Wiretapping For Beginners

Law360, New York (February 10, 2011, 6:04 PM ET) -- Much attention has been focused of late on the government’s recent use of wiretaps in high-profile insider-trading and Foreign Corrupt Practices Act cases. Some observers might be forgiven for wondering what is the big deal.

Wiretaps have been employed so often by prosecutors that they have become a frequent subject of pop culture.[1] The government used the same law and the same procedures in these while collar cases that it has used for years to build cases against terrorists, mobsters and drug dealers.

But if nothing else, the expanded use of wiretaps means that white-collar criminal practitioners, as well as those who may be drawn into civil enforcement cases, need to be familiar with the law underlying wiretaps.

Wiretaps can produce powerful evidence, but to get it the government is required to jump through a number of procedural hoops, any one of which can create an opening for a defendant later seeking to suppress that evidence. This article will briefly examine some of those hoops.

Scope

Communications Covered

First and foremost, the Federal Wiretap Act, 18 U.S.C. §§ 2510-2522, better known as “Title III,”[2] prohibits the interception and disclosure of wire, oral and electronic communications, as well as the manufacture, distribution and possession of such interception devices, 18 U.S.C. §§ 2511-15.[3] However, it expressly authorizes federal and state government authorities in certain criminal investigations to intercept, disclose and use such communications, which include e-mails, faxes and pager numbers, as well as telephone calls.[4]
It is also worth noting what Title III does not cover. The statute expressly does not apply to consensual recordings, including instances where a cooperating witness voluntarily records her own telephone calls. 18 U.S.C. § 2511(2)(c).[5] Nor does Title III apply to wire and electronic communications that are “stored.” That evidence is covered by a separate statute, 18 U.S.C. §§ 2701-2712.

Conduct Covered

The reach of Title III is also circumscribed by the conduct under investigation. State officials may apply under Title III to investigate a broad range of generic crimes, including murder, kidnapping, drug dealing and any other crime “dangerous to life, limb, or property” punishable by more than one year’s imprisonment. 18 U.S.C. § 2516(2).

Federal authorities may intercept electronic communications for investigations of any felony. 18 U.S.C. § 2516(3). For wire or oral intercepts, however, they are limited to investigations of a long and wide-ranging list of specific crimes. See 18 U.S.C. § 2516(1)(a)-(s).

Significantly, that list includes neither securities fraud nor the FCPA. This omission does not restrict the government’s ability to use intercepted evidence in such prosecutions, however. The government may use intercepted evidence in investigations of nonlisted offenses, even at trial if a judge first determines that the intercept otherwise accorded with Title III. 18 U.S.C. § 2517(5).

This provision was recently tested in United States v. Rajaratnam, where, after the government obtained extensive wiretap evidence, the defendants were charged with 17 counts, all securities fraud or conspiracy to commit securities fraud. The court rejected the defendants’ argument that the statute did not authorize wiretaps for securities fraud investigations, holding that as long as the government had obtained the wiretaps in good faith — i.e., had a bona fide investigation of a listed offense — the evidence was admissible.[6]

Given the broad reach of wire and mail fraud (both Title III listed offenses), defendants in most cases likely will have an uphill battle to show that the initial application was not made in good faith. However, as the government uses Title III evidence to prosecute more securities fraud and other nonspecified crimes, historical data may help.

The U.S. Department of Justice and the Administrative Office of the United States Courts are required annually to report various statistics concerning intercepted communications and the resulting prosecutions. See 18 U.S.C. § 2519. Evidence of a larger pattern in which the government charges only securities fraud after obtaining evidence in “other” investigations could buttress a defendant’s argument that an application in a particular case was a pretext to prosecute conduct not covered by Title III.

Cases Covered

While wiretaps can be obtained only in criminal investigations, there is a question whether Title III permits such evidence to be used in noncriminal cases.

Title III authorizes the content of intercepted communications to be shared with “another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.” 18 U.S.C. § 2517. Whether that definition includes the SEC or other civil agencies is an open question. In Rajaratnam, the government declined to share wiretap evidence with the SEC. In other jurisdictions, prosecutors have provided that information to civil agencies.[7]

In SEC v. Galleon Management LP, a parallel civil enforcement proceeding, the SEC used civil discovery
to seek wiretap evidence directly from the defendants, who had obtained the material in the criminal case. The Second Circuit determined that the SEC had a clear interest in discovering the tapes and directed the district court to balance that interest against the defendants’ privacy interest.[8]

What about a situation where civil enforcement authorities use intercepted evidence (obtained directly from criminal prosecutors) where criminal charges were not also brought? Title III expressly permits the suppression of that evidence in “any trial, hearing, or proceeding.” 18 U.S.C. § 2518(10)(a).

