1 OKLA. J. L. & TECH. 2 (2003)
(formerly 2003 OKJOLT Rev. 2)
www.okjolt.org

Abstract

Scott Griner, a 2003 University of Oklahoma Law School graduate introduces us to the FBI's email monitoring system, Carnivore. After a brief description of Carnivore and its use in criminal investigations, Mr. Griner analyzes Carnivore under the Fourth Amendment. Finally, Mr. Griner examines The USA PATRIOT Act's impact on the FBI's use of Carnivore and the future of electronic surveillance and searches.

FBI'S CARNIVORE: UNDER THE FOURTH AMENDMENT AND THE USA PATRIOT ACT

Scott Griner

I. Introduction

In the mid-1990's, the Federal Bureau of Investigation (FBI) recognized the use of the internet and e-mail by the criminal element to defeat traditional methods of surveillance. In 1996, the FBI developed the Omnivore program but abandoned it due to technical difficulties. The FBI then created a number of programs to replace Omnivore.

The current version of these programs, known as the "DragonWare Suite,"[1] contains the "Carnivore" and computer program. The FBI claims Carnivore is a tool that "surgically"[2] monitors e-mail between certain suspect parties while allowing e-mail of other parties to remain private.

The first part of this paper will perform a Fourth Amendment analysis regarding the use of the Carnivore program. The second part will explore the effects of the USA PATRIOT Act on the

[1] *FBI's Carnivore Hunts in a Pack*, MSNBC, Oct. 17, 2000, *available at* http://zdnet.com.com/2102-11-524798.html (last visited Jan. 9, 2003).
[2] Carnivore Diagnostic Tool, *available at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.html (last visited Jan. 9, 2003).

use of Carnivore by the FBI. It should be noted that Carnivore is used for national security investigations but this paper will only cover use in criminal investigations.

II. The Carnivore Diagnostic Tool (DCS-1000)

The exact date of the development of Carnivore is unclear, but FBI began using Carnivore in 1999.3 Carnivore was unknown to the general public until The Wall Street Journal published an article in July of 2000 revealing its existence. Due to the questions regarding protection of civil liberties created by this revelation,4 the Justice Department decided to publish a brief description of the function and the safeguards involved in the Carnivore program as well as an "independent review" of the software by the Illinois Institute of Technology and Research Institute.

A. Carnivore's Function

Agents attach the Carnivore tool to an Internet Service Provider's (ISP) server pursuant to a court order[5] and the traffic routing through that server is copied. The copy is then sent to a predefined "filter" which "sniffs"[6] the network packets comprising e-mail, instant messages and other types of communications.[7] Carnivore allows only the traffic matching the court order to pass the filter. The traffic not allowed past the filter is "dropped out" of the system. The communications

---

[3] *FBI's Carnivore Hunts in a Pack*, MSNBC, Oct. 17, 2000, *available at* http://zdnet.com.com/2102-11-524798.html (last visited Jan. 9, 2003).
[4] Letters from House Majority Leader Dick Armey to Attorney General Janet Reno, *available at* http://www.freedom.gov/library/technology/carnletter.asp and http://www.freedom.gov/library/technology/carnletter2.asp (last visited Jan. 9, 2003)
[5] A court order must be obtained pursuant to Title III guidelines for interception of private communications.
[6] Sniffing consists of searching each packet for predetermined information such as names, addresses, keywords, etc.
[7] Unlike the "Echelon" program run by the National Security Agency, the FBI claims Carnivore does not search through the contents of every message collecting the ones containing keywords, like "bomb" or "marijuana." Carnivore instead "sniffs" packets looking for messages sent from a certain account, or to a particular user, which is determined by the court order.

matching the filter are then copied to a permanent storage media. Only personnel authorized by the FBI can access the storage media, preserving the chain of evidence.

The Carnivore filter can be defined to allow a pen-register type of record, a content trap, as well as recording "instant message" exchanges. The FBI claims[8] this ability is superior to allowing the ISP's to "clone"[9] the communications because all communications not fitting the filter disappear. The ISPs are also unable to reliably reproduce instant messages. If the ISP "cloned" all communications the agents would be inspecting vast amounts of private communication needlessly, or missing messages in the instant message format.

