LOS ANGELES TIMES

THURSDAY, JULY 27, 2000

Who Needs Big Brother When There's 'Carnivore'?

■ Law enforcement: The FBI should not be granted such sweeping powers to search our e-mail and then be trusted to police itself.

By BART KOSKO

Now the FBI wants to recruit Internet service providers, or ISPs, to spy on U.S. citizens. The FBI already works with the credit companies to secretly snoop on large portions of our digital credit reports per the 1996 Intelligence Authorization Act. The FBI has installed digital phone-tapping equipment directly in phone companies under a similar congressional act passed in 1994. And the Treasury Department's Financial Crimes Enforcement Network has "deputized" all banks to monitor our bank accounts and to secretly file "suspicious activity reports" that it shares with the FBI and IRS and even with some foreign governments.

The FBI calls its new ISP surveillance software "Carnivore." An agent connects a laptop to the ISP server and then reads at least the address of every e-mail message that passes through the server. The FBI says it has used its Carnivore software 25 times in the last two years to search for terrorists or drug dealers or child pornographers. The FBI claims that it needs this search-'em-all software to help it find and catch such criminals when they use the Internet.

There are three problems with Carnivore, and each is fatal. The first is that Carnivore undermines the 4th Amendment's ban on unreasonable searches—if it does not violate it outright. The FBI still must get a judge to issue a search warrant based on "probable cause." This in practice can mean no more than that the FBI asks for the warrant. But the 4th Amendment further demands that the warrant be specific—"particularly describing the place to be searched."

Carnivore searches blindly through all private e-mails that flow through the ISP server while it looks for a suspicious few. This is as if the police have a warrant to search someone's bedroom closet and then search all houses in a city until they find it. The search itself invades privacy.

Carnivore switches the order of search and identification. Traditional searches first identify the suspect's property, which is then searched. Carnivore searches through private databases until it identifies a suspect's property—and perhaps learns some new things along the way. This is a big leap down the slippery slope of state invasion of privacy. And the very existence of such a monitoring system produces a chilling effect on e-mail-based free speech, because knowing that a state police agency will read at least part of your e-mail message affects what you say in that message.

The second problem is that the FBI does not need Carnivore to search for alleged criminal e-mails. Rep. John Conyers Jr. (D-Mich.) raised this issue with FBI Assistant Director Donald Kerr when Kerr testified before Congress at a hearing Monday on Carnivore: "Why do we need to put terminals on site at the ISPs rather than let the ISP itself turn over needed information much in the way that telephone companies do?"

Kerr conceded this point but claimed that the FBI still needs Carnivore for those ISPs that lack filtering software. This is plainly specious: The FBI or oversight sources could simply give such ISPs this filtering software. There is simply no need to grant the FBI such sweeping powers of search and then trust the agency to police itself as those powers inevitably grow in time.

The third problem is that Carnivore ultimately will not work despite all its costs. The criminals it tries to watch are the very people who will take the two obvious steps to evade it: They will change their fake digital IDs more often, and they will use ever more powerful digital encryption to scramble their messages.

Carnivore's software blueprints and performance quirks themselves will leak to the digital underground despite or because of the best efforts of those in Congress or the judiciary who oversee it. And hackers will surely study the software system and maybe crack it.

The only people Carnivore can confidently watch are the innocent citizens whom it has no right to watch. This sets a foolish and dangerous precedent for the type of heavy-handed government surveillance one would expect to find in Myanmar or China.

The only thing right about Carnivore is its name: This digital beast devours both personal privacy and constitutional limits on state police power. Congress should kill it.

Bart Kosko is a professor of electrical engineering at USC and the author of "The Fuzzy Future" (Random House, 1999).