Missouri Law Review

Volume 66
Issue 4 *Fall 2001*

Article 3

Fall 2001

# Don't Fear Carnivore: It Won't Devour Individual Privacy

Thomas R. McCarthy

# Don't Fear Carnivore: It Won't Devour Individual Privacy

*Thomas R. McCarthy**

## I. INTRODUCTION

A federal law enforcement agent in a small town is investigating a suspected terrorist cell operating within the United States.[1] He has no real leads until an informant[2] tips him off that the terrorist cell is planning to commit a terrorist act somewhere during the upcoming weekend. The informant does not know when or where, but the informant does know that the local head of the terrorist cell communicates with his fellow terrorists via electronic mail ("e-mail") and instant messaging. The informant reveals that the head of the cell has an account with the United States-based Internet service provider ("ISP") GoNet, his user name is Terror, and his e-mail address is terror@gonet.com. The law enforcement agent immediately contacts the system administrator at GoNet and asks the administrator for permission to search and seize the e-mail and instant messaging traffic recently sent from Terror's account.[3] Upon advice from GoNet's counsel, the GoNet administrator refuses to consent to the search and seizure of the traffic from Terror's account. As with all of its users, GoNet has a privacy agreement with Terror, which states that GoNet will not disclose or disseminate information about Terror or about Terror's Internet transmissions except in response to a valid legal subpoena.[4] The law enforcement agent issues a subpoena to GoNet, ordering

---

* Law Clerk to the Honorable Frank W. Bullock, Jr., United States District Judge for the Middle District of North Carolina. B.S., University of Notre Dame 1995; J.D., George Mason University School of Law 2001. The views expressed herein do not necessarily reflect those of Judge Bullock. The Author would like to thank Christian Genetski, Richard Salgado, William Consovoy, and especially Rachel Reda for their helpful comments on earlier drafts.

1. Investigations following the September 11, 2001 terrorist attacks on the United States have "exposed the rough outlines of at least a half-dozen centers of terrorist support on U.S. soil operating underground." Associated Press, *Terrorists May Have Support Among Us*, NEWS & RECORD (Greensboro), Nov. 18, 2001, at A1.

2. Note that an informant's tip can be used to establish probable cause. *See generally* Illinois v. Gates, 462 U.S. 213, 231-39 (1983). Such tips are judged under a totality of the circumstances test, through which the court will look to the informant's veracity, reliability, and basis of knowledge. *Id.* No one factor is dispositive; all are relevant to the always-fluid concept of probable cause. *Id.*

3. In order to obtain retrieved or fresh, unretrieved e-mail communications, law enforcement officials must comply with the Stored Wire and Electronic Communications and Transactional Access Act. *See* 18 U.S.C. §§ 3121-27 (1994 & Supp. V 1999).

4. The typical privacy agreement includes a similar provision. *See* STARPOWER,

GoNet to produce the transactional information associated with and the contents of Terror's recent e-mail and instant messaging communications. The subpoena further orders GoNet to transmit Terror's future communications to law enforcement in real time. GoNet cannot comply fully with the subpoena because it does not have the technical capabilities to relay the possibly time-sensitive e-mail information quickly to law enforcement. What can the law enforcement agent do?

Enter Carnivore,[5] the software created by the Federal Bureau of Investigation ("FBI") that functions as a cyberwiretap. The FBI states that "Carnivore is software . . . designed to capture network traffic . . . and save that traffic to a storage medium."[6] The Department of Justice ("DOJ") believes that Carnivore is a necessary tool for law enforcement to combat the increasing number of everyday crimes that are "migrating to the Internet."[7] Investigating and "tracking

---

*Internet Access Agreement* ("STARPOWER reserves the right under appropriate circumstances to disclose the identity of a subscriber to third parties in response to a valid legal subpoena and to otherwise cooperate with legitimate police inquiries and lawful civil proceedings."), *at* http://www.starpower.net/services/internet/agreement.html (last visited Nov. 13, 2001).