B. The Pen-Register and Carnivore

1. Legal Aspects of the Pen-Register Capability of Carnivore

The first interception mode which Carnivore allows is referred to as the "pen- register." This is much like a pen-register on a telephone, which logs only the numbers dialed from the monitored phone line. The pen-register mode on the Carnivore system displays the Internet Protocol (IP) address numbers of the recipient and sender. An IP address is assigned to each user by the Internet provider to allow for identification and also functions as an address for e-mail and instant messaging purposes.

---

[8] *Internet and Data Interception Capabilities developed by the FBI*: *Hearings Before Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 4 (2000) (statement of Donald M. Kerr, Asst. Dir., FBI Lab. Div.).

[9] "Cloning" by the ISP consists of the creation of a duplicate mailbox which receives a copy of all communications sent to the original.

The Assistant Director of the Laboratory Division of the FBI, Donald Kerr, argues the Supreme Court in *Smith v. Maryland* has upheld this type of interception.[10] The Court held that there was no reasonable expectation of privacy in electronic impulses dialed and transmitted over a telephone line.[11] Kerr also claims that *United States v. Miller* is controlling, because a person has no expectation of privacy in any records they voluntarily hand over to a third party.

The disclosure of identities and the billing records relied on in *Smith* easily distinguishes Carnivore's pen register mode from the use of the telephone pen register.

The Court in *Smith* pointed out that pen registers "disclose only telephone numbers" and that no identities were disclosed.[12] The use of an e-mail address could disclose the identity of the user. Many e-mail addresses contain the users' name, initials, birthday, and other personal information. The pen register would therefore disclose the user's identity to the agents. This was impossible with a telephonic pen register without looking through a phone directory, or a reverse lookup.[13]

Other e-mail addresses may disclose where the sender or recipient works, as well as their associations. For example, possible e-mail addresses could be "Me@mywork.com" or "Me@myassociation.com." These would all be outside the realm of information the Court allowed to be gathered in *Smith v. Maryland*.

---

[10] Carnivore Diagnostic Tool: Hearing before The Committee on the Judiciary of the US Senate, 106th Cong. 5 (2000) (statement of Donald M. Kerr, Asst. Dir., FBI Lab. Div.).
[11] United States v. Miller, 425 U.S. 435, 442-44 (1976).
[12] Smith v. Maryland, 442 U.S. 735, 741 (1979) (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).
[13] A reverse lookup lists phone numbers in numerical sequence followed by the name of the residence or business the number is assigned to.

Proponents of Carnivore would argue that using one's name for an e-mail address would be voluntarily disclosing that information to third parties, as in *United States v. Miller*. This voluntary revelation would disallow any reasonable "expectation of privacy."

In *Katz v. United States*, the Supreme Court established a two-prong test. The Court held the person must exhibit an actual expectation of privacy. The Court further established the expectation "be one that society is prepared to recognize as 'reasonable.'"[14] If the use of one's name as an e-mail address is not considered to destroy the reasonable expectation of privacy, the Court would likely find that it is not "one that society is prepared to recognize as 'reasonable'", and thus fail the two prong test of *Katz*. A reasonable expectation of privacy was also addressed by the Court in *Smith.* The Court reasoned that people have no expectation of privacy because numbers dialed are kept "for making permanent records...they see a list of their long distance (toll) calls on their monthly bills."[15] They are aware that they must send numbers to the telephone company in order to complete a call, or for other legitimate business purposes.

The billing or legitimate business purpose argument is untrue for ISP's. The billing for internet access is charged by number of hours of access, or by a flat monthly charge. The ISP does not keep a running total on the number and addresses of the sender or recipient. Further, there are many free e-mail services, such as Hotmail.com, that would not maintain records for billing purposes. However, this lack of billing records argument was attempted in *Smith* but failed to

[14] Katz v. United States, 389 U.S. 347, 361 (1967).
[15] Smith v. Maryland, 442 U.S. 735, 742 (1979) (quoting United States v. New York Tel. Co., 434 U.S. 159, 174-75 (1977)).

persuade the Court. The defendant claimed that phone companies do not record local calls for billing purposes, and thus he had an expectation of privacy in his local call. The court stated, "[T]he fortuity of whether or not the telephone company in fact elects to make a quasi-permanent record ... does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information... it was free to record."[16]

One aspect not discussed in any court cases thus far is the monitoring of thousands of users' data, to find one particular user's communications. Due to the placement of the Carnivore box on a specific server, every user's data passing through that server is passed through the "filter." In essence, there are random searches taking place at any given time of thousands of non-suspect users. This risk was not present in a "pen register" on a specific phone line.

