



WHITE COLLAR CRIME REPORT



VOL. 4, NO. 8

APRIL 10, 2009

Reproduced with permission from White Collar Crime Report, 4 WCR 266, 04/10/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

ELECTRONIC SURVEILLANCE

Someone's Listening: How Wiretaps Can Transform High-Profile White Collar Investigations

By PATRICK COLLINS

When the criminal charges against former Illinois Gov. Rod Blagojevich (D) were first unveiled in December, the most explosive allegations and revelations about the governor's alleged corruption stemmed from conversations acquired pursuant to a 40-year-old federal statute. These conversations, as outlined in the original complaint from the U.S. Attorney's Office for the Northern District of Illinois, provided dra-

matic evidence against Blagojevich, accelerated the government's "pay to play" investigation, and have caused, or likely will cause, countless headaches for those intercepted. Even at its earliest stages, the Blagojevich case underscores the strategic use of wiretaps as an important aspect of federal prosecutors' investigative arsenal.

Federal Wiretap Act

The Federal Wiretap Act was enacted in 1968 as part of an omnibus crime control bill. Traditionally, wiretaps have been used primarily in investigations of gangs, drug syndicates, and organized crime, but there is nothing in the statutory framework that precludes their use in white collar cases. The U.S. Attorney for the Northern District of Illinois's strategic, yet consistent, use of wiretaps in public corruption investigations provides a salient example of how an aggressive prosecutor can use this powerful tool with great effect. In addition to the Blagojevich matter, recorded conversations were critical to that office's Operation Safe Road, an eight-year investigation that led to more than 75 convictions and culminated in the successful prosecution and conviction of former Illinois Gov. George Ryan (R). In fact, in my years as deputy chief of the public corruption section of the U.S. Attorney's Office for the Northern District of Illinois under Patrick Fitzgerald, virtually every significant corruption case obtained a major break-

Patrick Collins is a partner in the Chicago office of Perkins Coie LLP and leads the firm's Investigations and White Collar Defense practice. A former federal prosecutor, he specializes in representing companies and individuals in complex civil and criminal matters and in sensitive probes before various U.S. Attorneys' Offices and the Securities and Exchange Commission, and he advises clients on other significant legal matters, including the Foreign Corrupt Practices Act.

The author would like to acknowledge Jonathan R. Buck, who assisted in the writing of this article. Buck, an associate in Perkins Coie's Chicago office, is a member of the firm's Investigations & White Collar Defense practice.

through as a result of wiretapped conversations. Wiretapped conversations have also played significant roles in high-profile investigations and prosecutions in other jurisdictions, including prosecutions of former U.S. Sen. Ted Stevens (R-Alaska) and former U.S. Rep. Rick Renzi (R-Ariz.), among others.²

A Perfect Storm. Use of wiretaps in high-profile corruption prosecutions spotlights a dramatic tool that could be deployed in another type of white collar investigation as well: white collar corporate fraud.

The economic crisis, revelations of massive Ponzi schemes, such as those involving Bernard Madoff and R. Allen Stanford, and demands by the public, media, and politicians for increased financial accountability have created a perfect storm that demands a greater focus on corporate fraud investigations. The government's distribution of billions of dollars in stimulus funds only heightens the likelihood that aggressive prosecutorial techniques will be used to combat corporate fraud. Indeed, there is an increasingly loud drumbeat for more aggressive white collar investigations from politicians such as Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.), who has said he "want[s] to see people prosecuted." Moreover, Justice Department and FBI officials recently have committed to devote more resources to business fraud cases.³

The use of wiretaps in corporate fraud cases has been relatively rare in the past. However, as the focus on white collar crimes continues to sharpen, many prosecutors may now turn to wiretaps as one of the most powerful investigative tools available to them. It is therefore crucial for practitioners to understand the foundations of wiretap authority and the potential impact of electronic surveillance on high-profile white collar prosecutions.

Standards for Constitutional Electronic Surveillance Established

The Federal Wiretap Act was enacted as part of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).⁴ The adoption of the act followed the U.S. Supreme Court's decisions in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967), which established standards for constitutional electronic surveillance. The dual purpose of the act was "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be autho-

² At the time of publishing, the prosecutions of Blagojevich and Renzi were pending at different stages of litigation. On April 7, a federal court overturned Stevens's conviction on the basis of prosecutorial misconduct.