5. In early 2001, the Federal Bureau of Investigation ("FBI") changed the name Carnivore to DCS1000 because the FBI feared that the "name Carnivore contributed to some perceptions that the application was a predatory program that could invade citizens' privacy." Matt McLaughlin, *FBI's Upgrade of Carnivore Includes a New Name*, GOV'T COMPUTER NEWS (Feb. 12, 2001), *at* http://www.gcn.com/vol1_no1/daily-updates/3661-1.html. The Author will continue to use the name Carnivore.

6. Electronic Privacy Information Center, *Carnivore FOIA Documents: Purpose*, *available at* http://www.epic.org/privacy/carnivore/purpose.html (last visited Nov. 13, 2001). These documents were heavily redacted by the FBI before they were released to the Electronic Privacy Information Center ("EPIC"). *See generally* Electronic Privacy Information Center, *Carnivore FOIA Documents* [hereinafter Carnivore FOIA Documents], *available at* http://www.epic.org/privacy/carnivore/foia_documents.html (last visited Nov. 13, 2001). David Sobel, an attorney for EPIC, "said that the [EPIC] intends to challenge the FBI's editing of the released documents." Kevin Poulsen, *Carnivore Details Emerge*, SECURITYFOCUS (Oct. 4, 2000), *at* http://www.securityfocus.com/news/97.

7. *See* Deputy Assistant Attorney General Kevin V. Di Gregory, "Carnivore" and the Fourth Amendment, Statement Before the Subcommittee on the Constitution of the House Committee on the Judiciary (July 24, 2000) [hereinafter Di Gregory Statement I], *available at* http://www.usdoj.gov/criminal/cybercrime/carnivore.htm. More recently, in the wake of the September 11, 2001, terrorist attacks on the United States, the government has sought to use Carnivore as a means to fight terrorism. *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified in scattered sections of 18, 47, & 50 U.S.C.).

the online criminal requires law enforcement to attempt to trace the 'electronic trail' from the victim back to the perpetrator. In effect, this 'electronic trail' is the fingerprint of the twenty-first century—only much harder to find and not as permanent as its traditional predecessor."[8] The DOJ stated that the nation's "vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also [our] critical infrastructure."[9] Testimony before Congress demonstrates the DOJ's belief that Carnivore is necessary for law enforcement to conduct the type of investigation required to make the Internet safe:

> [W]e have found that, at times, the Internet service provider has been unable or even unwilling to [comply with a request for information]. Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective . . . . If the Internet service provider can comply with [a lawful court] order . . . we will not employ Carnivore. If, however, the service provider is unwilling or unable to comply with the order, we cannot simply give a criminal a free pass. It is for that narrow set of facts that the FBI designed Carnivore.[10]

The DOJ believes that it can utilize Carnivore in a way that respects individual privacy.[11] However, electronic freedom activists and privacy groups, such as the Electronic Privacy Information Center ("EPIC") and the American Civil Liberties Union ("ACLU"), believe that Carnivore is an "excessive intrusion on individual privacy."[12] Both groups filed Freedom of Information Act requests with the FBI

---

8. Di Gregory Statement I, *supra* note 7.

9. Di Gregory Statement I, *supra* note 7. Deputy Assistant Attorney General Di Gregory attributed this remark to Deputy Attorney General Eric Holder. Di Gregory Statement I, *supra* note 7.

10. Di Gregory Statement I, *supra* note 7.

11. *See* Deputy Assistant Attorney General Kevin V. Di Gregory, The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age, Statement Before the Senate Committee on the Judiciary (Sept. 6, 2000) [hereinafter Di Gregory Statement II] (noting the "numerous mechanisms in place to prevent possible misuse of electronic surveillance"), *available at* http://www.usdoj.gov/criminal/cybercrime/kvd_0906b.htm.