The more interesting situation would arise where a civil enforcement defendant seeks to gain access to wiretap evidence for his own defense where there is no criminal prosecution and the enforcement agency does not have the evidence. Third parties, even those who could potentially benefit in their own litigation, have no right to access the wiretap application and order let alone the recorded communications.[9]

Nevertheless, the target of a wiretap is required at some point to be informed of the wiretap, and in its discretion the court may also order notice to other parties to the intercepted communications. 18 U.S.C. § 2518(8)(d). They may petition the court to inspect the tapes and their contents and to obtain a copy, which the court may allow in the interests of justice.[10]

But be careful what you ask for. Once a defendant obtains a copy of the intercepted communications, the civil agency may then have the right to obtain a copy through civil discovery.

Process

Pre-Intercept

State authorities applying in state court under Title III must be authorized by state statute. 18 U.S.C. § 2516(2). Any federal Title III application seeking a wire or oral communication must first be authorized by the attorney general or another specified high-level DOJ official. 18 U.S.C. § 2516(1). The federal interception of electronic communications, however, requires no such approval. 18 U.S.C. § 2516(3). Failure to obtain the required approvals can result in suppression.[11]

As a search and seizure, Title III interceptions are subject to the Fourth Amendment just as more traditional searches. For starters, this means that the government must secure a court order permitting the interception after a probable cause showing that a listed crime has occurred or will occur and that particular communications concerning that crime will be obtained through the intercept. 18 U.S.C. § 2518(3).

This requires a “full and complete statement of the facts and circumstances,” including “details” underlying the alleged offense and a “particular description” of the nature and location of the facilities or place to be wiretapped, the type of communication to be intercepted, and the persons committing the offense and whose communications are to be intercepted. 18 U.S.C. § 2518(1)(b). A wiretap application can be attacked for lack of probable cause just as any search warrant.[12]

Title III applications uniquely require an additional showing of necessity. The government’s application must provide a “full and complete statement” describing all other investigative techniques that have been tried and failed or explaining why such techniques are likely to be unsuccessful or too dangerous. 18 U.S.C. § 2518(1)(c). The court must determine that “normal investigative procedures” have been or would be unsuccessful or excessively dangerous. Id. § 2518(3)(c). A faulty necessity showing can result in suppression.[13]

In Rajaratnam, the government stumbled on the necessity prong by failing to disclose in its application that it was working closely with the SEC, which had at its disposal document subpoenas, witness
interviews and depositions, and the defendants sought to suppress the intercepted statements. The
court permitted a Franks[14] hearing to determine whether the government’s application included a
false statement or omission and if so whether it had been material to the court’s prior finding of
probable cause or necessity.

The court found that the government was reckless in failing to disclose the U.S. Securities and Exchange
Commission investigation but that the omission had not affected the necessity finding. The defendant
had been careful to conduct most of his business over the phone, so any information available through
the SEC’s procedures would still have been insufficient. In addition, the SEC’s investigation had produced
only circumstantial evidence and had “hit a wall.” Finally, the court found that conventional techniques
such as introducing an undercover agent or a wired informant were likely to be unsuccessful.[15]

The application also must set forth the period of time, not more than 30 days, that the government
seeks to maintain the interception. 18 U.S.C. § 2518(1)(d), (5). Interceptions should terminate as soon as
the government first obtains the type of communication described in the application, but if the
government establishes probable cause to believe that additional communications will occur thereafter
the interceptions can continue for the full 30 days. Id. § 2518(1)(d), (5).

Regardless of the 30-day time frame, Title III requires every order to provide that the authorization to
intercept “must terminate upon attainment of the authorized objective.” Id. § 2518(5). In those
instances where the government has taken the position that the conduct under investigation requires
continuing interceptions, no court has yet ruled that interception should have terminated at a point
sooner than the full time period permitted by the order.[16]

The government may apply for an unlimited number of 30-day extensions. 18 U.S.C. § 2518(5). Each
application is subject to the same requirements and standards as the original with the added
requirement that the government report its results so far obtained from the interception or explain why
it has failed to obtain any. Id. § 2518(1)(f). The court must again find probable cause, necessity and a
nexus between the crime and the place or device to be wiretapped to extend the authorization.