In *Berger v. New York*, Justice Douglas stated that a "traditional wiretap or electronic eavesdropping device constituted a dragnet, sweeping in all conversations within its scope without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations."[17] Justice Douglas would likely object to the use of the Carnivore system for monitoring thousands of non-suspect party's conversations to intercept the communications of a single target.

The government would likely argue that the information is not truly searched. For instance, the communications not matching the filter are allowed to pass without ever being copied to the

[16] *Id*. at 745.
[17] Berger v. New York, 388 U.S. 41, 65 (1967).

permanent media, or subjected to further scrutiny. Thus no agent of the government ever knows what information has passed by unrecorded. Based on prior decisions, the Court will likely continue to allow the use of Carnivore in the pen register setting.

2. Independent Review and Technical Problems with Carnivore's Pen Register Mode

The Illinois Institute of Technology and Research Institute (IITRI) and Chicago-Kent College of Law independently reviewed the Carnivore program at the request of the United States Department of Justice. The integrity of the review has been questioned due to the terms on which the review was performed.[18] However, during the review several problems with the software were uncovered which have direct implications on the constitutionality of intercepts made using Carnivore.

Due to the nature of internet traffic, e-mail and other communications are broken into network packets. Each packet contains the routing, or addressing information as well as a portion of the content. These packets travel along individual paths, choosing the quickest route through the server, and are then reassembled at the receiving point.

While in pen-register mode, Carnivore "collects more than is permitted by the strictest possible construction of the pen-trap statute."[19] It captures the entire communication, including the

---

[18] Many objections were raised due to the fact that the Justice Department refused to name the contractor which created the program and refused to release all source codes to the reviewing party. Many of the reviewers also had strong ties to the Justice Department, and the Clinton Administration. The most publicized objection was a letter dated Oct. 19, 2000, from House Leader Dick Armey to Attorney General Janet Reno, *available at* http://www.freedom.gov/library/technology/carnletter2.asp (last visited Jan 9, 2003).

[19] *Independent Technical Review of the Carnivore System*, Dec. 8, 2000, at 4-3, *available at* http://www.epic.org/privacy/carnivore/carniv_final.pdf (last visited Jan. 9, 2003).

content, and then replaces the content with an "X." As a result, the agent may know how many characters are in a communication, but they would be unable to discern any of the actual content.

Carnivore has also been proven by the independent review to capture entire "headers" in some protocols.[20] The "header" of an e-mail contains the sender and recipients address lines, as well as the subject line. The subject line could be considered to be part of the content of the communication since it might reveal the purpose of a communication or something more than the IP numbers needed for routing.

In addition, Carnivore's pen-register mode captures and displays the length of communications. Such information might allow an analysis which could identify the web pages the user accessed. This over collection would result in a violation of the "no content" rule in a pen-register warrant.

It is apparent that the problems in the technical aspects of Carnivore may lead to constitutional violations stemming from the pen-register mode's over-collection of information. Until such problems are fixed, Carnivore should not be operated in this capacity. By continuing to use Carnivore in pen-register mode, the FBI risks violating the Fourth Amendment rights of legitimate suspects, and perhaps more disturbing, the rights of countless persons not under suspicion.

C. Carnivore's Use in Monitoring the "Content" of Communications.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2522 (Title III) provides standards for the collection of "content" in electronic surveillance actions.

---

[20] *Id.*

Pursuant to Title III, the FBI must secure a warrant from a federal court before placing the Carnivore system on an ISP.[21]

The collection process is the same described in Section II A. In the "content" collection setting, Carnivore collects the address of the party sending the communication, the address of the recipient, the date, the time, and body of the communication. The communications matching the filters are then copied to a removable media[22] and examined by federal agents.