12. Richard Stenger, *Universities Decline to Review FBI's 'Carnivore' System: Agency's Restrictions Seen as Overbearing* (Sept. 6, 2000), *at* http://www4.cnn.com/2000/TECH/computing/09/06/carnivore/index.html. American Civil Liberties Union ("ACLU") Associate Director Barry Steinhardt has referred to Carnivore as a "mass invasion of the privacy of law-abiding Americans." Press Release, ACLU, ACLU Says Government Stacked Deck in Selection of Team to Review

in the summer of 2000, seeking all agency records relating to Carnivore, including the Carnivore object code, because these groups believe that Carnivore violates individual privacy.[13] In addition, some groups contend that Carnivore does not even work properly.[14] Earthlink, Inc., an Atlanta-based ISP, recently reached an agreement with the FBI that allows Earthlink to avoid future use of Carnivore.[15] Prior to this agreement, the FBI's use of Carnivore on Earthlink's systems caused some Earthlink servers to crash, disrupting Internet access for several Earthlink customers.[16]

The incident with Earthlink and the uproar from privacy groups led former Attorney General Janet Reno to call for "an independent technical review of Carnivore to evaluate whether it performs the functions it was designed to perform, and does so without any greater threat to privacy or to the smooth operation of private service providers."[17] The DOJ contracted with the Illinois Institute of Technology and the Illinois Institute of Technology Chicago-Kent College of Law ("IITRI") to perform this independent technical review, and a draft report of the review was released on November 17, 2000.[18] Although many

---

"Carnivore" Cyber-tapping System (Oct. 4, 2000) [hereinafter Press Release, Government Stacked Deck], *available at* http://www.aclu.org/news/2000/n100400.html. Since the advent of the Internet age, civil libertarians have feared government intrusion into individual privacy. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 76 (1994) ("Americans' growing reliance on computers has vastly increased the potential for the government to use electronic surveillance to intrude into its citizens' private lives.").

13. *See, e.g.*, Press Release, ACLU, In Unique Tactic, ACLU Seeks FBI Computer Code On "Carnivore" and Other Cybersnoop Programs (July 14, 2000) [hereinafter Press Release, Unique Tactic], *available at* http://www.aclu.org/news/2000/n071400a.html. The documents that EPIC received from the FBI pursuant to its Freedom of Information Act ("FOIA") request are available online. *See* Carnivore FOIA Documents, *supra* note 6.

14. *See, e.g.*, Patricia Fusco, *The Appetite of Carnivore*, *at* http://www.isp-planet.com/politics/carnivore.html (last visited Nov. 13, 2001).

15. Associated Press, *Earthlink Dodges FBI's Carnivore*, USA TODAY, July 14, 2000, *available at* http://www.usatoday.com/life/cyber/tech/cti231.htm.

16. *Id.*

17. *See* Di Gregory Statement II, *supra* note 11.

18. *See* IIT RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM, DRAFT REPORT, at vii (Nov. 17, 2000) [hereinafter IITRI DRAFT REPORT], *available at* http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf. Several privacy groups attacked the Department of Justice's ("DOJ's") selection of IITRI, arguing that this group was not "independent." *See* Press Release, Government Stacked Deck, *supra* note 12. The ACLU called the group "biased." Press Release, Government Stacked Deck, *supra* note 12. The report of the review team was to be "made public to the maximum extent that is consistent with otherwise applicable law or contractual

details of this review were kept secret to preserve Carnivore's effectiveness as a tool of law enforcement, enough knowledge about Carnivore is available to determine whether it represents the potential "mass invasion of the privacy of law-abiding Americans" that privacy groups fear.[19] Law enforcement officials recognize the importance of respecting individual privacy, but they note that the ability to apprehend Internet criminals is necessary to protect individual freedom, as well:

> If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.[20]

This "proper balance" is the center of the debate between privacy groups and those who support the strengthening of law enforcement. The volume of the debate only has risen in the wake of the September 11, 2001, terrorist attacks on the United States. Determining whether Carnivore will be able to strike a "proper balance" between the government's respect for individual privacy and its ability to protect freedom requires a description of what Carnivore is and of what it is capable.[21]

Part II of this Article is a description of the Carnivore program, its development, its known uses, and its safeguards against misuse.[22] Part III is an explanation of the relevant law that governs electronic surveillance and individual privacy.[23] This explanation begins with a discussion of the Fourth Amendment

---

obligations and with preserving the continued effectiveness of the software as a law enforcement tool." Di Gregory Statement II, *supra* note 11.

19. *See* Press Release, Government Stacked Deck, *supra* note 12.

