December 1, 2000

BY ELECTRONIC MAIL

(Review.Panel@usdoj.gov)

Carnivore Review Panel
U.S. Department of Justice
Room 1744
950 Constitution Ave., NW
Washington, D.C. 20530

Re: Independent Technical Review of the Carnivore System

Pursuant to the Review Panel's request, the Electronic Privacy Information Center ("EPIC") hereby submits comments on "non-technical issues" raised by the Draft Report of the Independent Technical Review of the Carnivore System ("Draft Report") prepared by the IIT Research Institute.

We note that the IIT review team undertook a purely "technical" review and expressly declined to address the significant legal issues surrounding the use of the Carnivore system. The reviewers did, nonetheless, allude to those issues:

> Although IITRI specifically excluded questions of constitutionality and of illegal activity by the FBI from this evaluation, IITRI is concerned that the presence of Carnivore and its successors without safeguards as recommended below: (1) fuels the concerns of responsible privacy advocates and reduces the expectations of privacy by citizens at large and (2) increases public concern about the potential unauthorized activity of law enforcement agents. Draft Report, Sec. 5.

Unfortunately, we believe that the review team's findings do little to alleviate those concerns. While DOJ and FBI spokespersons have attempted to characterize the Draft Report as a vindication of the Carnivore system, a close reading of the reviewers' conclusions in fact validates much of the public and Congressional criticism that has been expressed since the existence of the surveillance system was revealed earlier this year.

1. Over-Collection of Communications

Much of the controversy concerning Carnivore grows out of the fact that the system accesses and processes a great deal of ISP traffic, the vast majority of which contains the communications of Internet users not targeted for surveillance and not named in any court authorization. Unlike traditional electronic surveillance techniques, which are capable of complying with the strict specificity and minimization requirements of federal wiretap law, Carnivore provides law enforcement with access to the private communications of all subscribers of a particular service provider. It is this unique aspect of Carnivore that gives rise to fundamental privacy risks.

The Draft Report states that Carnivore is, indeed, capable of collecting more information than law enforcement is legally authorized to acquire:

> While the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors. Draft Report, Section ES.5.

While the reviewers apparently considered only the potential that the system could be "incorrectly configured," the ease with which Carnivore can mistakenly conduct a "broad sweep" suggests that it is clearly subject to intentional abuse as well. The unauthorized over-collection of private communications, whether accidental or intentional, raises fundamental issues under both federal wiretap law and the Fourth Amendment. We do not believe that this infirmity can be cured through any sort of technical "fix." Rather, it is an inherent flaw in any system that provides law enforcement with direct access to an ISP's data traffic.

This issue was recently addressed by the U.S. Court of Appeals for the D.C. Circuit, which held that when law enforcement seeks access to packet-mode communications (as with Carnivore) there can be no lessening of "the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped." United States Telecom v. Federal Communications Commision, 227 F.3d 450, 465 (D.C. Cir. 2000) (citation omitted). The Court stressed that carriers cannot be required "to provide the government with information that is 'not authorized to be intercepted.'" Id. But that, of course, is precisely what ISPs are required to do when ordered to route their traffic through the Carnivore system.

2. Lack of Accountability

Standing alone, Carnivore's inherent ability to "over-collect" communications renders it legally and constitutionally suspect. That flaw is exacerbated by the system's lack of an effective accountability mechanism. The Draft Report states that the reviewers "did not find adequate provisions (e.g. audit trails) for establishing individual accountability for actions taken during use of Carnivore." Id. The review team thus concluded that

> it is not possible to determine who, among a group of agents with the password, may have set or changed filter settings. In fact, any action taken by the Carnivore system could have been directed by anyone knowing the Administrator password. It is impossible to trace the actions to specific individuals. Auditing is crucial in security. It is the means by which users are held accountable for their actions. Draft Report, Section 4.2.4.

By underscoring the inadequacy of Carnivore's existing accountability mechanisms, we do not mean to suggest that an improvement of those mechanisms, as recommended by the reviewers, will render the continued use of Carnivore acceptable. Internal auditing mechanisms of any kind fail to establish the independent oversight of electronic surveillance required by federal statute and the Constitution.

3. Lack of Openness and Contradictory Information

The review team cited the many concerns that have been raised about Carnivore and expressed its opinion that "many of these concerns should be allayed by . . . Freedom of Information Act (FOIA) releases by the DoJ." Draft Report, Section 1.1.3. In fact, the FOIA process has produced a far different result. EPIC is currently litigating an FOIA lawsuit against DOJ and the FBI

seeking the full disclosure of information concerning Carnivore. Electronic Privacy Information Center v. Department of Justice, et al., Civ. No. 00-1849 (D.D.C.). While a great deal of responsive material has been withheld from disclosure, the information released thus far indicates that the capabilities of Carnivore are more far-reaching than earlier believed.

One of the documents EPIC obtained, dated June 5, 2000, reports the results of tests performed on Carnivore version 1.3.4, which is currently in use. The report indicates that Carnivore, in apparent contradiction of FBI assertions, can "reliably capture and archive all unfiltered traffic."

The FBI's public defense of Carnivore has centered on the claim that the system only captures traffic that has been isolated by a software filter that limits collection to the particular information authorized for seizure in a court order. Thus, in testimony before the Senate Judiciary Committee on September 6, 2000, FBI Assistant Director Kerr stated:

> If the subject's identifying information is detected [by the filter], the packets of the subject's communication associated with the identifying information that was detected, and those alone, are segregated for additional filtering or storage. However, it's critically important to understand that all . . . other communications are instantaneously vaporized after that one second. They are totally destroyed; they are not collected, saved, or stored.

This discrepancy was recently noted by Senators Hatch and Leahy in a letter to FBI Director Freeh. They wrote that "[s]kepticism about Carnivore is based precisely on concerns about this program's capability and whether this capability would be exploited to do more than just intercept narrowly targeted pieces of information." The Senators have therefore requested "complete and unredacted copies of the documents produced thus far in response to the FOIA lawsuit together with any other documents related to Carnivore's capability to intercept and archive unfiltered traffic."

4. Conclusion

EPIC agrees that the serious questions surrounding Carnivore can only be resolved through the full public disclosure of relevant information. We thus join Senators Hatch and Leahy in requesting the disclosure of all material withheld from us under the FOIA. We further believe that comprehensive Congressional oversight hearings and review of Carnivore's source code by the technical community must occur to determine (1) the actual capabilities of the Carnivore system; (2) whether use of Carnivore complies with federal statutory requirements; and (3) whether amendments to federal wiretap law are required before use of this system is permitted. While the IITRI review represents an important contribution to public understanding of Carnivore, it is clearly no substitute for the open process we suggest. Until Carnivore is subject to such open review and debate, we urge the Department of Justice and the Attorney General to suspend its use.

Respectfully submitted,

David L. Sobel
General Counsel
Electronic Privacy Information Center