# FBI taps cell phone microphone as eavesdropping tool

**By Declan McCullagh and Anne Broache**
**Staff Writers, CNET News**

The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations.

The technique is called a "roving bug," and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him.

Nextel cell phones owned by two alleged mobsters, John Ardito and his attorney Peter Peluso, were used by the FBI to listen in on nearby conversations. The FBI views Ardito as one of the most powerful men in the Genovese family, a major part of the national Mafia.

The surveillance technique came to light in an opinion published this week by U.S. District Judge Lewis Kaplan. He ruled that the "roving bug" was legal because federal wiretapping law is broad enough to permit eavesdropping even of conversations that take place near a suspect's cell phone.

**Kaplan's opinion said that the eavesdropping technique "functioned whether the phone was powered on or off." Some handsets can't be fully powered down without removing the battery; for instance, some Nokia models will wake up when turned off if an alarm is set.**

While the Genovese crime family prosecution appears to be the first time a remote-eavesdropping mechanism has been used in a criminal case, the technique has been discussed in security circles for years.

The U.S. Commerce Department's security office warns that "a cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone." An article in the Financial Times last year said mobile providers can "remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call."

Nextel and Samsung handsets and the Motorola Razr are especially vulnerable to software downloads that activate their microphones, said James Atkinson, a counter-surveillance consultant who has worked closely with government agencies. "**They can be remotely accessed and made to transmit room audio all the time**," he said. "**You can do that without having physical access to the phone**."

Because modern handsets are miniature computers, downloaded software could modify the usual interface that always displays when a call is in progress. The spyware could then place a call to the FBI and activate the microphone--all without the owner knowing it happened. (The FBI declined to comment on Friday.)

"If a phone has in fact been modified to act as a bug, the only way to counteract that is to either have a bugsweeper follow you around 24-7, which is not practical, or to peel the battery off the phone," Atkinson said. Security-conscious corporate executives routinely remove the batteries from their cell phones, he added.

FBI's physical bugs discovered

The FBI's Joint Organized Crime Task Force, which includes members of the New York police department, had little luck with conventional surveillance of the Genovese family. They did have a confidential source who reported the suspects met at restaurants including Brunello Trattoria in New Rochelle, N.Y., which the FBI then bugged.

But in July 2003, Ardito and his crew discovered bugs in three restaurants, and the FBI quietly removed the rest. Conversations recounted in FBI affidavits show the men were also highly suspicious of being tailed by police and avoided conversations on cell phones whenever possible.

That led the FBI to resort to "roving bugs," first of Ardito's Nextel handset and then of Peluso's. U.S. District Judge Barbara Jones approved them in a series of orders in 2003 and 2004, and said she expected to "be advised of the locations" of the suspects when their conversations were recorded.

Details of how the Nextel bugs worked are sketchy. Court documents, including an affidavit (p1) and (p2) prepared by Assistant U.S. Attorney Jonathan Kolodner in September 2003, refer to them as a "listening device placed in the cellular telephone." That phrase could refer to software or hardware.

One private investigator interviewed by CNET News.com, Skipp Porteous of Sherlock Investigations in New York, said he believed the FBI planted a physical bug somewhere in the Nextel handset and did not remotely activate the microphone.

"They had to have physical possession of the phone to do it," Porteous said. "There are several ways that they could have gotten physical possession. Then they monitored the bug from fairly near by."

But other experts thought microphone activation is the more likely scenario, mostly because the battery in a tiny bug would not have lasted a year and because court documents say the bug works anywhere "within the United States"--in other words, outside the range of a nearby FBI agent armed with a radio receiver.

In addition, a paranoid Mafioso likely would be suspicious of any ploy to get him to hand over a cell phone so a bug could be planted. And Kolodner's affidavit seeking a court order lists Ardito's phone number, his 15-digit International Mobile Subscriber Identifier, and lists Nextel Communications as the service provider, all of which would be unnecessary if a physical bug were being planted.

A BBC article from 2004 reported that intelligence agencies routinely employ the remote-activiation method. "A mobile sitting on the desk of a politician or businessman can act as a powerful, undetectable bug," the article said, "enabling them to be activated at a later date to pick up sounds even when the receiver is down."

For its part, Nextel said through spokesman Travis Sowders: "We're not aware of this investigation, and we weren't asked to participate."

Other mobile providers were reluctant to talk about this kind of surveillance. Verizon Wireless said only that it "works closely with law enforcement and public safety officials. When presented with legally authorized orders, we assist law enforcement in every way possible."

A Motorola representative said that "your best source in this case would be the FBI itself." Cingular, T-Mobile, and the CTIA trade association did not immediately respond to requests for comment.

Mobsters: The surveillance vanguard

This isn't the first time the federal government has pushed at the limits of electronic surveillance when investigating reputed mobsters.

In one case involving Nicodemo S. Scarfo, the alleged mastermind of a loan shark operation in New Jersey, the FBI found itself thwarted when Scarfo used Pretty Good Privacy software (PGP) to encode confidential business data.

So with a judge's approval, FBI agents repeatedly snuck into Scarfo's business to plant a keystroke logger and monitor its output.

Like Ardito's lawyers, Scarfo's defense attorneys argued that the then-novel technique was not legal and that the information gleaned through it could not be used. Also like Ardito, Scarfo's lawyers lost when a judge ruled in January 2002 that the evidence was admissible.

This week, Judge Kaplan in the southern district of New York concluded that the "roving bugs" were legally permitted to capture hundreds of hours of conversations because the FBI had obtained a court order and alternatives probably wouldn't work.

The FBI's "applications made a sufficient case for electronic surveillance," Kaplan wrote. "They indicated that alternative methods of investigation either had failed or were unlikely to produce results, in part because the subjects deliberately avoided government surveillance."

Bill Stollhans, president of the Private Investigators Association of Virginia, said such a technique would be legally reserved for police armed with court orders, not private investigators.

There is "no law that would allow me as a private investigator to use that type of technique," he said. "That is exclusively for law enforcement. It is not allowable or not legal in the private sector. No client of mine can ask me to overhear telephone or strictly oral conversations."

Surreptitious activation of built-in microphones by the FBI has been done before. A 2003 lawsuit revealed that the FBI was able to surreptitiously turn on the built-in microphones in automotive systems like General Motors' OnStar to snoop on passengers' conversations.

**When FBI agents remotely activated the system and were listening in, passengers in the vehicle could not tell that their conversations were being monitored.**

Malicious hackers have followed suit. A report last year said Spanish authorities had detained a man who write a Trojan horse that secretly activated a computer's video camera and forwarded him the recordings.