

FBI Develops Eavesdropping Tools

By *Ted*
Associated Press

Bridis
Writer

Thursday, November 22, 2001; 2:34 AM

WASHINGTON — The FBI is going to new lengths to be sure it can eavesdrop on high-tech communications, secretly building "Magic Lantern" software to monitor computer use.

Separately, the agency is urging phone companies to change their networks for more reliable wiretaps in the digital age.

At a conference Nov. 6 in Tucson, Ariz. — and in a 32-page follow-up letter sent about two weeks ago — the FBI told leading telecommunications officials that increasing use of Internet-style data technology to transmit voice calls is frustrating FBI wiretap efforts.

The FBI told companies that it will need access to voice calls sent over data networks within a few hours in some emergency situations, and that any interference caused by a wiretap should be imperceptible to avoid tipping off a person that his calls might be monitored.

The Magic Lantern technology, part of a broad FBI project called "Cyber Knight," would allow investigators to secretly install over the Internet powerful eavesdropping software that records every keystroke on a person's computer, according to people familiar with the effort.

The software is somewhat similar to so-called trojan software already used illegally by some hackers and corporate spies. The FBI envisions one day using Magic Lantern to record the secret unlocking key a person might use to scramble messages or computer files with encryption software.

The bureau has been largely frustrated in efforts to break open such messages by trying different unlocking combinations randomly, and officials are increasingly concerned about their ability to read encrypted messages in criminal or terrorist investigations.

The FBI said in a statement Wednesday that it can not discuss details of its technical surveillance efforts, though it noted that "encryption can pose potentially insurmountable challenges to law enforcement when used in conjunction with communication or plans for executing serious terrorist and criminal acts."

The FBI added that its research is "always mindful of constitutional, privacy and commercial equities," and that its use of new technology can be challenged in court and in Congress.

Magic Lantern would largely resolve an important problem with the FBI's existing monitoring technology, the "Key Logger System," which in the past has required investigators to sneak into a target's home or business with a so-called sneak-and-peak warrant and secretly attach the device to a computer.

In contrast, Magic Lantern could be installed over the Internet by tricking a person into double-clicking an e-mail attachment or by exploiting some of the same weaknesses in popular commercial software that allow hackers to break into computers. It's unclear whether Magic Lantern would transmit keystrokes it records back to the FBI over the Internet or store the information to be seized later in a raid. The existence of Magic Lantern was first disclosed by MSNBC.

"If they are using this kind of program, it would be a highly effective way to bypass any encryption problems," said James E. Gordon, who heads the information technology practice for Pinkerton Consulting and Investigations Inc. "Once they have the keys to the kingdom, they have complete access to anything that individual is doing."

At least one antivirus software company, McAfee Corp., contacted the FBI on Wednesday to ensure its software wouldn't inadvertently detect the bureau's snooping software and alert a criminal suspect.

Experts said the FBI software could be used with a court order against criminals, terrorists or foreign spies. People familiar with the project, who spoke only on condition of anonymity, said the package is being developed at the FBI's electronic tools laboratory, the same outfit that built the bureau's "Carnivore" Internet surveillance technology.

Some experts said Magic Lantern raises important legal questions, such as whether the FBI would need a wiretap order from a U.S. judge to use the technology. The government has previously argued that the FBI can capture a person's computer keystrokes under the authority of a traditional search warrant, which involves less oversight by the courts.

"It's an open question whether the covert installation of something on a computer without a physical entry requires a search warrant," said David Sobel, a lawyer with the Washington-based Electronic Privacy Information Center, a civil liberties group.

© 2001 The Associated Press



[E-Mail This Article](#)

[Printer-Friendly Version](#)

[Subscribe to The Post](#)