1. Minimization

One area of concern in electronic surveillance is the minimization process. Title III requires an interception to be executed "in such a way as to minimize the interception of communications not otherwise subject to interception" in the order.[23] In no way does Title III forbid the interception of all other communications, instead it requires there are steps taken to reduce the amount of non-conforming communications intercepted.

The FBI argues that the Carnivore's filter setting, which can be "extremely complex,"[24] reduces the number of intercepts not matching the order. Carnivore will record only those messages matching the filter, and allow those not matching the filter to pass freely.[25] An authorized agent then sorts through the e-mail to ascertain whether it is of interest to the investigation. If not of interest the e-mail is deleted.

---

[21] 18 U.S.C.A. § 2516 (2002).
[22] The removable storage media is reportedly an Iomega Jazz Disk.
[23] 18 U.S.C.A. § 2518(5) (2002).
[24] Presumably the filters may be set to allow communications from certain addresses, at certain times, etc...allowing for a precise intercept of communications matching the court order.

Opponents of Carnivore may argue that if the program records disallowed information, the case agent then has access to it before it is deleted. However, this argument is unpersuasive. During the process of a normal telephone intercept, an agent hears the conversation and then determines whether it is relevant to the investigation authorized by the warrant. This process allows the agent to listen to parts of all conversations before deciding whether the conversation is included under the terms of the warrant.

Less information is screened by the agent when Carnivore is used than is screened in a telephone tap. Carnivore "prescreens" what the agent views; essentially allowing the agent to see only previously "minimized" material. The agent then views only material determined to be relevant to the investigation.

In the area of minimization, Carnivore may be an improvement over the previous methods of minimization. The agents only have access to materials already screened by Carnivore, in effect cutting their knowledge of areas outside of the scope of their investigation. In an ordinary minimization process the agents would see all communications then decide which are relevant to the investigation.

---

[25] *Internet and Data Interception Capabilities developed by the FBI*: *Hearings before Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106 Cong. 4 (2000) (statement of Donald M. Kerr, Asst. Dir., FBI Lab. Div.)

2. Over-breadth

FBI Assistant Director Robert Kerr claimed that Carnivore program is not a keyword search utility and that Carnivore searches only those messages matching the preset filters.[26] Since his statement, there has been much speculation regarding the abilities of Carnivore.

The independent review concluded that Carnivore can "scan a subset of network traffic for specific strings or access by or to specific sites."[27] This contradicts Assistant Director Kerr's statement of Carnivore's ability to search for "keywords." As stated by the independent review panel, Carnivore can also go a step further and monitor access to specific web sites by the target user.[28] The panel qualifies the statement by adding that the program can collect this type of data in "court authorized cyber-terrorism" activities.

The review also disclosed that although Carnivore "was designed to, and can, perform finely tuned searches, it is also capable of broad sweeps."[29] The review does not elaborate as to the meaning of the term "broad sweeps." However, taken in context with Carnivore's abilities, like keyword searching and monitoring website access, Carnivore goes beyond the capabilities of previous electronic surveillance.

The potential for abuse of the system alone is not enough to make it unconstitutional. A neutral judge oversees the use of Carnivore's content mode and this introduces a roadblock to an

---

[26] *Id.* at 4.
[27] *Independent Technical Review of the Carnivore System*, 8 Dec. 2000, at 4-4, *available at* http://www.epic.org/privacy/carnivore/carniv_final.pdf (last visited Jan. 9, 2003).
[28] *Id.*
[29] *Id.*

overreaching investigator. In this manner, Carnivore is no different than other tools of electronic surveillance already in use. Various district courts have upheld the use of Carnivore in approximately 50 cases thus far and will likely continue to do so.

III. A Constitutional Analysis of Carnivore

Obviously, technological advances such as Carnivore are necessary to stem the use of technology by the criminal element. The court in *United States v. United States District Court for the Eastern District of Michigan* reasoned:

> The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law abiding citizens.[30]

This statement, written in 1972, is no less applicable today. When the criminal element seeks to use technological advances to hide their crimes, the government must be permitted to use the same covert measures to protect the public.

