly intercepted calls – should be suppressed because of the claimed egregious nature of the failure to minimize. *See, e.g.*, *United States v. Goffer*, No. 10-CR-0056, 2011 WL 1512326, at *1 (S.D.N.Y. Apr. 20, 2011).

In *Goffer*, the defendant argued that the monitoring agents violated the federal wiretap statute by failing to properly minimize privileged calls between the defendant and his wife, many of which discussed intimate aspects of their relationship. *Id.* at *2. The court agreed that "several of the marital conversations were improperly minimized," and characterized the monitoring agents' failure to minimize as "inexcusable," "disgraceful," and "an embarrassment generally." *Id.* at *5, 7, 8. Nevertheless, the court denied the defendant's motion to suppress the entirety of the wiretap evidence, holding that the government's isolated deficiencies in minimizing the wiretaps were "insufficient to demonstrate the type of 'pervasive disregard of the minimization requirement' that would warrant total suppression." *Id.* at *7 (quoting *United States v. Pierce*, 493 F. Supp. 2d 611, 636 (W.D.N.Y. 2006)). The court further noted that "Title III also provides civil remedies for individuals alleging a failure by the government to properly minimize intercepted conversations." *Id.* at 8 n.5 (citing 18 U.S.C. § 2520).[14]

c. Failure to Seal

"Although sealing may seem like a meaningless ministerial requirement, it is actually a vital step in the wiretap process." Parker, *supra* note 7, § 1A.01[3] (and cases cited therein at n.92). While reviewing courts have accepted numerous justifications for sealing delays, there is authority for the proposition that lengthy unexcused delays require

[14] In *Goffer*, the Court alluded to suppression of the entire wiretap being warranted where the government's attempt at minimization does not meet "a standard of honest effort." *Goffer*, 2011 WL 1512326, at *8 (quoting *United States v. Uribe*, 890 F.2d 554, 557 (1st Cir. 1989)).

suppression. *See Gigante*, 538 F.2d at 504 ("egregious delay" ranging from 8 to 12 months from expiration of the wiretap order and subsequent sealing where government "provided no explanation whatsoever" warranted suppression).

d. Improper Authorization of Wiretap Application

As mentioned above, Title III requires that the Attorney General or a properly-designated subordinate authorize an application for a wiretap. The wiretap order must specify the individual at the Department of Justice who authorized the application. *See* 18 U.S.C. § 2518(4). Authorization of a wiretap by an individual other than a senior official in the Department of Justice may in rare cases lead to suppression of the wiretap. *See, e.g., United States v. Giordano*, 416 U.S. 505, 524-26 (1974) (upholding suppression of wiretap when application was approved by the Attorney General's Executive Assistant).

e. Necessity

Although the legal standards for establishing necessity are stated easily enough, their application can be challenging. Historically, challenges to wiretaps on the basis of failure to demonstrate necessity rarely have been successful, even where the court admits that the factual basis for demonstrating necessity was insufficient or that other techniques may have, in combination, produced adequate evidence. *See United States v. Young*, 822 F.2d 1234, 1237 (2d Cir. 1987); *United States v. Steinberg*, 525 F.2d 1126, 1130 (2d Cir. 1975); *but cf. Lilla*, 699 F.2d at 103-05 (holding that the prosecution did not demonstrate necessity for a wiretap because it failed to specify the facts on which the officer concluded that other investigative techniques would have been futile).

Despite the lack of past success of such challenges, counsel representing defendants in white collar cases where a wiretap has been used should carefully evaluate whether the government has met its burden of establishing necessity. Given the obvious differences between legitimate businesses and criminal enterprises, one might expect a more rigorous showing of necessity to be made to permit a wiretap of a legitimate business. Indeed, specific conventional investigative techniques procedures were contemplated by the Senate when passing Title III as those that might be utilized before resorting to wiretapping: "[N]ormal investigative procedure would include, for example, standard visual or aural surveillance[,] . . . general questioning or interrogation under an immunity grant, use of regular search warrants, and the infiltration of conspiratorial groups by undercover agents or informants." *Lilla*, 699 F.2d at 103 n.5 (quoting S. REP. No. 1097, 90th Cong., 2d Sess. 101, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2190). Presumably, these types of conventional investigative procedures would have an even greater likelihood of success when applied to the investigation of a legitimate business than in the context of a criminal enterprise. Likewise, the risks of danger would appear to be practically nonexistent in the white collar context. Thus, as wiretaps become used more often in white collar cases, practitioners should expect more challenges to wiretaps on grounds of necessity.

f. Probable Cause

As discussed above, a defendant may challenge a wiretap for lack of probable cause because of false or misleading statements in the application for the wiretap. As with challenges to necessity, however, such challenges are often unsuccessful, even where the court points out "inaccuracies and inadequacies" in a supporting affidavit. *Rajaratnam*, 2010 WL 4867402, at *11.

Legal questions can arise, however, as to whether the facts supporting the affidavit are too dated and have thus become "stale" and insufficient to support a probable cause finding. *See* Gordon Mehler et al., *supra* 4 at p. 270 ("A determination as to whether facts have become too 'stale' to support a finding of probable cause depends upon 'the age of those facts and the nature of the conduct alleged to have violated the law.'"); *see also United States v. Domme*, 753 F.2d 950, 953 (11th Cir. 1985) ("As with other types of search warrants, the probable cause needed to obtain a wiretap must exist at the time surveillance is authorized . . . . It does not satisfy the probable cause standard if the government can demonstrate only that the items to be seized could have been found at the specified location at some time in the past."). Therefore, defense counsel should consider staleness as a possible basis to challenge probable cause, particularly where the allegedly "dirty call" was not made on the wiretapped phone close in time to the making of the wiretap application.

