# Aggressive Wiretap Affirmed with Little Fanfare

*This article appeared in Law360 on February 20, 2013.*

On Jan. 8, 2013, in a surprisingly quiet summary order, the Second Circuit upheld the judgment of conviction of James Fleishman, who was convicted for conspiracy to commit securities fraud and wire fraud based in part on a "trunk line" wiretap. *United States v. Fleishman*, Summary Order, No. 12-94-cr (2d Cir. Jan. 8, 2013).

The wiretap order was aggressive and unique. It captured 104 different PIN numbers of a third-party conference call line housed in Las Vegas. Wiretapping such a large number of users was not necessarily remarkable, but what was really surprising was that the government did not allege, and no court ever found, that there was probable cause that each separate PIN number was being used to facilitate criminal activity—only that evidence of criminality could be found on the conference call line as a whole.

The *Fleishman* case presented unique hurdles to law enforcement's investigation, although the hurdles were more logistical than apparently legal. By statute, wiretaps cannot be used to purely investigate insider trading. See 18 U.S.C. § 2516. This is by no means a new issue. Law enforcement typically solves this problem by adding wire fraud as the crime being investigated (which is authorized by statute), and courts have held that when a law enforcement officer is lawfully searching for evidence for a crime such as wire fraud and "may happen upon evidence of another crime," such as insider trading, he is not obligated to "ignore what is in plain view." See Memorandum Opinion & Order, *United States v. Rajaratnam*, 09 Cr. 1184 (RJH) (Nov. 24, 2012); *United States v. Masciarelli*, 558 F.2d 1064, 1067 (2d Cir. 1977); 18 U.S.C. § 2517(5).

Law enforcement is required to have a good faith investigation into the enumerated crime, and should not use it as a "subterfuge" to gather evidence for a non-enumerated crime, *United States v. Marion*, 535 F.2d 697, 700 (2d Cir. 1976), but in current-day insider trading cases where inevitably there were communications by phone or by email, this is largely a distinction without a difference.

Thus the hurdle in the *Fleishman* case was not legal, but logistical, and was principally a result of trying to adapt the use of wiretaps—an investigative tool that has predominantly been used in drug trafficking cases—to securities cases. Drug dealers typically use unsubscribed and/or month-to-month cellphones where the difficulty is in identifying the phone being used, but once that phone is identified every conversation relates directly to the individual being investigated. Wall street traders and executives, however, use a variety of ever-changing methods to communicate—one of which being third-party conference call lines.

In the *Fleishman* case, law enforcement agents were able to identify the conference call company that Fleishman and his firm used, and obtain the specific PIN numbers that were assigned to the targets of their investigation. Each of their targets would call the same 1-800 number and then input their unique PIN number to start the conference. However, law enforcement took the wiretap one step further. Rather than just limit their request to the four PIN numbers of their target subjects, law enforcement agents sought and received authorization to intercept 104 individual PINs on the conference calling line that included 97 clients of Fleishman's firm. See Memorandum and Order, *United States v. Fleishman*, 11 Cr. 32 (JSR) (S.D.N.Y. Aug. 30, 2011); Affidavit in Support of Application for Authorization to Intercept Wire Communications, Document 81-2, *United States v. Fleishman*, 11 Cr. 32 (JSR) (S.D.N.Y. July 30, 2011).

To be clear, there is no allegation in the wiretap application that the investigators had reason to believe each of these 97 clients were involved in criminal activity. Rather, the theory was that there was probable cause to believe that the four target individuals were using the conference call number in furtherance of their crimes and the 97 clients were included because they had a business relationship to the targets. If indeed each of the 104 PIN numbers were seen as separate telephone lines, it would be akin to asking for authorization to intercept the phone lines of every person the targets did business with, regardless of whether there was any cause to believe those individuals were involved in the criminality. And that's exactly as defense counsel saw it.

However, both the district court and the Second Circuit agreed with the government and saw it as a straightforward matter. With little fanfare, each court semantically found that: Title III authorizes wiretaps on a "communication facility"; the conference call line was a such a facility; and there was probable cause to believe that evidence of wire fraud would be found on the "communication facility."

Rather than looking at the third-party conference call line as a conglomeration of hundreds of different users with unique PINs each placing their own calls, the entire conference line was the "communication facility" and could be intercepted en masse because there was one 1-800 number all the customers dialed before putting in the PIN number (or, in the *Fleishman* case, actually two main numbers that they called before putting in their PIN number).

The reach of this holding is unprecedented. Both courts cited the government's self-imposed limits on the number of PINs it was seeking to intercept—a mere 104 different accounts of clients and employees of one firm as opposed to all PIN numbers. However, the logic of the district court and Second Circuit's orders certainly does not require such a limitation. If the "communications facility" is indeed the 1-800 number used to place a conference call, then as long as one person is using that conference line to commit a criminal act, every single call on that same conference line can be intercepted. It doesn't matter what company you are with or whether you are a private individual and it doesn't matter how many people use the conference line—if you are using a third-party conference line that someone else you don't even know is using to commit a crime, then your calls, too, can be intercepted. In upholding the wiretap, Judge Jed Rakoff cited the "well-established principle that Title III focuses on facilities independently of the people who use them." Memorandum and Order, *United States v. Fleishman*, 11 Cr. 32 (JSR) (S.D.N.Y. Aug. 30, 2011).

To be fair, both courts did note that the government is required to "minimize" the interceptions—that is, to turn off the monitoring equipment when law enforcement determines that the conversation is unrelated to criminal communications. Typically, the law enforcement official will listen to the first few minutes of a call, and, if the call seems unrelated to criminal activity, turn off the call and then spot check it by turning on the recording equipment every few minutes.

In addition, Judge Rakoff did make reference to a "hypothetical case" where the government doesn't limit itself at all, and seemed to suggest such a case might deserve closer scrutiny. However, the limits the government placed on itself was not based on probable cause (i.e. it did not only intercept PINs for which it had probable cause to believe evidence of criminality could be found). The government limited itself only relationally—to those PINs that had a known business relationship to their targets of interest. Such a limitation has no real legal meaning within Title III.

**Conclusion**

The question of what constitutes a "communications facility" will likely become increasingly more difficult with further technological advances. Most pressingly, courts are going to have to tackle issues related to Voice over IP ("VoIP") and the different ways that those companies send packets of data across the Internet. Some of these VoIP companies route all calls through a central server. The *Fleishman* decision could be seen to support a view that the "communications facility" is the company's server and thus if there is probable cause to believe anyone is using that VoIP company in furtherance of

their criminal activities, law enforcement may be able to intercept the entire "communications facility" — meaning all calls from everyone that use that particular VoIP company's services.

The wiretap statutes originally envisioned calls being placed by a criminal to another criminal by dialing a number on their private phone. It simply doesn't work that way anymore, and if the courts do not put limits on what they deem to be "communications facilities," then law enforcement's ability to intercept calls will be much more expansive than ever originally envisioned.

–By Michael M. Rosensaft, Katten Muchin Rosenman LLP