³ Carrie Johnson, *Justice Department Putting New Focus on Combating Corporate Fraud*, Washington Post, Feb. 12, 2009, at A6.

⁴ This article does not address wiretaps authorized under the Foreign Intelligence Surveillance Act of 1978, which originally permitted wiretapping of aliens and citizens in the United States under certain circumstances involving investigations of foreign terrorist groups and agents of foreign powers. The USA PATRIOT Act later expanded FISA to allow intercepts in investigations of national security crimes.

itized."⁵ Congress later expanded the scope of permissible wiretaps with the Electronic Communications and Privacy Act of 1986, which covers interception of electronic communications such as cellular phone conversations. Although many states also have laws that authorize wiretaps, historically most white collar cases have been investigated and prosecuted at the federal level. The Federal Wiretap Act, as amended, is codified at 18 U.S.C. §§ 2510-2522.

Wiretaps under Title III require a warrant. The attorney general or an assistant attorney general may authorize a wiretap application to a federal judge when an interception may provide evidence of various enumerated offenses, which notably include mail fraud, wire fraud, and various financial crimes.⁶ Each application must be made in writing and must include the identity of the applicant as well as a "full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued," including details of (i) the particular offense that has been or is about to be committed; (ii) a description of the nature and location of where the interception will take place; (iii) the type of communications sought to be intercepted; and (iv) the identity of the person, if known, committing the offense and whose communications will be intercepted.⁷ Information about previous related applications and the anticipated period of time the intercept will be in place must also be provided.⁸ To obtain court approval, a judge must find there is probable cause to believe that an individual is committing, has committed, or is about to commit one of the enumerated predicate offenses *and* probable cause to believe that communications concerning the offense will be obtained through the wiretap.⁹

More Than Probable Cause. Probable cause alone is not enough, however, to obtain a wiretap warrant. A proper wiretap request also requires the government to demonstrate the "necessity" of the interception. Under 18 U.S.C. § 2518(1)(c), the government may establish necessity for a wiretap by showing that traditional investigative procedures either (1) have been tried and have failed; (2) reasonably appear unlikely to succeed if tried; or (3) are too dangerous to try. Each order approving an interception must set forth specifics of the location and nature of the wiretap, as well as the nature of the anticipated communications and the identities of those involved, if known.¹⁰

Federal authorities' obligations under Title III do not end once a wiretap application is approved. If prosecutors seek to extend the wiretap beyond the original authorization period—which is limited to 30 days—then a court-ordered extension is required.¹¹ Many court orders also require regular reports to the issuing judge showing what progress has been made and the need for continued interception.¹² Perhaps more important, authorities are required to conduct a wiretap "in such a

⁵ *Gelbard v. United States*, 408 U.S. 41, 48 (1972) (quoting S. Rep. No. 90-1097, at 66 (1968), reprinted in 1968 U.S.C.A.N. 2112, 2153).

⁶ 18 U.S.C. § 2516.

⁷ 18 U.S.C. § 2518.

⁸ *Id.*

⁹ 18 U.S.C. § 2518(3)(a).

¹⁰ 18 U.S.C. § 2518(4).

¹¹ 18 U.S.C. § 2518(5).

¹² See 18 U.S.C. § 2518(5).

way as to minimize the interception of communications not otherwise subject to interception.”¹³ The Supreme Court has held that the minimization requirement “does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such manner as to ‘minimize’ the interception of such conversations.”¹⁴ The tests courts use to evaluate the minimization requirement vary slightly by circuit, but most courts consider various factors, such as whether a large number of the calls are very short, one-time only, or in guarded or coded language; the breadth of the investigation underlying the need for the wiretap; whether the phone is public or private; and whether challenged recordings occurred early in the surveillance.

Applications Routinely Approved. Historically, the judiciary routinely grants wiretap applications, and defense challenges to the admissibility of wiretaps almost always fail. According to data reported by the Administrative Office of the U.S. Courts, only one application has been denied in the last three reporting years (2005-2007).¹⁵ The administrative office data is collected from the Department of Justice and requested from state authorities.¹⁶ The statistics on motions to suppress intercepts also demonstrate the uphill battle that potential targets of investigations face. For example, in 2006 the Administrative Office of the U.S. Courts reported that 64 federal and state motions to suppress intercepts were denied and only one was granted.¹⁷ Proponents of wiretaps would credit the solid track record of wiretap applications to a stringent internal application review process in most prosecutors’ offices. Critics, on the other hand, might argue that the review of wiretap applications has become too deferential.