Post-Intercept

The government’s obligations continue even after it obtains an order authorizing an intercept. That
order is required to direct the government to take steps to minimize the interception of irrelevant

The government typically minimizes by turning off monitoring equipment once it determines a
conversation is irrelevant.[17] The government’s failure to minimize is another basis for suppression. For
example, in United States v. Renzi, the district court suppressed all of the wiretap evidence because the
government failed to minimize attorney-client conversations.[18]

Finally, Title III requires the contents of the intercepts to be recorded on tape or wire or other
comparable device. 18 U.S.C. § 2518(8)(a). Once the wiretap order has expired the recordings must be
turned over to the court and then sealed. Id. A delay or failure in sealing requires a “satisfactory
explanation” in order for the evidence to be used or disclosed. Id. These requirements provide
defendants with a further avenue for suppressing wiretap evidence.[19]

Conclusion

Despite recent notoriety, it remains to be seen how frequently wiretaps will be used in white collar
investigations, which tend to be reactive in nature. Of the 663 intercepts authorized by federal courts in
2009 (the most recent year for which data is available), for example, only 22 were reported to be related
to anything other than corruption, gambling, homicide and assault, kidnapping, narcotics, or
That said, like with any new toy, white collar prosecutors and their civil counterparts may well be looking for opportunities to try out their newly discovered enforcement tools. Whether a wiretap was properly authorized and whether the government conducted an interception by the book could be issues to address in criminal and civil enforcement proceedings coming soon to a jurisdiction near you.

--By Timothy P. Crudo and Nicholas Y. Lin, Latham & Watkins LLP

Timothy Crudo (timothy.crudo@lw.com) is a litigation partner in the San Francisco office of Latham & Watkins and a former Assistant U.S. Attorney with the U.S. Department of Justice in the Northern District of California. Nicholas Lin (nicholas.lin@lw.com) is an associate in the firm’s San Francisco office.

Latham & Watkins represents an individual in a matter related to the Rajaratnam and Galleon Management matters discussed in the article.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360.

[1] See, e.g., HBO’s The Wire (2002-08); D. Byrne, Life During Wartime (“We got computers, we’re tapping phone lines/I know that that ain’t allowed.”) (1979). From 2000-2009, state and federal courts have authorized over 17,000 wiretaps. See 2000-2009 Reports 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 (“Reports”) Table 3.


[7] See, e.g., In re Motion to Unseal Elec. Surveillance Evidence, 990 F.2d 1015, 1018 (8th Cir. 1993) (en banc) (IRS); Fleming v. United States, 547 F.2d 872, 875 (5th Cir. 1977) (same).


[9] See, e.g., In re N.Y. Times Co., 577 F.3d 401 (2d Cir. 2009); United States v. Dorfman, 690 F.2d 1230, 1233-35 (7th Cir. 1982); In re Motion to Unseal Elec. Surveillance Evidence, 990 F.2d 1015, 1018-20 (8th Cir. 1993) (en banc) (denying the disclosure of evidence to civil litigant); National Broadcasting Co. v. United States Dep’t. of Justice, 735 F.2d 51, 53-55 (2d Cir. 1984) (“Congress [] did not intend this section to be used as an avenue for discovery by all private litigants in civil cases, unless they are directly aggrieved by a wiretap.”); United States v. Dorfman, 690 F.2d 1230, 1233-35 (7th Cir. 1982).

[10] See United States v. Wold., 466 F.2d 1143, 1145 (8th Cir. 1972) (noting defendants were allowed to inspect and copy tapes).


[13] United States v. Gonzales, Inc., 412 F.3d 1102 (9th Cir. 2005) (affidavits revealed that other investigative procedures were likely to be successful and were not dangerous); United States v. Ippolito, 774 F.2d 1482 (9th Cir. 1985) (where the government encouraged confidential informant to lie about his willingness to testify and unearth evidence in a conventional matter, wiretap was unnecessary); United States v. Lilla, 699 F.2d 99 (2d Cir. 1983) (undercover work had been successful and the affidavit did not contain facts to support assertion that traditional investigative techniques would fail); United States v. Fletcher, 635 F. Supp. 2d 1253, 1259 (W.D. Okla. 2009) (general and conclusory statements regarding the necessity of wiretapping 10 additional individuals was insufficient).


[17] See, e.g., United States v. Rivera, 527 F.3d 891, 904-05 (9th Cir. 2008) (describing government’s minimization efforts); United States v. Mansoori, 304 F.3d 635, 643-44 (7th Cir. 2002) (describing minimization order); United States v. Hurley, 63 F.3d 1, 17-18 (1st Cir. 1995); see also United States v. McGuire, 307 F.3d 1192, 1200 (9th Cir. 2002) (describing minimization instruction for faxes).


[19] See, e.g., United States v. Amanuel, 615 F.3d 117, 128-29 (2d Cir. 2010) (handwritten log and attempt to seal were improper and evidence not permitted at trial); United States v. Jackson, 207 F.3d 910 (7th Cir. 2000) (government’s explanation that it wanted to compare new recordings with a different microphone to old recordings was insufficient to explain a 32-day delay), overruled in part on other grounds by United States v. Nance, 236 F.3d 820, 822 (7th Cir. 2000); United States v. McWilliams, 530 F. Supp. 2d 813 (S.D. W.Va. 2008) (excluding wiretap evidence where there was an almost four-week delay in getting the evidence sealed and the government’s unsatisfactory explanation for delay was that it wanted to keep the disc in case there were problems with copies).