B. Practice Observations

The number of state and federal electronic interceptions authorized has generally maintained an increasing trend since the passage of Title III. For example, there were 1,190 authorized wiretaps (479 federal, 711 state) in 2000, but 2,376 (663 federal, 1,713 state) in 2009. *See* http://epic.org/privacy/wiretap/stats/wiretap_stats.html (visited May 6, 2011).

The most recent statistics compiled by the Director of Administrative Office of the United States Courts for fiscal year 2010 indicate that "[d]rug crimes were the most prevalent type of criminal offenses investigated using wiretaps" accounting for "84 percent of all applications for intercepts (2,675 wiretaps)". *See* AO Wiretap Report 2011 at 8. Wiretap investigations are expensive. The average cost of a federal wiretap was approximately $63,556. *Id*. at 9. One wiretap in Massachusetts reportedly cost the state $1,697,030. *Id.* And wiretaps are a huge investment of other resources by the government, requiring a massive number of hours on the part of federal agents and AUSAs. This suggests that wiretaps should be reserved for the most serious investigations.

C. The Future of Wiretaps

The use of wiretaps, both in terms of frequency and in types of cases, appears to be expanding. In light of the government's recent successes in using wiretaps in major insider trading cases, many expect to see the government continue to use wiretaps in

insider trading cases in the future.[15] Indeed, at least one commentator has noted, "the DOJ's use of wiretaps in [the Galleon] case represented a tactical sea change in pursuit of financial malefactors."[16] As the government's reliance on wiretaps in white collar cases increases, necessity and minimization will continue to be major battlegrounds between the government and the defense over suppression of wiretaps.

III. Search Warrants

In a number of recent investigations involving alleged insider trading at hedge funds, the government has used search warrants to gather evidence. The federal government's authority to issue search warrants comes from the Fourth Amendment Guarantee against unreasonable searches and seizures. U.S. Const. amend. IV. The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id*. The procedure for obtaining and executing a search warrant is set forth in Federal Rule of Criminal Procedure 41.

A. Getting Documents the Old-Fashioned Way: Grand Jury Subpoenas

In white collar cases, the conventional method by which the government obtains documents is pursuant to a grand jury subpoena. A grand jury subpoena is issued on the basis of the signature the United States Attorney and need not be approved by any judicial officer. Typically, line assistants have the authority to sign subpoenas on behalf of the U.S. Attorney. The federal government enjoys nationwide service of process for grand jury subpoenas. *See* FED. R. CRIM. P. 17(e); *see generally* Gordon Mehler et al., *supra* 4, § 20-2 at p. 320 ("The grand jury has nationwide subpoena power over persons and documents, and the Supreme Court has protected the unimpeded use of that power."). Failure to comply with a grand jury subpoena can be punishable as contempt of court. *See* FED. R. CRIM. P. 17(g) ("The court (other than a magistrate judge) may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by a federal court in that district."). For these reasons, grand jury subpoenas can be a convenient and cost effective method of getting documents in a criminal investigation.

However, there can be disadvantages to the government in using grand jury subpoenas. There can be delays in obtaining documents pursuant to a grand jury subpoena. These delays are often caused by, among other things, the volume of documents called for production, the need to locate and review responsive documents, and the assertion of privilege with respect to certain documents. Grand jury subpoenas may also be ineffective when there are concerns of destruction of evidence. In certain

---

[15] *See* Dunstan Prial, *Memo to Wall Street Crooks: Hang Up the Phone*, FOX BUSINESS , May 11, 2011, http://www.foxbusiness.com/markets/2011/05/11/memo-insider-traders-hang-phone ("I think prosecutors are salivating at the opportunity to use [wiretaps] in future Wall Street cases and we're going to see them utilized much more going forward.").

[16] Abigail Field, *Sorry, Judge Rakoff: You Can't Give the SEC the Galleon Wiretaps . . . Yet*, DAILYFINANCE.COM, Sept. 30, 2010, *available at* http://www.dailyfinance.com/2010/09/30/galleon-wiretaps-insider-trading-rakoff-overturned-sec-justice-trial.

circumstances, the prosecutor may accelerate the production of documents by issuing what is known as a "forthwith subpoena." Under DOJ policy, "'[f]orthwith' subpoenas should be used only when an immediate response is justified and then only with the prior approval of the United States Attorney." U.S. DOJ, U.S. Attorney's Manual § 9-11.140. A forthwith subpoena, as its name implies, requires immediate compliance. *See United States v. Lartey*, 716 F.2d 955, 962 (2d Cir. 1983) ("Although a subpoena calling for immediate production of documents hampers the ability of one to contest its validity before a judicial officer, we decline to rule that such subpoenas are *per se* illegal. Rather the issuance of a 'forthwith' subpoena may be justified by the facts and circumstances of a particular case.") (citation omitted).

Documents produced pursuant to a federal grand jury subpoena are generally subject to the rule of grand jury secrecy set forth in Rule 6(e) of the Federal Rules of Criminal Procedure. "Prosecutors are not automatically permitted to share grand jury materials with other government attorneys or investigators." Gordon Mehler et al., *supra* 4, § 20-11 at p. 330.[17] By contrast, documents obtained pursuant to a search warrant are not subject to the grand jury secrecy requirements of Rule 6(e), and can be shared with other government agencies.

B. The Application for a Search Warrant

Rule 41 allows the federal government to obtain a search warrant from a federal magistrate within the district where the property to be searched is located. FED. R. CRIM. P. 41(b)(1).[18] An application for a search warrant may be issued to search for and seize any "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained." FED. R. CRIM. P. 41(c).