The legal theories behind the use of Carnivore are sound. In pen-register searches, the only difficulty may be deciding whether an e-mail address discloses the identity of the sender, in conflict with the decision in *Smith v. Maryland.*[31] The Supreme Court's ruling in this regard will ultimately resolve the constitutional questions presented.

---

[30] United States v. United States Dist. Court, 407 U.S. 297, 312 (1972).
[31] Smith v. Maryland, 442 U.S. 735 (1979).

The technical problems with Carnivore in the pen register mode make it unconstitutional in its current state. The inclusion of content, as well as the ability to track web site access in pen register mode clearly puts it outside the acceptable limits on data collection without a warrant.

Clearly, a flawless version of Carnivore is the tool that would allow the government to protect the public interest in privacy, while furthering the government's interest in law enforcement.

A. The Effects of the USA PATRIOT Act on the Use of Carnivore.

In response to the terrorist attacks in New York, Washington D.C. and Pennsylvania, the United States Congress passed the USA PATRIOT Act.[32] This law made changes to many aspects of criminal law and procedure. Sections 216 and 218 of the USA PATRIOT Act specifically deal with the area of electronic surveillance.

B. Section 216 Exclusion of Contents

Section 216 of the USA PATRIOT Act modifies the use of pen register and trap and trace devices. Under § 216, 18 U.S.C. § 3121 is changed to permit the monitoring of "electronic communications so as not to include the *contents*" of the electronic communication.[33] (emphasis added) However, nowhere in the Act does the Congress define the word "content."

As previously discussed, "contents" should include the capturing of the body of the communication which is then replaced by "X's", or the ability to monitor the target's access to web sites by use of the length of the communications. Carnivore's abilities in these areas would clearly

[32] Pub. L. No. 107-56, 115 Stat. 272 (2001). The full title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT ACT).
[33] USA PATRIOT Act § 216(a) (amending 18 U.S.C. § 3121(c) (2000)).

violate the USA PATRIOT Act's limitations in pen register mode. The definition of "content" must be established before the legality of Carnivore's use under the Patriot Act may be determined with any certainty.

C. The "General Warrant" Argument

Section 216 of the USA PATRIOT Act also modifies 18 U.S.C. § 3123(a) in other minor ways. The changes allow an order to be issued "authorizing the installation and use of a pen register or trap and trace device *anywhere in the United States*".[34] (emphasis added)

Previously, the statute allowed the warrant to be issued only by the district in which the facility to be searched was located. This would allow a judge in Oklahoma City to issue a warrant for a facility in Mountain Home, Idaho, effectively blunting the Idaho facility's ability to contest the warrant.

The most disturbing part of section 216 of the USA PATRIOT Act to civil libertarians is a section they claim directly contravenes the specificity requirement of the Fourth Amendment. Section 216(b) mandates:

> the order *shall apply to any person or entity* providing wire or electronic communication service in the United States...Whenever such an order is served on any person or entity *not specifically named in the order*, upon request of such entity, the *attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served*.[35] (emphasis added).

The Fourth Amendment clearly states,

---

[34] USA PATRIOT Act § 216(b) (amending 18 U.S.C. § 3123(a)(1) (2000)).
[35] USA PATRIOT Act, § 216(b) (amending 18 U.S.C. § 3123(a) (2000)).

> 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.[36] (emphasis added).

The opponents claim that under the USA PATRIOT Act, the government essentially obtains a blank warrant they may apply to anyone or any ISP, at any location in the country. In essence, the particularity requirement of the Fourth Amendment is wholly eviscerated.