Relatedly, federal law expressly allows federal prosecutors to obtain recorded conversations without a court order when one party to the communication has given prior consent.¹⁸ Of course, consensual recordings are also a standard investigative tool, including in white collar investigations. Consensual recordings are used frequently in investigations because they can take place without independent judicial review. In cases involving institutional or high-level corruption or fraud, a cooperating (or “flipped”) witness who consents to recordings may be critical to gaining an understanding of the true scope and nature of the suspected criminal activity. Consensual recordings, in turn, can sometimes form the foundation of wiretap applications made under Title III. A minority of state laws forbid recordings based on one-party consent, but in those states federal authorities are nevertheless authorized to use the investigative procedures available under federal law.

¹³ *Id.*

¹⁴ *Scott v. United States*, 436 U.S. 128, 140 (1978).

¹⁵ Administrative Office of U.S. Courts, Report of Director on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications (2008) (2007 Wiretap Report); see also 2006 Wiretap Report and 2005 Wiretap Report. The report reflecting 2008 data has not yet been released. The Administrative Office of U.S. Courts makes the Wiretap Reports for the years 1997 forward available at <http://www.uscourts.gov/library/wiretap.html>.

¹⁶ See 2007 Wiretap Report, at p. 5.

¹⁷ See 2007 Wiretap Report, at Table 8, p. 37.

¹⁸ 18 U.S.C. § 2511(2)(c).

Expanding the Use of Wiretaps

In 2007 there were 2,208 authorized intercepts completed, which reflected a 20 percent increase over the number of authorized wiretaps completed in 2006.¹⁹ The number of authorized wiretaps has grown each year since 2002, and from 1997 to 2007 the number of intercept applications authorized increased by 86 percent.²⁰ Telephone wiretaps accounted for 94 percent of all Title III intercepts installed in 2007, with the vast majority involving wiretaps of portable devices such as a cellular phone.²¹

Historically, wiretaps were used as an investigative tool against gangs and mobsters. The legislative history of the Federal Wiretap Act shows that its “major purpose” was “to combat organized crime.”²² Even now, the vast majority of wiretap applications are made in connection with drug-related offenses.²³ There are numerous indications, however, that electronic surveillance has played and will continue to play an increasingly broad role in white collar investigations involving corruption and corporate fraud.

The number of wiretap applications reportedly involving corruption offenses has seen a steady increase in recent years.²⁴ In the Northern District of Illinois, for example, wiretaps and/or consensual recordings have provided the foundation for dozens of successful corruption prosecutions by the U.S. Attorney’s Office. Recent published decisions and media reports provide further evidence of federal authorities’ use of Title III wiretaps in fraud and corruption cases across the country.²⁵

There is reason to believe that the use of wiretaps will increasingly spread to other types of white collar investigations as well, and that such use is unlikely to subside soon. The economic crisis and recent disclosure of financial improprieties has left the public, politicians, and the media hungry for targets to blame. Significant budget deficits at federal, state, and local levels have also increased the political appetite for investigations into waste and fraud in public contracts. The FBI and other investigative agencies are therefore likely to continue to pursue both new and ongoing white collar investigations.

Moreover, the publicly available data may actually underreport white collar wiretaps. The Department of Justice, for example, omits wiretap data involving certain sensitive and/or sealed matters (presumably includ-

¹⁹ 2007 Wiretap Report, at p. 5.

²⁰ *Cf.* 1997 Wiretap Report (reporting 1,186 intercepts), with 2007 Wiretap Report. The data do not include consensual recordings. 2007 Wiretap Report, at p. 6.

²¹ 2007 Wiretap Report, at 8, 11.

²² 1968 U.S.C.C.A.N. 2112, 2157 (1968).

²³ 2007 Wiretap Report, at p. 9.

²⁴ See 2007 Wiretap Report, at p. 9 (32 orders for corruption offenses); 2006 Wiretap Report, at p. 9 (19 orders for corruption offenses); 2005 Wiretap Report, at p. 9 (11 orders for corruption offenses).