20. Di Gregory Statement I, *supra* note 7.

21. To date, there is still some information about Carnivore (most notably, its source code) that has been withheld from the public in order to preserve Carnivore's effectiveness as a law enforcement tool. *See supra* text accompanying note 19. Upon conclusion of its review of Carnivore, the IITRI actually recommended that the FBI "work toward public release of Carnivore source code." IITRI DRAFT REPORT, *supra* note 18, at xv.

22. *See infra* notes 26-82 and accompanying text.

23. *See infra* notes 83-147 and accompanying text.

and includes a discussion of applicable statutory law. Part IV is an analysis of Carnivore's effectiveness as a tool of law enforcement balanced against its compliance with the law respecting individual privacy.[24] Part V concludes that Carnivore fills an important need of law enforcement while complying the Fourth Amendment jurisprudence and statutory protections of individual liberties.[25]

## II. WHAT IS CARNIVORE?

Public opinion of Carnivore varies greatly. Depending upon the particular opinion, Carnivore may be either a system used to implement lawful "court-ordered surveillance of electronic communication"[26] or a "cybersnoop"[27] program "running out of a black box"[28] that constitutes an "excessive intrusion on individual privacy."[29] While many have an opinion about Carnivore, until recently, not much actual information has been available about the program. As requested by former Attorney General Janet Reno, an independent technical review of the program was conducted and a draft report made available information about Carnivore heretofore unknown by the general public.[30]

### *A. Carnivore: The Program and Its Development*

The FBI's electronic surveillance tool now known as Carnivore began as a different FBI project under a still-secret name sometime in the mid-1990s.[31] The FBI shut this original project down due to design problems and began development of a project called Omnivore in February of 1997.[32] By the end of October of that year, the first Omnivore prototypes were ready for field testing on Sun's Solaris operating system.[33] During this development and testing stage, the FBI deployed Omnivore in several emergency situations.[34]

In September of 1998, the FBI network surveillance lab in Quantico, Virginia, launched a project called "Phiple Treonix" to transfer Omnivore from the Solaris system to a Windows NT platform in order, among other things, to

---

24. *See infra* notes 148-64 and accompanying text.
25. *See infra* notes 165-68 and accompanying text.
26. IITRI DRAFT REPORT, *supra* note 18, at viii.
27. Press Release, Unique Tactic, *supra* note 13.
28. Press Release, Unique Tactic, *supra* note 13.
29. Stenger, *supra* note 12.
30. *See supra* note 18 and accompanying text.
31. *See* Poulsen, *supra* note 6. The "secret" name is redacted from the documents produced to EPIC pursuant to its FOIA request. *See* Poulsen, *supra* note 6.
32. *See* Poulsen, *supra* note 6.
33. *See* Poulsen, *supra* note 6.
34. *See* Poulsen, *supra* note 6.

"facilitate the miniaturization of the system and support a wide range of personal computer (PC) equipment."[35] The "Phiple Treonix" project produced the first official version of Carnivore.[36] This first official version was released in September of 1999 as version 1.2.[37]

Carnivore has undergone a series of tests and modifications since it was first released. In May of 2000, Carnivore was in version 1.3.4.[38] At that point, it had performed positively in several tests at the FBI network surveillance lab; the FBI reported that "Carnivore is remarkably tolerant of network aberration[s], such as speed change, data corruption and targeted smurf attacks."[39] IITRI noted that "Carnivore is [continuously] evolving to improve its performance, enhance its capabilities, and keep pace with Internet development and court rulings."[40]

Version 1.3.4 is the most current usable version of Carnivore, and it is the version that IITRI recently reviewed.[41] IITRI defines Carnivore as "a software-based tool used to examine all Internet Protocol (IP) packets on an Ethernet and record only those packets or packet segments that meet very specific parameters."[42] It is a "sniffer that can select and record a defined subset of the traffic on the network to which it is attached."[43] IITRI stated that the Carnivore architecture "comprises: (1) a one-way tap into an Ethernet data stream; (2) a general purpose computer to filter and collect data; (3) additional general purpose computers to control the collection and examine the data; and (4) a telephone link to the collection computer."[44] The one-way tap allows Carnivore to collect data

---

35. Poulsen, *supra* note 6. The other reasons for the transfer from the Solaris to the Windows system were redacted from documents received by EPIC pursuant to its FOIA request. *See* Poulsen, *supra* note 6.