An application for a search warrant must be accompanied by an affidavit which demonstrates that there is probable cause to search a given location. *See* FED. R. CRIM. P. 41(d). The warrant and affidavit must identify and describe the property to be searched. As a practical matter, descriptions of the premises to be searched are sometimes provided by cooperating witnesses or informants. While the search warrant affidavit usually provides detailed information concerning the government's investigation, it is generally

[17] When there are parallel criminal and civil investigations being conducted into possible securities fraud, the U.S. Attorney's Office does not share materials obtained pursuant to a grand jury subpoena with the SEC. However, there is no prohibition against the SEC sharing the fruits of its subpoenas with the criminal authorities. The Securities Act and Exchange Act both expressly authorize such sharing of information. *See* Securities Act, Section 20(b), 15 U.S.C. § 77t(b); Exchange Act, Section 21(d), 15 U.S.C. § 78u(d). Rule 203.2 of the Commission's Rules Relating to Investigations expressly authorizes SEC staff to release non-public information in the Commission's investigative files to the criminal authorities. 17 C.F.R. Part 203.2. Typically, the criminal authorities file what is known as an "access request" with the SEC to obtain these materials.

[18] Rule 41(b) also permits the federal government to obtain a search warrant by making an application to a state judge in certain instances. *See* FED. R. CRIM. P. 41(b)(1).

filed under seal and is not unsealed until after an indictment is returned and discovery is produced in the underlying criminal case.

Where exigent circumstances are present, Rule 41(d)(3) allows the federal government to dispense with the requirement of a written affidavit and to seek a warrant based upon sworn oral testimony "communicated by telephone or other reliable electronic means." FED. R. CRIM. P. 41(d)(3).

Unlike a wiretap application that requires the government to demonstrate "necessity" for the wiretap, there is no requirement that the government demonstrate that other conventional investigative techniques have failed or are likely to fail before obtaining a search warrant. Thus, the government need not demonstrate that it tried to acquire the evidence sought through the use of grand jury subpoena before obtaining a warrant. A search warrant is issued solely on the basis of probable cause.

1. Rules Concerning the Search and Seizure of Computers

In 2009, Rule 41 was amended to add a new provision concerning searches and seizures of computers and other electronic storage media. The Rule permits warrants for "the seizure of electronic storage media or the seizure or copying of electronically stored information" and "authorizes a later review of the media or information." *See* Fed. R. Crim. P. 41(e)(2)(B). According to the Advisory Committee's Notes, "[t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Advisory Committee Notes 2009 Amendments FED. R. CRIM. P. 41(e)(2). The Rule also makes clear that the 14-day period (or shorter period provided in the search warrant) applies only "to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." FED. R. CRIM. P. 41(e)(2)(B). The new rule "does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development." Advisory Committee Notes 2009 Amendments FED. R. CRIM. P. 41(e)(2).

2. Remedy for False Statements in a Search Warrant Affidavit

As in the case of a wiretap, the remedy for false statements in a search warrant affidavit is suppression of the evidence obtained during the search. The procedure outlined above for a *Franks* hearing is to be followed.

C. The Execution of the Search Warrant

A search warrant must be executed within the time period specified in the warrant; that time period cannot exceed 14 days from the date of the warrant's issuance. Fed. R. Crim. P. 41(e)(2)(A)(i). As a general matter, a search warrant must be executed during the day time (between the hours of 6:00 a.m. and 10:00 p.m.) although the magistrate may permit execution at other times where good cause is shown. FED. R. CRIM. P. 41(a)(2)(B) & (e)(2)(A)(ii).

An agent executing a search warrant will follow the knock-and-announce rule and inform those on the premises that he is a federal agent executing a search warrant. If he is refused entry, the agent "may break open any outer or inner door or window" to execute a search warrant. 18 U.S.C. § 3109; *see* Cissell, *supra* 4, § 2-4(d)(3).

Depending on the scope of the warrant, federal agents may search and seize books and records of a business as well as data stored on its computer network and on individual computer hard drives. Federal agents may copy or "image" the computer network and/or individual computers and leave the originals behind. It should be noted that federal agents are also entitled to seize evidence of criminal activity even though it is not within the four corners of the search warrant as, for example when, contraband or other evidence of criminal activity is within plain view of the searching agents. The application of the "plain view" doctrine to the search of computer files recently has been – and likely will to continue to be – the subject of litigation.[19]

Executing a search warrant of a business provides a tremendous advantage to the federal government. If the search is executed during normal business hours, it is likely that employees will be present who may have witnessed the alleged criminal behavior. Other employees who are subjects or targets of the government's investigation may also be present. During the execution of the search warrant, the government may have an opportunity to interview these employees. The employees may be without counsel and may be unfamiliar with the search warrant process and their rights when dealing with federal agents (including the right to remain silent). Employees may also be particularly vulnerable to government interrogation in the face of such an exercise of government power. Thus, interviews of employees incident to a search warrant can lead to a treasure trove of information for the government.

An agent executing a search warrant must provide a copy of the warrant and a receipt for the property taken. FED. R. CRIM. P. 41(f)(1)(C). The agent is not required to provide a copy of the underlying affidavit. In practice, most warrants remain under seal until after indictments have been returned by the grand jury. The agent must then return

[19] *See, e.g., United States v. Comprehensive Drug Testing, Inc*., 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring) ("When the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium to search for certain incriminating files, or when a search for evidence could result in the seizure of a computer, . . . magistrate judges should insist that the government forswear reliance on the plain view doctrine. . . . If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether.").

the warrant and a copy of the inventory of the property taken from the searched premises to the magistrate. FED. R. CRIM. P. 41(f)(1)(D).

D. Sneak and Peek Warrants

In certain circumstances, federal agents may conduct a covert search – sometimes referred to as a "sneak-and-peek" search or a "delayed-notice" search – without providing a copy of the warrant and receipt of the property taken immediately after the search where reasonable cause exists to delay the notice and approval from the court is obtained. The benefit to law enforcement by using a sneak and peek warrant is obvious – the target of the investigation does not know that his home or office has been searched and therefore, all things being equal, the investigation remains covert.