²⁵ See, e.g., *United States v. Kincaid-Chauncey*, 556 F.3d 923, 2009 WL 415567, at *1 (9th Cir. Feb. 20, 2009) (reporting use of wiretaps in investigation of former elected officials in Nevada); *United States v. De Castro Font*, 593 F. Supp. 2d 393 (D.P.R. 2009) (denying motion to suppress Title III wire intercepts in public corruption investigation); *United States v. Ketter*, 566 F. Supp. 2d 568 (W.D. Tex. 2008) (discussing wiretaps used in public corruption investigation in Texas).

ing certain white collar investigations) from its reports.²⁶

More Tools, Resources for White Collar Investigations. In addition, at the federal level there may be even more tools and resources directed toward white collar investigations. The FBI is reportedly conducting a review of resources in order to ensure that a sufficient number of agents are assigned to corporate fraud investigations.²⁷ Senate Judiciary Committee Chairman Leahy and Sen. John Cornyn (R-Texas) have introduced legislation designed to provide additional tools to help prosecutors identify, investigate, and prosecute criminal corruption by public officials. Among other things, the bill would authorize funding increases for public corruption investigations and add additional corruption-related crimes to the list of predicates for the federal wiretap statute.²⁸ More recently, Leahy and Sen. Charles Grassley (R-Iowa) introduced legislation—styled the Fraud Enforcement and Recovery Act of 2009—that would provide the federal government more tools and resources to investigate and prosecute financial fraud in particular.²⁹ Among other things, the bill would authorize funding to hire additional fraud prosecutors and investigators to help staff fraud task forces. Both bills have been placed on the Senate’s legislative calendar. Legislation has also been introduced in some states that would expand the authority of investigators to record conversations and pursue white collar crimes.

Practical Considerations

Given U.S. attorneys’ and federal courts’ willingness to support the use of wiretaps and their potential to “accelerate” critical investigations, prosecutors are apt to increasingly look for wiretap opportunities in white collar investigations. From a prosecutor’s perspective, the upsides of recorded conversations are readily apparent. In an ongoing investigation, wiretap evidence can create persuasive opportunities to encourage a subject or minor target to cooperate with prosecutors, which is often critical to developing an understanding of the scope and nature of the suspected criminal activity. The mere fact of a wiretap itself, once disclosed, can add fuel to an investigation by creating anxiety and uncertainty in the minds of individuals who interacted with the known target. At trial, recorded conversations generate powerful evidence for use with a jury and enhance the chance for a conviction.

As explained by DOJ’s Public Integrity Section in a 2007 report to Congress: “Public corruption cases tend to raise unique problems of public perception that are generally absent in more routine criminal cases. . . . A successful public corruption prosecution requires both the appearance and the reality of fairness and impartiality. This means that a successful corruption case includes not just a conviction, but public perception that the conviction was warranted, not the result of im-

proper motivation by the prosecutor, and free of conflicts of interest.”³⁰ Where a defendant’s own incriminating statements can be presented as evidence of criminal conduct, it becomes more difficult for critics to attack the integrity of an investigation.

Price to Pay. The increased use of wiretaps in white collar investigations does come with a price, however. Wiretaps are expensive and time intensive. The resources required to receive authorization for, implement, and monitor a Title III wiretap are substantial, which often leads the government to strategically use wiretaps in only its more significant cases. There is also an out-of-pocket cost associated with such surveillance. The average cost of a wiretap in 2007 was \$65,660, and installed wiretaps were in operation an average of 44 days. Consequently, prosecutors will be forced to carefully choose the targets of wiretap applications and the scenarios under which they will be sought.

Moreover, the necessity requirement of a wiretap application will often limit the ability of prosecutors to obtain wiretap authority early in an investigation.

Prosecutors must also remain wary of potential evidentiary pitfalls with the use of wiretaps, because the statutory remedy for violations of Title III is suppression of the illegally acquired evidence and the fruits derived therefrom.³¹ Under 18 U.S.C. § 2515, when a wire or oral communication is intercepted illegally, “no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing or other proceeding” in or before any court, grand jury, or other agency.

For example, if the affidavit supporting the intercept application is later shown to be deficient, evidence obtained as a result of the wiretaps may be suppressed.³² The concealment or misrepresentation of material facts in a wiretap application may also lead to suppression of evidence, particularly where the errors lead a judge to inappropriately grant a wiretap request.³³ As most practitioners are aware, the Supreme Court has fashioned a good-faith exception to the exclusionary rule that may apply when a warrant is issued in violation of a suspect’s Fourth Amendment rights.³⁴ However, federal circuits are split as to whether the good-faith exception applies to Title III wiretaps, and thus a good-faith claim of mistake or lack of knowledge may not be sufficient to cure a defect.³⁵

³⁰ Report to Congress on the Activities and Operations of the Public Integrity Section for 2007, at 1-2; Submitted Pursuant to Section 603 of the Ethics in Government Act of 1978.