36. *See* Poulsen, *supra* note 6.

37. Carnivore FOIA Documents, *supra* note 6.

38. *See* Electronic Information Privacy Center, *Carnivore FOIA Documents: Test Report of June 2000, available at* http://www.epic.org/privacy/carnivore/test_6_00.html (last visited Nov. 13, 2001).

39. *Id.* A smurf attack is an attack in which a computer hacker creates a computer program that "sends out an ICMP [Internet Control Message Protocol] echo request packet . . . to a computer network with the return IP address of the targeted victim. The network's server broadcasts the [echo request packet] through the system's network and the computers send a reply back. If the network is large enough, those [reply] packets will swamp the victim's computer and possibly bring the computer down." Eric J. Sinrod & William P. Reilly, *Cyber Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 194 (2000).

40. IITRI DRAFT REPORT, *supra* note 18, at vii-iii.

41. *See generally* IITRI Draft Report, *supra* note 18, at 2-1 to 2-2.

42. IITRI DRAFT REPORT, *supra* note 18, at vii.

43. IITRI DRAFT REPORT, *supra* note 18, at 1-1.

44. IITRI DRAFT REPORT, *supra* note 18, at viii.

but "ensures that Carnivore cannot transmit data on the network."[45] Currently, Carnivore simply stores the collected data as raw packets.[46] It requires a separate post-processing program called "Packeteer" to process "the raw output of Carnivore to reconstruct higher-level protocols from IP packets."[47] Another post-processing program called CoolMiner uses Packeteer's output to "develop statistical summaries and displays either pen-register or full content information via an Internet browser."[48] Carnivore can operate so that it selectively targets a certain subset of Internet traffic on a system. It can select a target "based on IP address, protocol, or, in the case of e-mail, on the user names in the TO and FROM fields."[49] In limited cases, it also can target certain data based on content.[50] Carnivore has two modes for collecting data: (1) full mode, in which data packets can be recorded in their entirety, and (2) pen mode, in which recording is limited to addressing information.[51] The FBI has used Carnivore in one or both of these modes at least twenty-five times, including in ten national security cases and six domestic criminal cases in 2000.[52]

### *B. Carnivore's Primary Uses*

The FBI utilizes Carnivore to collect two kinds of data. In pen mode, it collects addressing information under 18 U.S.C. §§ 3121-27,[53] and in full mode, it collects the full content of communications under 18 U.S.C. §§ 2510-22.[54]

#### 1. Pen Mode: Obtaining Addressing Information

The FBI can use Carnivore to obtain the addressing information (sometimes referred to as transactional information) associated with Internet activity. The FBI refers to this as pen mode, in reference to pen registers, which are devices that

---

45. IITRI DRAFT REPORT, *supra* note 18, at ix.

46. *See* Poulsen, *supra* note 6.

47. IITRI DRAFT REPORT, *supra* note 18, at xii; *see also* Poulsen, *supra* note 6.

48. IITRI DRAFT REPORT, *supra* note 18, at xii; *see also* Poulsen, *supra* note 6. The FBI refers to Carnivore, Packeteer, and CoolMiner, collectively, as the "DragonWare suite." *See* IITRI DRAFT REPORT, *supra* note 18, at xii; *see also* Poulsen, *supra* note 6. Unless otherwise indicated, the Author refers to the entire software package as Carnivore, as is the common usage.

49. IITRI DRAFT REPORT, *supra* note 18, at 1-1.

50. *See* IITRI DRAFT REPORT, *supra* note 18, at 1-1.

51. *See* IITRI DRAFT REPORT, *supra* note 18, at 1-1.

52. *See* Associated Press, *Reno Plans Study of FBI's "Carnivore"* (Aug. 10, 2000), *available at* http://www.aclu.org/news/2000/w081000a.html.

53. 18 U.S.C. §§ 3121-27 (1994 & Supp. V 1999).