The rules relating to sneak-and-peek search warrants are set forth in Section 213 of the Patriot Act. *See* 18 U.S.C. § 3103a. Prior to the enactment of Section 213, federal courts had allowed delayed-notice warrants under certain circumstances. *See United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) ("if a delay in notice is to be allowed, the court should nonetheless require the officers to give . . . notice of the search within a reasonable time after the covert entry"); *see also Dalia v. United States*, 441 U.S. 238, 258-59 (1978) (permitting covert entry to install a Title III bug in defendant's office). Section 213 codifies uniform standards for delayed-notice search warrants. Under Section 213, notice of a search warrant can be delayed by court order for an initial period "not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(b)(3). The period of delay "may be extended by the court for good cause shown" provided that "each additional delay should be limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay." *Id*. § 3103a(c).

Judges who receive applications for sneak-and-peek warrants must file a report to the Administrative Office of the United States Courts indicating the nature of the application, whether the application was granted as applied for, modified or denied; the period of delay in giving notice of the search; the number and duration of any extensions delaying notice; and the offense specified in the application. *Id*. § 3103a(d). This data is maintained by the Director of the Administrative Office of the United States Courts who, in turn, issues a report to Congress annually.

On July 2, 2010, the Director's report to Congress indicated that in fiscal year 2009, "judges in 69 districts reported 1,899 requests for delayed notice, including 150 initial requests for delay and 749 for extensions. Six applications were denied, 27 were granted as modified, and the rest were granted as requested." *See* Annual Report of the Director Administrative Office of the United States Courts 19 (2010).

E. Motion for Return of Property

Depending on the size and nature of the business and the scope of the warrant, the execution of a search warrant can be devastating to a business. FED. R. CRIM. P. 41(g) allows a person subject to a search to move the district court to seek the return of

property seized. FED. R. CRIM. P. 41(g). To prevail on a Rule 41(g) motion, "the moving party must demonstrate that (1) he is entitled to lawful possession of the seized property; (2) the property is not contraband; and (3) either the seizure was illegal or the government's need for the property as evidence has ended." *Mendoza v. United States*, No. 10-CV-9002, 2011 WL 1345712, at *1 (S.D.N.Y. Apr. 4, 2011) (internal quotation marks and citations omitted).

F. Privileged Material Seized

When a search of a business is executed, difficult issues can arise with respect to privileged documents taken in the search. "Courts sometimes allow privilege review by government attorneys uninvolved in the matter; they are called a 'privilege team' or 'taint team.'" *See United States v. Myers*, 595 F.3d 338, 341 n.5 (4th Cir. 2010). Some courts have expressed concerns with the practice, noting that "reliance on the implementation of a [taint team], especially in the context of a criminal prosecution, is highly questionable, and should be discouraged." *United States v. Jackson*, No. 07-CR-0035, 2007 WL 3230140, at *5 (D.D.C. Oct. 30, 2007) (quoting *In re Search Warrant for Law Offices Executed on March 19, 1992 and Grand Jury Subpoena Duces Tecum Dated March 17, 1992*, 153 F.R.D. 55, 59 (S.D.N.Y. 1994)).

G. The Future of Search Warrants

As with the use of wiretaps, many expect that the use of search warrants in white collar cases will become more prevalent in the coming years.[20] Because there are fewer procedural and substantive requirements for the government to meet in order to obtain a search warrant as opposed to a wiretap, so too are there fewer available challenges for defense counsel.

IV. Undercover Investigations and the Use of Confidential Informants in White Collar Cases

Undercover investigations, long a crucial component of covert narcotics trafficking and violent crime prosecutions, have been used more recently in white collar criminal cases. In remarks delivered last year, Assistant Attorney General Lanny Breuer stated that the Department of Justice has "begun increasingly to rely, in white collar cases, on undercover investigative techniques that have perhaps been more commonly associated with the investigation of organized and violent crime."[21]

---

[20] *See, e.g.*, Peter Lattman and Azam Ahmed, *F.B.I. Agents Raid 3 Hedge Fund Offices*, N.Y. TIMES, Nov. 22. 2010, *available at* http://dealbook.nytimes.com/2010/11/22/f-b-i-agents-raid-2-hedge-funds-offices/ ("Law enforcement officials at the highest levels of the Justice Department have in recent weeks publicly stated that they would continue to use more aggressive techniques when investigating business fraud").

[21] Lanny A. Breuer, Assistant Attorney Gen., Dep't of Justice, Address at Practising Law Institute on Financial Crisis Fallout 2010: Emerging Enforcement Trends (Nov. 4, 2010), http://www.justice.gov/criminal/pr/speeches/2010/crm-speech-101104.html.

In an undercover investigation, a law enforcement agent will pose as someone engaged in criminal activity. He or she will meet with potential targets of the investigation to discuss a contemplated future crime. The meetings and phone calls between the agent and the target are typically recorded through the use of a hidden recording device. These recordings (audio and sometimes also video) and the government agent's testimony can provide direct evidence of criminal intent, which is often proved only through circumstantial evidence. In some cases, law enforcement will use a confidential informant (who is typically paid by the government) or a cooperating witness (who has been charged with a crime and who is providing assistance to the government in order to reduce his sentence) to pose as the person engaged in criminal activity.

A. Background

Although there appears to be an increase in the prevalence of undercover investigations in white collar cases, it is certainly not an entirely new technique in cases involving public corruption or business crimes. Perhaps the most memorable investigation to use undercover agents was the ABSCAM investigation in the late 1970s, in which FBI agents posed as Arab sheikhs who offered to pay bribes to government officials. ABSCAM led to the conviction of one senator, five members of the House of Representatives, and several other government officials.