³¹ See, e.g., *United States v. Gonzalez Inc.*, 412 F.3d 1102, 1113 (9th Cir. 2005), *amended on denial of petition for rehearing* at 437 F.3d 854 (2006) (“we are cognizant that the necessity requirement should not be interpreted to require law enforcement to exhaust every possible technique before resorting to wiretapping, but to ensure that in the usual case wiretapping is not used as the first meaningful step in an investigation”).

³² See, e.g., *Gonzalez Inc.*, 412 F.3d at 1113.

³³ See, e.g., *United States v. Rice*, 478 F.3d 704 (6th Cir. 2007).

³⁴ *United States v. Leon*, 468 U.S. 897 (1984).

³⁵ *Cf. Rice*, 478 F.3d at 712-13, with *United States v. Moore*, 41 F.3d 370 (8th Cir. 1994); *United States v. Malekzadeh*, 855 F.2d 1492 (11th Cir. 1988).

²⁶ DOJ reports that in cases where wiretap information is omitted due to investigative concerns, the information should be reported in subsequent years as records or investigations are completed and/or unsealed. See 2007 Wiretap Report, at 8.

²⁷ See n. 3, *supra*.

²⁸ Public Corruption Prosecutions Act, S. 49, 111th Cong. (2009).

²⁹ Fraud Enforcement and Recovery Act, S. 386, 111th Cong. (2009).

Defensive Strategies

For defense counsel, it is imperative that clients be advised early about the potency of wiretap evidence and the potential for the increased use of this powerful investigative technique. Particularly in high-profile white collar investigations, practitioners should help their clients develop a heightened awareness about the risks of electronic surveillance and identify potential pitfalls as early as possible. This is not only true for investigation targets. Even clients who are engaged in completely innocent conduct should be aware that, due to the nature of wiretaps, innocent bystanders conducting legitimate business can be ensnared in recordings, which can lead to federal scrutiny.

As discussed above, legal challenges to wiretap evidence face significant hurdles. The increased use of wiretaps in significant investigations, however, may actually lead to greater opportunities to challenge their validity. As more prosecutors resort to using wiretap evidence as an investigative tool, there is more potential for abuse of the “necessity” requirements of Title III. In white collar investigations, the government may find it harder than in traditional drug or organized crime cases to establish, for example, that other investigative procedures are too dangerous to try.³⁶ Each case is unique, but counsel should carefully evaluate the underlying wiretap application to see whether a credible challenge to the “necessity” of the original wiretap authorization is available.

Viable, Strategic Options. When wiretap evidence leads to an indictment, in many cases a defendant still has viable strategic options when recordings are placed in the proper context. Prosecutors ordinarily will pick and choose the “greatest hits” of recorded conversa-

tions to present to the jury, but in most cases there are significant numbers of recordings that prosecutors will choose not to present. Diligent counsel should scour the wiretap record in search of conversations in which the recorded party overrules, contradicts, or withdraws statements prosecutors wish to highlight. In cases where recordings suggest contradictions, or even ambiguity, in recorded statements, the strongest defense may actually involve embracing the existence of the recordings as a basis for a defense verdict.

In the right case, counsel might also adopt a “talk is cheap” theme in an effort to drive home the point that a government prosecution lacks evidence of subsequent improper conduct (if the facts bear that out). The specific defense opportunities will depend on the unique facts and circumstances of a given case but, at a minimum, counsel should be aware of the totality of recorded conversations that led the government to any “key” wiretap evidence.

Conclusion

Given the compelling nature of wiretap evidence, wiretaps are a device that aggressive prosecutors are likely to use with greater frequency, particularly in high-profile cases. Now, more than ever, investigative targets and unsuspecting individuals alike need to be mindful of the risks associated with wiretaps and other electronic surveillance tools. The risks for investigation targets are obvious. Because wiretaps create a web of recordings that can lead to new and even unplanned investigations, however, even unsuspecting individuals must be wary. Looking ahead on the white collar horizon, wiretaps likely will be used with increased frequency, expanding their role as an effective investigative tool for prosecutors and creating a potential nightmare for prosecutors’ targets and even innocent bystanders.

³⁶ 18 U.S.C. § 2518(1)(c).