54. 18 U.S.C. §§ 2510-22 (1994 & Supp. V 1999).

record the numbers dialed from a telephone.[55] The label "pen mode" suggests that the FBI believes that obtaining addressing information is essentially the same as obtaining phone numbers via a pen register. The similarity is apparent—in both situations, law enforcement simply obtains the information necessary to make a communications connection. In pen mode, the FBI can use Carnivore to obtain "the TO and FROM e-mail addresses and the IP addresses of computers involved in File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) sessions."[56]

### 2. Full Mode: Obtaining the Content of Real-Time Communications

In addition to pen mode, Carnivore also has a full mode of operation. When utilizing Carnivore's full mode, the FBI can obtain the actual content of real-time communications.[57] The fact that Carnivore can intercept real-time communications is significant because the nation's legal system provides more protection for real-time electronic communications than it does for stored electronic communications.[58] In full mode, the FBI can "view the content of e-mail messages, HTTP pages, [and] FTP sessions."[59]

### 3. "Grabbing" Extra Information

Contrary to some public opinion and the concern of privacy advocates, Carnivore does not "grab" information other than its intended target information.[60] Carnivore has a filtering system that allows the program to collect information from only its intended target.[61] It does not "read all incoming and outgoing e-mail

---

55. Pen registers record the numbers dialed from a telephone—the outgoing numbers. *See* 18 U.S.C. § 3127(3) (1994 & Supp. V 1999). Pen registers are similar to trap and trace devices, except that trap and trace devices record the "originating" numbers, or incoming numbers, dialed from a telephone to the phone on which the trap and trace device is attached. *See* 18 U.S.C. § 3127(4) (1994 & Supp. V 1999).

56. IITRI DRAFT REPORT, *supra* note 18, at ix.

57. *See* IITRI DRAFT REPORT, *supra* note 18, at 1-1.

58. *See generally* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994). Note also that the Stored Wire and Electronic Communications and Transactional Records Access Act, which governs access to stored communications, provides no suppression remedy for violations of its provisions. *See* 18 U.S.C. §§ 2701-11 (1994 & Supp. V 1999).

59. IITRI DRAFT REPORT, *supra* note 18, at ix.

60. In pen mode, Carnivore does indicate the length of messages; however, it reveals no content of the communications. *See* IITRI DRAFT REPORT, *supra* note 18, at xii.

61. IITRI DRAFT REPORT, *supra* note 18, at xii-xiii.

messages" or "monitor the web-surfing habits and downloading habits of all [an] ISP's customers."[62] It only stores data packets for later analysis "after they are positively linked by the filter settings to a target."[63] In fact, IITRI found that "in order to work effectively, [Carnivore] must reject the majority of packets it monitors."[64] Furthermore, in the few cases where IITRI tests found differences between the targeted data and the output retrieved and reproduced by the Packeteer and CoolMiner programs, these differences were attributable to bugs in the Packeteer and CoolMiner software.[65] Subsequent IITRI examination of the corresponding raw Carnivore data revealed that the targeted data were in fact collected correctly.[66]

### C. *Carnivore's Safeguards Against Misuse*[67]

The FBI plans to use Carnivore in only limited circumstances—"when other implementations (e.g., having an ISP provide the requested data) do not meet the needs of the investigators or the restrictions placed by the court."[68] In these circumstances, "[FBI] agents follow a rigorous, detailed procedure to obtain court orders and surveillance is performed under the supervision of the court issuing the order."[69] Currently, multiple approvals are required before a court order can be requested.[70] In addition, the supervising judge can "independently verify that traffic collected is only what was legally authorized."[71]

In addition to the prerequisite court order and the requirement of supervision, the FBI provides for separation of responsibilities among agents when operating Carnivore. Case agents, whose incentive is to solve or prevent crimes, "establish the need and justification for the surveillance."[72] In order to remove this incentive