There is no judicial oversight on the government's use of the warrant because under the Act, the government attorney or law enforcement officer serving the warrant certifies to the person served that the warrant covers the unnamed party. Prior to passage of the Act, a judge or magistrate determined its applicability to the parties. This process effectively cuts off judicial review of the appropriate use of the warrant. According to *United States v. United States District Court for the Eastern District of Michigan*, "those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[37] Later the court also observed "the independent check upon executive discretion is not satisfied...by extremely limited post-surveillance judicial review."[38]

However, in *Smith v. Maryland*, the court held there was no need for a warrant to collect pen-register information because it was not a "search" under the meaning of the Fourth Amendment.[39]

---

[36] USA PATRIOT Act § 216(b) (amending 18 U.S.C. § 3123(a)(1) (2000)).
[37] United States v. United States Dist Court, 407 U.S. 297, 317 (1972)
[38] *Id.* at 317-18.
[39] Smith v. Maryland, 442 US 735, 746 (1979).

Therefore, there is no constitutional basis for the requirement of a warrant for pen-register information.

Since there is no "search", the only requirement for a warrant for pen-register information was codified in 18 U.S.C. § 3123. Congress enacted this requirement; they may modify it as they have done in the Patriot Act.

D. The Section 216 (b) Requirements and Carnivore's Technical Problems

Section 216 of the USA PATRIOT Act added some basic requirements to 18 U.S.C. § 3123 for an agency's use of its own device in collecting pen-register information. It requires that a law enforcement agency installing its own pen-register or tap and trace device:

> Shall ensure that a record will be maintained that will identify-
>
> i. any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
> ii. the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
> iii. the configuration of the device at the time of its installation and any subsequent modification thereof; and
> iv. any information collected which has been collected by the device.[40]

These requirements are of the basic type to ensure accountability in the record, and to preserve the chain of custody. In the technical review of Carnivore each of these requirements were not met by the current version of the program.

[40] USA PATRIOT Act § 216(b) (amending 18 U.S.C. § 3123 (2000)).

All FBI agents had access to the information in Carnivore through the use of the password "Administrator."[41] Anyone could access the device and information without being identified as required by the modifications to § 3123 (a)(3)(A)(i) in the USA PATRIOT Act. The independent review stated, "[I]t is impossible to trace the actions to the specific individuals."[42]

The independent review board also disclosed the fact that "it is not possible to definitively show what settings were used to collect any given set of data."[43] There is a possibility that information collected to be used in court could have been collected in violation of the court order by using the "content" setting instead of the pen-register setting with the current version of Carnivore.

The review also stated that there are no safeguards to prevent the information colleted from being changed. The disks used to store the data are not tamper proof, non-magnetic disks. Since all users also logged in as "Administrator," there would be no record or evidence of changed files, or who changed them.[44]

The requirements for the FBI's use of Carnivore are clearly delineated in the statute. Based on the independent review of the current version of Carnivore, it is clear that its use violates the congressional mandate set out in the USA PATRIOT Act.

---

[41] *Independent Technical Review of the Carnivore System*, Dec. 8, 2000, at 4-5, *available at* http://www.epic.org/privacy/carnivore/carniv_final.pdf (last visited Jan. 9, 2003).
[42] *Id*.
[43] *Id*. at 4-6.
[44] *Id.*

E. Section 218 and the "Significant Purpose" Standard

The USA PATRIOT Act modified the standard used to obtain a warrant under the Foreign Intelligence Surveillance Act (FISA).[45] Under FISA, there is no showing of probable cause of criminal activity needed to obtain a warrant. The government was required to show that foreign intelligence was the "purpose" of the surveillance.[46]

As a result of Section 218 of the USA PATRIOT Act, the standard has been lowered and the government must prove that a "significant purpose"[47] of the surveillance is to obtain foreign intelligence information. There is a possibility the government can now tap the lines of a suspect for primarily criminal purposes, but also for some aspects of a foreign intelligence interest, without a showing of probable cause. This would clearly be contrary to the protections of the Fourth Amendment.

There is a feeling by some that the FBI and other agencies will attempt to use this provision as an end around the more stringent probable cause standard for criminal investigations. The American Civil Liberties Union (ACLU) is one of the groups leading this protest. The ACLU accuses the government of an unwarranted power grab.

