

FBI Has a Magic Lantern

To light the path to suspects' computers

Calling it a just "workbench project," that could not be further commented on, the FBI has confirmed the existence of its latest Internet-eavesdropping, controversy-raising snooping device exotically code-named "Magic Lantern."

Magic Lantern is software that, once installed on the suspect's computer, will record every keystroke typed. The gathered keystrokes will then be analyzed by the FBI to extract passwords. The harvested passwords will be used by the FBI to access the suspect's email messages and other encrypted documents, or to gain access to other computers contacted by the suspect via the Internet.

While the FBI has long acknowledged using its controversial Carnivore system to intercept data transmitted to and from a suspect's computer over the Internet, Magic Lantern differs substantially in design and, as civil liberty advocates will argue, its level of intrusion on personal privacy.

Carnivore is installed between the suspect's PC and the Internet, typically on hardware under the control of the suspect's Internet service provider. Magic Lantern, however, is installed directly on the suspects computer via a Trojan horse virus delivered over the Internet. Identity-stealing hackers have recently been sending similar viruses to computer users around the world via disguised email attachments hoping to gather passwords, user names, bank account and credit card numbers, and similar personal information.

When asked if use of Magic Lantern would require a court order, as does Carnivore, FBI spokesman Paul Bresson told reporters only that, "Like all technology projects or tools deployed by the FBI it would be used pursuant to the appropriate legal process."

Since Magic Lantern is essentially "just another virus," anti-virus software can be written to defeat it. According to a Reuters report of December 12, the FBI has not asked anti-virus software vendors to refrain from creating anti-Magic Lantern software. Most vendors, however, have stated they would not cooperate with the FBI unless ordered to do so by the courts.

Civil liberty groups argue that use of an Internet snooper systems like Carnivore and Magic Lantern represents an unreasonable search and seizure according to the Fourth Amendment to the Constitution.

The FBI claims authority to intercept telephone and Internet communications under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and parts of the Electronic Communications Privacy Act of 1986, or "ECPA".

According to the Department of Justice, interception of Internet data requires a much higher level of judicial approval than traditional searches.

"Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are viewed by federal district court judges. Further, interception of communications is limited to certain specified federal felony offenses." -- Testimony of FBI Assistant Director Donald M. Kerr before the House Judiciary Committee - July 24, 2000.

Congress, however, had concerns about possible misuse or overuse of Internet snooping systems in August, when lawmakers required the FBI to provide them with detailed reports on the Agency's actual use of Carnivore. [[Congress Clamps Down on Carnivore](#)]

Of course, that action came before Sept. 11, 2001. Given the importance of the war on terrorism and the fact that terrorist groups are known to formulate plans, raise funds and spread propaganda over the Internet, do not look for Congress to clip the wick of the Magic Lantern.

Subscribe to the Newsletter

Name Email

From [Robert Longley](#),
Your guide to [U.S. Gov Info / Resources](#).
FREE Newsletter. [Sign Up Now!](#)

Related Articles

- [Stopping Carnivore Doesn't](#)
- [Congress Clamps Down On Carnivore](#)
- [Carnivore No Threat to Privacy FBI Says](#)
- [Carnivore, Sniffers, And You - Computer Networking](#)
- [FBI Battles Computer Crime](#)

Join the Discussion

Anti Carnivore:
"Carnivore is just another invention of 'Big Brother' to control our lives."
[WICCANWOLF](#)
[Click to Read/Reply](#)

Pro Carnivore:
"The conspiracy theorists have yet another morsel to sate their paranoid appetites of future destruction. ... I feel this is yet another attack on a tool that can help stop the misuse of our free communication systems by those who are out to kill our nation's freedoms and our children. Period."
[ELS358](#)
[Click to Read/Reply](#)

Related Resources

- [Congress Clamps Down on Carnivore](#)
- [Carnivore No Threat to Privacy Says FBI](#)
- [House Votes to Slap Special Oversight on FBI](#)
- [From the Files of the FBI](#)

From Other Guides

- [Carnivore, Altivore, Echelon](#)
- [Carnivore Resources](#)
- [Carnivore Keeps Its Secrets](#)
- [Say 'Cheese'](#)

Elsewhere on the Web

- [FBI Defends Carnivore](#)
- [FBI Details on Carnivore](#)
- [Stop Carnivore.org](#)

Are systems like Magic Lantern and Carnivore necessary tools for preventing crime and terrorism or simple invasions of personal privacy?

Necessary Tools

Invasions of Privacy

Not sure

[Current Results](#)