---

62. IITRI DRAFT REPORT, *supra* note 18, at xiii.
63. IITRI DRAFT REPORT, *supra* note 18, at xiii.
64. IITRI DRAFT REPORT, *supra* note 18, at xiii.
65. *See* IITRI DRAFT REPORT, *supra* note 18, at xii.
66. *See* IITRI DRAFT REPORT, *supra* note 18, at xii.
67. In addition to the procedural safeguards laid out by the FBI and the structural safeguards within Carnivore, there are judicial safeguards—suppression motions, civil litigation, and potential criminal prosecution of law enforcement agents who violate an individual's rights. *See, e.g.*, 42 U.S.C. § 1983 (1994 & Supp. V 1999) (civil litigation); United States v. Leon, 468 U.S. 897, 898 (1984) (suppression motions); Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) (civil litigation).
68. IITRI DRAFT REPORT, *supra* note 18, at viii.
69. IITRI DRAFT REPORT, *supra* note 18, at viii.
70. *See* IITRI DRAFT REPORT, *supra* note 18, at xii.
71. IITRI DRAFT REPORT, *supra* note 18, at xii.
72. IITRI DRAFT REPORT, *supra* note 18, at viii.

from the collection process and prevent the problem of overzealous investigation by law enforcement agents "engaged in the often competitive enterprise of ferreting out crime,"[73] these case agents do not actually install the necessary equipment and configure it for proper operation.[74] This task is handled by a separate team of "technically trained agents," which installs the equipment and sets the filtering system "to restrict collection to that allowed by the court order."[75] These agents are "motivated by FBI policy and procedures to ensure that collection adheres strictly to court orders and will be admissible in court as evidence."[76] FBI officials also contend that Carnivore "creates an audit trail"[77] that tracks its collection activity; however, IITRI found that these audit functions are less than adequate.[78] Legislation enacted since the IITRI study has remedied the inadequacy of the audit functions by requiring that information intercepted by Carnivore be turned over to the judge who issued the order authorizing the particular usage of Carnivore.[79]

In addition to these procedural limitations, there are structural limitations within Carnivore that prevent misuse. As indicated above, the system utilizes a one-way tap, which "ensures that Carnivore cannot transmit data on the network."[80] Also, the absence of an installed protocol stack prevents Carnivore from processing data packets other than to filter and record them.[81] Thus, "Carnivore can neither alter packets destined for other systems on the network nor initiate any packets."[82]

---

73. Johnson v. United States, 333 U.S. 10, 14 (1948).

74. IITRI DRAFT REPORT, *supra* note 18, at viii.

75. IITRI DRAFT REPORT, *supra* note 18, at viii.

76. IITRI DRAFT REPORT, *supra* note 18, at viii. The Author notes that the incentive to ensure admissible evidence is not likely present in a pen mode situation. The Fourth Amendment's exclusionary rule does not apply to pen register or trap and trace devices as they do not constitute searches under Fourth Amendment jurisprudence. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding that a pen register device does not constitute a search). For a discussion of Fourth Amendment jurisprudence, see *infra* notes 83-133 and accompanying text. Furthermore, the pen register and trap and trace provisions of the Electronic Communications Privacy Act ("ECPA") have no exclusionary remedy to prevent the use of evidence obtained via the unauthorized use of a pen register. *See generally* 18 U.S.C. §§ 3121-27 (1994 & Supp. V 1999).

77. Di Gregory Statement I, *supra* note 7.

78. *See* IITRI DRAFT REPORT, *supra* note 18, at xii.

79. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288-290 (2001) (to be codified in scattered sections of 18, 47, & 50 U.S.C.).

80. IITRI DRAFT REPORT, *supra* note 18, at ix.

81. *See* IITRI DRAFT REPORT, *supra* note 18, at ix.