The ACLU, in one of its publications, admitted that Section 218 could not be used for the purposes of criminal investigations. The ACLU publication states: "[C]ourts will exclude the evidence gathered from surveillance conducted under section 218, because the probable cause of

[45] 50 U.S.C. §§ 1801-1811
[46] 50 U.S.C. § 1804.
[47] USA PATRIOT Act § 218 (amending 50 U.S.C. § 1804 (2000)).

crime requirement was not met for a search conducted primarily to gather evidence of crime."[48] The publication also stresses, "Americans who oppose U.S. policies and who are believed to have ties to foreign powers could find their homes broken into and their phones tapped."[49]

The ACLU has clearly overlooked the requirements of 50 U.S.C. § 1805. This section requires that there must be "probable cause" to believe that the person is an agent of a foreign power before a warrant is issued. It provides that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution."[50] To establish probable cause the prosecution must demonstrate to the court that the target has performed suspicious actions, or has participated in activities that would lead others to believe the target is acting as an agent of a foreign power.

IV. Conclusion

The need for law enforcement agencies to possess the proper skills and tools to enable them to combat today's technology savvy criminals cannot be underestimated. However, the need for protection of the public's civil liberties cannot be overlooked in a rush to fight crime.

The FBI's motive for creating Carnivore was to combat the flagrant use of the internet and e-mail as a tool of criminals. It seems that, in a rush to develop a working program, the FBI has

[48] *How the USA-Patriot Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases, available at* http://www.aclu.org/congress/1102301i.html (last visited Dec. 15, 2002).
[49] *Id.*
[50] 50 U.S.C. § 1805 (a)(3)(A) (2000).

skipped some integral steps that would allow the use of the program in an efficient and constitutional manner.

The legal foundation theory for the use of Carnivore as a pen-register device lies in the *Smith v. Maryland*,[51] and *United States v. Miller*[52] decisions noted earlier. The one foreseeable problem is the ability of e-mail addresses to disclose the identity of the sender.[53]

The technical problems with Carnivore in the pen register setting should disqualify it from use under Section 216 of the USA PATRIOT Act. Section 216 plainly states that there must be audit trails, which are presently unavailable. The accessibility by all agents using the "Administrator" password specifically contravenes the requirement of accountability.

The use of Carnivore in a Title III based "content" search will likely continue to be upheld by the courts. The minimization procedure is one of the main concerns expressed by opponents of the system. However, in this respect Carnivore is clearly superior to the previous types of electronic surveillance. The filter takes out the vast majority of communications unrelated to the investigation before a human ever sees the material.

The actual abilities of Carnivore are somewhat still unclear. The independent review answers some questions regarding its capabilities, while leaving others unanswered. The program does have the ability to track web site access, and perform keyword searches of the target's communications.

---

[51] Smith v. Maryland, 442 U.S. 735 (1979).
[52] United States v. Miller, 425 U.S. 435 (1976).
[53] The decision in *Smith v. Maryland* was adamant regarding this point. The Supreme Court will likely decide the disclosure of the identity is no more than a voluntary disclosure under *United States v. Miller*. If so, the use of Carnivore as a pen-register device can be upheld.

All these capabilities are the type of activity allowed by a Title III warrant and therefore, if done pursuant to a validly issued warrant, perfectly legal.

In the post September 11th climate, many citizens, as well as our elected leaders, seem willing to trade some of our civil liberties in exchange for a sense of security. The USA PATRIOT Act is one of the measures born out of this desperation. Predictably, some decry the USA PATRIOT Act as a blatant attack on civil liberties.

This attack is unfounded when it pertains to the changes in electronic surveillance measures affected by the Act. These changes have not affected the rights of Americans in a criminal investigation involving electronic surveillance. In fact, the use of the current, flawed version of Carnivore constitutes an express violation of the statute. The USA PATRIOT Act may contain worrisome changes in some areas, but electronic surveillance of criminal cases is not among them.

The government is slowly creeping into all areas of its citizens' lives under the guise of protection from terrorism, child endangerment, or whatever is fashionable at the time. Justice Douglas foresaw this in 1966. In *Osborn v. United States*, he wrote, "we are rapidly entering an age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the government increase by geometric proportions."[54]

[54] Osborn v. United States, 385 U.S. 323, 341 (1966).

In the thirty-six years since this statement was written, technology has made amazing advances allowing the government to enter before unknown areas of surveillance. It will continue to do so, unless we remain vigilant.