Philip Heymann, who oversaw the ABSCAM investigation while serving at the Department of Justice, explained that undercover investigation allows prosecutors to avoid reliance on "[the] testimony of unsavory criminals and confidence men, whose credibility may be questionable and, in any event, can often be destroyed on cross-examination by able defense counsel."[22] Instead, the prosecutors "can muster the testimony of credible law enforcement agents, often augmented by unimpeachable video and oral taps which graphically reveal the defendant's image and voice engaged in the commission of crime."[23]

ABSCAM was subject to criticism by Congress because the sting operation was not aimed at any known, ongoing criminal activity; instead it involved the undercover agent creating a new crime from whole cloth. Some observers expressed concerns that undercover agents were committing illegal activity, that innocent people could be victims of government entrapment, that innocent non-targets could have their reputations damaged, and that legitimate privacy rights could be impaired by the investigations.[24] Courts, however, rejected the argument that ABSCAM violated the Due Process Clause,

[22] Glenn A. Fine, Inspector Gen., Dep't of Justice, The Federal Bureau of Investigation's Compliance With The Attorney General's Investigative Guidelines, (Sept. 2005), at 138 (hereinafter "DOJ-OIG Report") (quoting *FBI Undercover Guidelines: Oversight Hearings Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 97th Cong. 33-48 (1981) (statement of Philip B. Heymann, Assistant Attorney General, Criminal Division, Department of Justice)).

[23] *Id.*

[24] *Id.* at 41-43.

and also concluded that the convicted defendants were not entrapped.[25] Still, courts have periodically expressed concern about the possible harm that an undercover investigation can inflict on innocent third parties who unknowingly may be used as "tools of deception in an undercover operation."[26] Also, as discussed below, courts have enforced the entrapment defense, which places an important limitation on the government's ability to conduct sting operations.

Since ABSCAM, undercover investigations have been employed in a variety of successful white collar prosecutions. One of the best known and most extensive sting operations, "Operation Greylord," was aimed at corruption in the Illinois state courts in Cook County, Illinois. The four-year investigation, conducted in the 1980s, was prompted by a pattern of acquittals that led participants in the criminal courts to believe that certain trials were being fixed. FBI agents posed as prosecutors and defense attorneys in fake cases that were developed for purposes of the investigation, and the agents recorded incriminating conversations with judges and attorneys, successfully demonstrating that some judges routinely accepted bribes in exchange for the dismissal of cases. The investigation resulted in the conviction of 15 judges and 49 lawyers for bribery and tax-related offenses.[27] In response to defense arguments on appeal that challenged the legality of such a complicated sting operation, Judge Easterbook wrote that "[t]he creation of opportunities for crime is nasty but necessary business." *United States v. Murphy*, 768 F.2d 1518, 1529 (7th Cir. 1985).[28]

B. Procedures for Undercover Investigations

In the aftermath of ABSCAM, the Department of Justice promulgated a set of guidelines for the FBI to follow when conducting of undercover investigations ("Guidelines").[29] The Guidelines have been modified to some degree over time, and the most recent version require an FBI supervisor considering whether to authorize a proposed undercover application to weigh the risks and benefits involved in conducting such an operation, including the following:

> (1) The risk of personal injury to individuals, property damage, financial loss to persons or businesses, damage to reputation, or other harm to persons;
> (2) The risk of civil liability or other loss to the government;

---

[25] *See, e.g.*, *United States v. Williams*, 705 F.2d 603, 620 (2d Cir. 1983); *United States v. Myers*, 692 F.2d 823, 837-47 (2d Cir. 1982).

[26] DOJ-OIG Report at 142-44 (citing *Brown v. Nationsbank Corp.*, 188 F.3d 579, 591 (5th Cir. 1999) (holding that it is not "constitutionally permissible for federal agents to inflict damages of innocent non-targets)).

[27] DOJ-OIG Report at 139.

[28] *See also id.* ("The FBI and the prosecutors behaved honorably in establishing and running Operation Greylord.").

[29] DOJ-OIG Report at 42-43.

(3) The risk of invasion of privacy or interference with privileged or confidential relationships and any potential constitutional concerns or other legal concerns;
(4) The risk that individual engaged in undercover operations may become involved in certain illegal acts, such as acts or violence, entrapment, or illegal investigative techniques; and
(5) The suitability of government participation in the type of activity that is expected to occur during the operation.[30]

Undercover operations require the permission of the Special Agent in Charge of the FBI Field Office (or a designated Special Agent in Charge) involved in the operation, and in some circumstances also require the approval from officials at FBI headquarters in Washington, DC.[31]

The Guidelines permit undercover agents to participate in activity that would otherwise be illegal, but with certain limitations. The otherwise illegal activity must be required to obtain information or evidence that is necessary for the success of the investigation, to establish or maintain credibility of a cover identity, or to prevent death or serious bodily injury.[32] The FBI is required to take "reasonable steps" to minimize the undercover agent's participation in illegal activity, and in no event may the agent participate in any act of violence (other than self-defense), initiate or instigate a plan to commit criminal acts that would amount to entrapment, or participate in unlawful investigative techniques (such as illegal wiretapping or searches).[33] The Guidelines require frequent review of undercover operations by FBI supervisors and by the appropriate federal prosecutor.[34]

Entrapment, in particular, it is to be "scrupulously avoided."[35] The Guidelines define entrapment as something that occurs "when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute."[36] The Guidelines also mandate that an undercover agent should not induce an individual to engage in crime unless certain additional conditions are satisfied:

(1) The illegal nature of the activity is reasonably clear to potential subjects; and

---

[30] John Ashcroft, Attorney Gen., Office of the Attorney General, The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (May 2002) (hereinafter "AG Undercover Guidelines"), at 3.

[31] *Id*. at 3-9.

[32] *Id*. at 12-13.

[33] *Id*. at 12.

[34] *See id*. at 17.

[35] *Id*. at 16.

[36] This is consistent with the legal definition of entrapment, as discussed *infra* at IV. E.

