

# High-Tech FBI Tactics Raise Privacy Questions

By Jonathan Krim

Washington Post Staff Writer

Tuesday, August 14, 2001; Page A01

When federal prosecutors set their sights on Nicodemo Scarfo, son of reputed Philadelphia mob boss Nicodemo "Little Nicky" Scarfo, for alleged illegal gambling and loan-sharking, they had to employ some sophisticated high-tech techniques.

The younger Scarfo, it seemed, was savvy enough about computers to use an encryption program to protect his electronic files.

So investigators secretly installed a way to capture every keystroke so they could learn his password. In the process, they made Scarfo an unlikely symbol for privacy advocates, who are worried about the government's ability to conduct surveillance of personal computers.

It is a case at the heart of how technology increasingly strains notions of privacy and whether established law works in a digital age. Scarfo's defense team, with assistance from privacy organizations, is trying to force the government to reveal how the "key-logging" technology works as a possible prelude to asking that the evidence it yielded be thrown out.

Privacy advocates are especially concerned that the key logger was planted on the basis of a simple search warrant and not a court-approved wiretap order, which is more difficult to obtain and carries far greater restrictions.

Federal law requires that any device that listens in on communication, whether it be a bug in a room or a phone tap, requires a wiretap order. In the case of electronic communication via computers, the law specifically requires a wiretap order only if the communication is intercepted in transmission via computer modems and phone lines. That preserves the government's ability to seize a computer, with a simple search warrant, and examine copies of e-mail already sent or received, or anything else that might be stored on the computer's hard drive.

Prosecutors insist that the key logger planted by the FBI did not intercept communication, but they have refused to divulge how the technology works to back up that claim.

And privacy groups note the new issue posed by key-logging technology, which is commercially available and used by some companies: Even if the key logger didn't intercept communication after it was sent by the computer's modem, it effectively does the same thing by capturing what is typed on an e-mail or instant message form just before the user hits the send button.

"The logical consequence of the government's argument is that the government will never need to get a

wiretap order for a computer," said Mark Rasch, a former federal prosecutor who is now vice president of cyberlaw at Predictive Systems Inc., a Reston-based computer-security consulting firm. "With the technology that's available today, the government can remotely install software on a computer to capture all keystrokes and transmit that report to its agents in real time."

Attorneys on both sides are under a court order not to speak about the case, but prosecutors argue in court filings that disclosing the key-logging technology would enable criminals to find ways to defeat it in the future. As a result, it's unclear whether the key logger used by the FBI is purely software or whether it involved some sort of device attached to the keyboard. It's also unknown how the data from the key logger was collected.

The key logger is "a highly sensitive law enforcement search and seizure technique, the disclosure of which would compromise use of this technology . . . and jeopardize the safety of law enforcement personnel," according to an affidavit by Donald Kerr, assistant director of the FBI's laboratory division.

In an initial ruling last week, U.S. District Judge Nicholas Politan in Newark rejected that argument.

"The government has not satisfactorily confirmed for the court that the key-logger device did not operate in conjunction with the computer's modems, or otherwise, to cause the interception of a communication," Politan wrote.

He added that pages of captured keystrokes that the government placed in evidence "are in the truest sense 'gobbledygook,' " and that he cannot determine whether the search was legal if he doesn't know how this key-logging technology works.

But the judge gave prosecutors one last chance to convince him otherwise, saying he would review the technology in secret before making his final decision. Prosecutors have until tomorrow to respond.

According to court records, confidential informants told FBI agents in January 1999 that Scarfo and an associate, Andrew Knapik, had been running a sports-betting and loan-sharking operation linked to the Gambino crime family out of a one-room office of a company known as Merchant Services Inc. in Belleville, N.J.

It appeared to agents that Scarfo, 35, who had several arrests and convictions on assault, conspiracy and weapons charges, was being groomed to take over the operation from Knapik, who was heading to prison. The two would drive around collecting on bets and loan payments, and when Scarfo was arrested he had more than \$6,000 in cash on him, according to court records. Scarfo also would use the Merchant Services office for loan collection, the records said.

As part of the investigation, FBI agents went into Scarfo's office with a search warrant and copied his computer files. One of them, labeled "Factors," was encrypted, or scrambled, with a program called PGP -- Pretty Good Privacy -- which can be bought on the Internet for as little as \$50.

Unable to crack the encryption code without a password, agents went back again with a search warrant and placed the key-logging device on his computer, and monitored it for about two months. The surveillance ultimately produced the password -- nds09813-050 -- which a source close to the case confirmed is the prison identification number of Scarfo's father.

Former law enforcement officials said that criminals are increasingly using sophisticated high technology and that the government must have, within reason, the ability to keep one step ahead of them.

"Encryption is virtually unbreakable by police today, with programs that can be bought for \$15," said Stewart Baker, former general counsel of the National Security Agency and now partner at the Washington law firm Steptoe & Johnson.

Although agreeing that surveillance should be done under strict guidelines, Baker said that "to a degree, the privacy groups got us into this by arguing that there should be no limits on encryption, and the police have to deal with it."

David Sobel, general counsel of the Electronic Privacy Information Center in Washington, which has been advising the defense team, disagreed.

"Because of this technology there are a lot of gray areas," Sobel said, "but law enforcement is always attempting to resolve them in favor of more aggressive techniques."

As an example he wondered whether, if the key-logging system used in the Scarfo case was able to turn itself off when the modem was activated to ensure that a wiretap order was not required, why it couldn't instead have been configured to activate only when an encryption program was run.

© 2001 The Washington Post Company