

## **The FBI's Carnivore**

**The FBI says Carnivore is an essential tool, the American Civil Liberties Union is crying foul... • July 24, 2000 •**

The Federal Bureau of Investigations has a new tool to conduct lawful surveillance of criminal activity. It is called "Carnivore" and was created by the FBI in response to the inability of an Internet Service Provider to discriminate communications from criminal suspects to the exclusion of all the other communications that the ISP handles. Carnivore can be installed at your ISP and employed for 30 days to intercept specific suspect communications. Surveillance must cease sooner if the desired evidence is obtained. Proper authorization has to have been obtained first through the appropriate judicial channels and extensions to the surveillance period of 30 days are permitted if required for further investigation. Approval to use Carnivore is granted where probable cause can be demonstrated, where normal investigative methods may not work, or are too dangerous, and when prior electronic surveillance warrants further interest in the criminal subject. Carnivore functions somewhat like typical packet-sniffers and resembles other network diagnostic tools currently in use by ISPs. The difference with Carnivore, says the FBI, is that Carnivore has "a unique ability to distinguish between communications which may be lawfully intercepted and those which may not". Carnivore is designed to limit the material that can be viewed from its surveillance to just the data described and authorized by the electronic surveillance order.

We're hearing a lot about Carnivore now because efforts to integrate Carnivore into ISPs requires that common standards for complying with wiretap requirements be developed. It is at the behest of the FCC that standards for Internet surveillance be set. The recent implementation of Carnivore at a Pasadena, California EarthLink network hub site proved difficult. Carnivore caused unspecified disruptions to EarthLink ISP customers and "actually brought pieces of the EarthLink network down" per Steve Dougherty, EarthLink's Director of Technology Acquisition. EarthLink had previously unsuccessfully gone to court to prevent the implementation of Carnivore onto its system. Older versions of Carnivore had caused remote access servers to crash and adversely affected service to EarthLink customers.

Detractors and critics loudly claim that Carnivore can be used to violate our civil liberties. The American Civil Liberties Union is taking the stand that our Fourth Amendment can be used to defend the American public against Carnivore. The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The FBI points out that Carnivore is not a new angle on surveillance, it's just the FBI's response to keep up with changing technology. It is the potential for abuse that causes concern. Some advocate that if you don't want your secret family recipe for pumpkin pie read by non-family members, you might consider encryption to protect your email's contents. Encryption isn't worth a nickel, though, if another person has the encryption key. I suspect the FBI has a "pretty good" set of encryption keys in their pockets, and those pockets are surely deep.

**Sandra Underhill, Associate Editor, InfiniSource.com**