(2) The nature of any inducement offered is justifiable in view of the character of the illegal transaction in which the individual is invited to engage; and
(3) There is a reasonable expectation that offering the inducement will reveal illegal activity; and
(4) One of the two following limitations is met:
    i. There is reasonable indication that the subject is engaging, has engaged, or is likely to engage in the illegal activity proposed or in similar illegal conduct; or
    ii. The opportunity for illegal activity has been structured so that there is reason to believe that any persons drawn to the opportunity, or brought to it, are predisposed to engage in the contemplated illegal conduct.[37]

The Guidelines state that they do not create any enforceable rights for defendants.[38] But defendants may point to the fact that an investigation did not follow these Guidelines in order to cross-examine witnesses or to challenge the government's proof.[39]

C. The Use of Confidential Informants

Law enforcement also makes use of confidential informants in covert investigations. Confidential informants are individuals who often were involved in criminal activity, but who now provide information and assistance to agents and detectives. FBI Director, Robert Mueller, has stated that informants give law enforcement "critical intelligence and information we could not obtain in other ways, opening a window into our adversaries' plans and capabilities."[40] The problems inherent in the use of confidential informants in white collar cases are somewhat different from those raised by their use in investigations into narcotics trafficking or organized crime, in that confidential informants in white collar cases are less likely to commit acts of violence or engage in other illegal activity that could endanger the safety of others.[41] Still, it is worth briefly discussing the FBI Guidelines governing the use of confidential

[37] AG Undercover Guidelines, at 16.

[38] *Id*. at 19.

[39] *Cf.* Benjamin Rosenberg & Robert Topp, "FBI Agent's Obligation To Take Notes at Witness Interviews," N.Y.L.J. (Oct. 30, 2006) (stating that an FBI agent's failure to take notes, contrary to FBI procedures, "might support a motion to dismiss the indictment, to preclude a government witness from testifying, or for a particular adverse inference jury instructions; it might also provide fertile ground for cross-examination")

.

[40] DOJ-OIG Report at 65.

[41] *Id*. at 71-72, 85-87 (discussing improper handling of confidential informants in cases involving prosecution of South Boston's Winter Hill Gang and New York's La Cosa Nostra); *see also id*. at 93 (finding systematic deficiencies in how the FBI supervised its confidential informants, finding that there was one or more deficiency in 87% of the confidential informant files that were reviewed).

informants because it is reasonable to expect that their use will increase in white collar cases.

Initially, the FBI must make a suitability determination about whether an individual is suitable to be a confidential informant.[42] The FBI must then consider the extent to which the informant's information can be corroborated and assesses the person's reliability and truthfulness.[43] There are rules about the relationship between the FBI agents involved in the operation and the informant. The agent may not interfere with any investigation of an informant, and he or she shall not exchange gifts or socialize unnecessarily with the informant.[44] Payments to an informant are permitted (and are commonplace), but payments must be recorded and "commensurate with the value . . . of the information he or she provided or the assistance he or she rendered. . . ."[45] The limitations on the informant's ability to engage in illegal activity are similar to the limits placed on undercover agents, and such activity must be pre-authorized in order for it to be legal.[46]

D. Recent Investigations in White Collar Cases Involving Undercover Agents or Confidential Informants

As Assistant Attorney General Breuer has observed, there are many recent white collar cases in which significant evidence was gathered through the use of undercover agents or confidential informants. The following are a selection of some of the best-known cases to use such techniques during the past two years.

- *United States v. Goncalves*, No. 09-CR-335 (D.D.C. Dec. 11, 2009): Breuer specifically referenced this case in his November 2010 remarks. It involves charges brought against 22 defendants (across a total of 16 indictments) for violations of the Foreign Corrupt Practices Act. The charges arose out of an attempt to bribe undercover FBI agents who were posing as foreign officials from African nations who had the authority to enter into contracts to sell military equipment.[47] At the time of the initial arrests, DOJ officials stated that "[t]his ongoing investigation is the first large-scale use of undercover law enforcement

[42] This is a multi-faceted question that looks at many factors including the relationship between the informant and the target of the investigation, and the informant's motivation for providing assistance or information, including the consideration sought from the government. *See* John Ashcroft, Attorney Gen., Office of the Attorney General, The Attorney General's Guidelines Regarding The Use of Confidential Informants (May 2002) (hereinafter "AG CI Guidelines) at 8-9.

[43] *Id*. at 9.

[44] *Id*. at 17.

[45] *Id*. at 17-18.

[46] *Id*. at 19-22.

[47] Press Release, Dep't of Justice, Twenty-Two Executives and Employees of Military and Law Enforcement Products Companies Charged in Foreign Bribery Scheme (Jan. 19, 2010), http://www.justice.gov/opa/pr/2010/January/10-crm-048.html.

techniques to uncover FCPA violations[.]"[48] Invoking the possibility of future undercover investigation in the FCPA area, DOJ officials warned "would-be FCPA violators [to] stop and ponder whether the person they are trying to bribe might really be a federal agent."[49] In the course of the investigation, one FBI agent posed as "Jean-Pierre Mahmadou," supposedly a procurement adviser to the defense minister of Gabon.[50] At the trial of four defendants, defense counsel focused their jury addresses on alleged misconduct by the FBI and its paid informants in the course of the investigation.[51] The defense alleged that a confidential informant who assisted in the investigation lied repeatedly to one defendant when he stated that illegal payments were, in fact, legal. The defense contended that, absent such assurances, the defendant would not have made the payments.[52]

- *United States v. Cook*, No. 10-CR-00075 (D. Minn. Mar. 30, 2010): This is the other case to which Breuer made specific reference in his November 2010 comments. Trevor Cook was convicted of participating in a scheme to defraud at least 1,000 people out of approximately $190 million by pretending to sell them investments in a foreign currency trading program, while he was keeping the investors' money or using it to pay off earlier investors. During the course of the investigation, a confidential informant attended at least 10 meetings with Cook and his associates, wearing two microphones and carrying a hidden camera.[53] These recordings of the informant's dealings with Cook provided key evidence for the prosecution.[54]

- *United States v. Chu*, No. 10-MAG-2625 (S.D.N.Y. Nov. 23, 2010): Although the ongoing investigation into insider trading committed through the use of expert networking firms has relied heavily on wiretap evidence, it also has involved the use of cooperating witnesses and informants. Chu, who was employed at Primary

---

[48] *Id*.

[49] *Id*.

[50] Christopher Norton, *FBI Agent Details Undercover Role in Gabon FCPA Case*, LAW 360, Jun. 2, 2011, http://www.law360.com/topnews/articles/248903/fbi-agent-details-undercover-role-in-gabon-fcpa-case (subscription required).

[51] Christopher Norton, *FBI's Tactics in Gabon FCPA Sting Come Under Fire*, LAW 360, Jun. 22, 2011, http://www.law360.com/articles/253246/fbi-s-tactics-in-gabon-fcpa-sting-come-under-fire; *see also* Mike Scarella, *DOJ Sting Denounced–Defense Lawyers Say FBI Scripted Bribery Deal Just To Prosecute It*, NAT'L L.J., Mar. 28, 2011, http://www.nlj-digital.com/nlj/20110328/?pg=23 (subscription required) (quoting defense attorneys who argued that the government's informant misled the defendants by claiming the deal was legal and approved by the State Department).

[52] Christopher Norton, *Gabon FCPA Informant Told Execs Deal Was Legal: FBI*, LAW 360, Jun. 9, 2011, http://www.law360.com/articles/250367/gabon-fcpa-informant-told-execs-deal-was-legal-fbi (subscription required).

[53] Edward Wyatt, *Whistle. Then Worry and Wait*, N.Y. TIMES, Oct. 9, 2010, *available at* http://www.nytimes.com/2010/10/10/business/10whistle.html?scp=1&sq=trevor%20cook&st=cse.

[54] Breuer, *supra* note 21.

Global Research, an expert networking firm, was arrested[55] in part based on his dealings with Richard Choo-Beng Lee, a hedge fund employee who was also (unbeknownst to Chu) a cooperating witness working with the U.S. Attorney's Office in the Southern District of New York.[56]

- *United States v. Bell*, No. 10-CR-80107 (S.D. Fla. Aug. 5, 2010): This prosecution of 24 defendants across several indictments resulted from a two-year undercover investigation into a Boca Raton loan brokerage firm. An undercover agent paid bribes to defendants in exchange for obtaining fraudulent loans or receiving false deposit verifications. The undercover agent also asked bankers to launder funds that were described as drug proceeds. Finally, the undercover investigation also led to the discovery and prosecution of an identity theft ring.[57]

- *United States v. Horohorin*, No. 09-CR-00305 (D.D.C. Nov. 12, 2009): Horohorin was accused of wire fraud, and later arrested,[58] after he directed undercover Secret Service agents to a website that he operated for purposes of selling stolen credit card information.[59] Horohorin advertised himself as a seller of stolen credit card information for approximately eight years. Agents purchased seventy-one credit card numbers from Horohorin's website, for a total of approximately US $2,323.

E. Entrapment and Other Limitations On Undercover Investigations

1. The Entrapment Doctrine

The most important restriction on the government's authority to conduct undercover investigations is the entrapment doctrine. As the Supreme Court has held, "[g]overnment agents may not originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the [g]overnment may prosecute." *Jacobson v. United States*, 503 U.S. 540, 548 (1992) (quoting *Sorrells v. United States*, 287 U.S. 435, 441 (1932)). When the government engages in entrapment, its conduct can become "as objectionable police methods as the coerced confession and the unlawful search." *Sherman v. United States*,

---

[55] Complaint, United States v. Chu (No. 10-MAG-2625) (S.D.N.Y. Nov. 23, 2010), *available at* http://blogs.reuters.com/felix-salmon/files/2010/11/complaint.pdf (last visited Jun. 27, 2011).

[56] *Id.*; *see also* Steve Johnson & Pete Carey, *First Arrest in Unfolding Inquiry*, SAN JOSE MERCURY NEWS, Nov. 25, 2010, *available at* 2010 WLNR 23588144.

[57] Press Release, United States Attorney's Office, S.D. Fla., Long-Term FBI Undercover Operation Nabs A Total of 24 Defendants (Jan. 12, 2011), http://www.justice.gov/usao/fls/PressReleases/110112-03.html.

[58] Indictment, United States v. Horohorin (No. 09-CR-00305) (D.D.C. Nov. 12, 2009), *available at* http://www.wired.com/images_blogs/threatlevel/2010/08/BadB-Indictment-in-DC.pdf.

[59] Spenser S. Hsu, *French Arrest Cyber-Crime Suspect for U.S.*, WASH. POST, Aug. 12, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/08/11/AR2010081105791.html; *see also* Press Release, Dep't of Justice, Alleged International Credit Card Trafficker Arrested in France on U.S. Charges Related to Sale of Stolen Card Data (Aug. 11, 2010), http://www.justice.gov/opa/pr/2010/August/10-crm-921.html.

356 U.S. 369, 372 (1958). The courts have recognized that "a line must be drawn between the trap for the unwary innocent and the trap for the unwary criminal." *Id*.

Entrapment is an affirmative defense that is proved in two stages. First, the defendant must carry his or her burden of showing that he was induced to commit the crime by the government. *See, e.g.*, *United States v. Brand*, 467 F.3d 179, 189 (2d Cir. 2006). If the defendant makes this initial showing, the government can rebut his showing by proving—beyond a reasonable doubt—that the defendant was predisposed to commit the crime. *Id*. This second inquiry asks whether the defendant was "ready and willing[,] without persuasion" to commit the crime, simply "awaiting any propitious opportunity[.]" *United States v. Mayo*, 705 F.2d 62, 67 (2d Cir. 1983).

a. Inducement

To prove inducement, the defendant only needs to show that it was the government who originated "the criminal design." *Brand*, 467 F.3d at 189 (quoting *Jacobson*, 503 U.S. at 548). The Second Circuit has described the defendant's burden as "relatively slight." *Mayo*, 705 F.2d at 67. The defendant satisfies this prong by proving that "[it was] the prosecution [that] set the accused in motion[.]"*United States v. Sherman*, 200 F.2d 880, 883 (2d Cir. 1952). In many cases, this will be relatively easy to establish, as the undercover agent or confidential informant proposes the commission of the crime. *Brand*, 467 F.3d at 190.

b. Predisposition

The defendant's predisposition to commit a crime is ordinarily proved in one of three ways: "(1) an existing course of criminal conduct similar to the crime for which [the defendant] is charged, (2) an already formed design on the part of the accused to commit the crime for which he is charged, or (3) a willingness to commit the crime for which he is charged as evidenced by the accused's ready response to the inducement." *United States v. Brunshtein*, 344 F.3d 91, 101-02 (2d Cir. 2003) (quoting *United States v. Salerno*, 66 F.3d 544, 547 (2d Cir. 1995)). The Supreme Court has held that it is not sufficient to show that the defendant had a "generic inclination to act within a broad range, not all of which is criminal[.]" *Jacobson*, 503 U.S. at 550. Rather, the government must show predisposition to commit a crime, and not merely a predisposition to engage in bad acts that were similar in some regard to the charged crime. Also, the defendant must have had a predisposition to commit a crime prior to the initiation of the government's investigation. *Id*. at 549 n.2. When a defendant does not have a prior criminal record, the defendant's "ready response" is the most common way in which the government will prove predisposition. *Brand*, 467 F.3d at 192-93 & n.8 (explaining that the government is not forced to rely exclusively on past criminal conduct in proving predisposition, but that it may also prove predisposition by showing that the defendant "jumped" at the opportunity to commit a crime).

2. Outrageous Government Conduct

Separate and apart from the entrapment defense, a court may dismiss an indictment in that rare case in which "the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction." *United States v. Russell*, 411 U.S. 423, 431-32 (1973); *see also United States v. Schmidt*, 105 F.3d 82, 91 (2d Cir. 1997) (stating that "[p]olice overinvolvement in crime would have to reach a demonstrable level of outrageousness before it could bar conviction") (quoting *Hampton v. United States*, 425 U.S. 484, 495 n.7 (1976)). As Judge Friendly explained, "there is a limit to allowing governmental involvement in crime," as it would be "unthinkable . . . to permit government agents to instigate robberies and beatings merely to gather evidence to convict other members of a gang of hoodlums." *United States v. Archer*, 486 F.2d 670, 677 (2d Cir. 1973).

This doctrine is based on the constitutional right to due process of law. By contrast, entrapment is based not on principles of constitutional law, but is derived from "the notion that Congress could not have intended criminal punishment for a defendant who has committed all elements of a proscribed offense but was induced to commit them by the government." *United States v. Taylor*, 475 F.3d 65, 69 (2d Cir. 2007) (quoting *United States v. Russell*, 411 U.S. 423, 435 (1973)). Given this difference, the court may still dismiss an indictment if it finds outrageous governmental conduct even where the jury rejects an entrapment defense. *See United States v. Cuervelo*, 949 F.2d 559, 565 (2d Cir. 1991). While this doctrine is infrequently invoked, only very extreme facts have led to the dismissal of indictments.[60]

V. Conclusion

The government's use of unconventional investigative techniques has been hailed in the press. In a string of recent high-profile cases, these techniques have uncovered devastating evidence that would likely have gone undiscovered without them. As this paper has shown, the current state of the law in the area of unconventional investigative

[60] *See, e.g.*, *United States v. Twigg*, 588 F.2d 373, 381-82 (3d Cir. 1977) (dismissing indictment where informant and agents violated "[f]undamental fairness" when they set up drug lab for defendant, provided essential supplies and technical assistance and assisted defendant in overcoming technical problems); *United States v. Sabri*, 973 F. Supp. 134, 146-47 (W.D.N.Y. 1996) (dismissing indictment where defendant's immigration lawyer functioned as a confidential informant for law enforcement; "[a]s a general matter, the use of informants is a prevalent, effective and legitimate investigative technique[, but] this does not mean there are no limits as to how and when the technique is employed"); *United States v. Marshank*, 777 F. Supp. 1507, 1523-24 (N.D. Cal. 1991) (dismissing indictment where defendant's lawyer provided information to prosecutors and agents); *see also United States v. Nolan-Richardson*, 155 F.3d 221, 232-35 (3d Cir. 1998) (recognizing doctrine but declining to dismiss indictment where undercover agent engaged in sexual intercourse with defendant during course of investigation); *United States v. Cuervelo*, 949 F.2d at 567 (setting forth standard for when an indictment is to be dismissed based on outrageous governmental misconduct when a sexual relationship exists between a defendant and a governmental agent); *United States v. Smith*, 924 F.2d 889, 897 (9th Cir. 1991) (declining to dismiss indictment where undercover agent encouraged defendant, then a patient in a drug treatment center, to deal drugs).

techniques – wiretaps, search warrants and sting operations – is highly favorable to the government. While it is no doubt hard to argue with the government's recent successes, the use of these techniques raises the specter that they will be misused in the future. Indeed, the recent challenges to wiretaps in high profile cases revealed significant failures by the government to comply with Title III's strictures. Courts should closely examine the government's justifications for probable cause and necessity given the *ex parte* nature of these proceedings and defense counsel's inability to challenge the government's assertions at the time of the application. As a practical matter, judges may be less likely to overturn a prior finding of probable cause or necessity in a case where electronic surveillance uncovers significant criminal activity. Rather than focus on these issues only in hindsight, after the eavesdropping has occurred, judges should focus on these safeguards before the wiretap is authorized. In the meantime, defense counsel have a tough road ahead of them as these unconventional investigative techniques gain greater acceptance.