82. IITRI DRAFT REPORT, *supra* note 18, at ix.

## III. GUIDING LAW AND RELEVANT LEGAL PRINCIPLES

### A. Fourth Amendment Jurisprudence

*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.*[83]

The purpose of the Fourth Amendment is "to preserve our individual privacy while protecting the safety of our citizens."[84] Although the Fourth Amendment protects individual privacy, this protection is not absolute. The text of the Fourth Amendment acknowledges the legitimacy of reasonable searches.[85] Specifically, the Warrant Clause authorizes warrants issued "upon probable cause."[86] The Supreme Court has interpreted the Fourth Amendment such that the Warrant Clause is the controlling clause,[87] and under this interpretation, the Court has stated that searches and seizures are presumed to be unreasonable unless carried out pursuant to a warrant.[88] The Supreme Court's interpretation presents the following question: what is a search (or seizure)? When the actions of law enforcement constitute a search, the Fourth Amendment's protections kick in; however, where law enforcement does not engage in a search, the Fourth Amendment warrant protection is not triggered.[89]

In his concurring opinion in *Katz v. United States*,[90] Justice Harlan outlined the test that has been accepted as the determinant of whether a search has taken place.[91] Justice Harlan's test has both a subjective and an objective component: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[92] This test has come to be known as the *Katz* test or the

---

83. U.S. CONST. amend. IV.

84. Di Gregory Statement I, *supra* note 7.

85. U.S. CONST. amend. IV.

86. U.S. CONST. amend. IV.

87. *See* TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 23-24 (1969).

88. *See* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE 34 (6th ed. 2000).

89. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745-46 (1979) ("[T]he [government action] was not a 'search,' and no warrant was required.").

90. 389 U.S. 347 (1967).

91. *Id.* at 361 (Harlan, J., concurring).

92. *Id.* (Harlan, J., concurring).

"reasonable expectation of privacy"[93] test. Since *Katz*, the Supreme Court has applied this test to numerous situations. In instances that the Court finds that an individual has a reasonable expectation of privacy, law enforcement must obtain a warrant before searching that place. However, where there is no reasonable expectation of privacy, there is no search.[94]

### 1. Pen Registers

The Supreme Court has determined that the use of a pen register device is not a search.[95] In *Smith v. Maryland*,[96] the telephone company, at police request, installed a pen register device in phone company offices and recorded the numbers called by the defendant from his home phone.[97] When the defendant used his telephone, he "voluntarily conveyed numerical information to the [tele]phone company."[98] Because, under *United States v. Miller*,[99] a person has no legitimate expectation of privacy in information he turns over to third parties, the defendant had no expectation of privacy in the numbers he dialed.[100] The Court held that the use of the pen register did not constitute a search;[101] therefore, neither a warrant nor probable cause was required.

### 2. Wiretaps

Early this century, the Supreme Court held that a wiretap was not a search.[102] In *Olmstead v. United States*,[103] Justice Taft wrote for the majority that "one who

---

93. *Id.* (Harlan, J., concurring).

94. *Smith*, 442 U.S. at 745-46 (finding no expectation of privacy and, thus, holding that the government action "was not a 'search'").

95. *Id.* at 742.

96. 442 U.S. 735 (1979).

97. *Id.* at 737.

98. *Id.*

99. 425 U.S. 435 (1976). In *Miller*, the Court found that an individual had no reasonable expectation of privacy in bank records because these records were accessible by another person or party. *See id.* at 442-43.

100. *See Smith*, 442 U.S. at 742.

101. *See id.*

102. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928). Justice Brandeis, dissenting in *Olmstead*, actually foresaw the issues relevant to the modern debate regarding electronic surveillance: "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrence of the home." *Id.* at 474 (Brandeis, J., dissenting).

103. 277 U.S. 438 (1928).

installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside."[104] Justice Taft noted that telephone messages are not papers or effects under the Fourth Amendment and held with regard to the wiretap: "The amendment does not forbid what was done here. There was no searching. There was no seizure."[105]

Some forty years after *Olmstead*, the Supreme Court looked once again at whether wiretapping constituted a search or seizure, and this time, the Court reached a different result.[106] In *Katz*, FBI agents attached a listening device to the outside of a public telephone booth so that they could overhear the defendant's end of his telephone conversations.[107] The agents used the information they obtained to charge the defendant with interstate transferring of wagering information.[108] The Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[109]

### 3. Mail and E-mail[110]

The Supreme Court has long held that letters and sealed packages sent through the mail can be opened and examined only pursuant to a warrant. Justice Field announced this rule in *Ex parte Jackson*,[111] noting that the "constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[112] Although this rule still stands, the Supreme Court has allowed the detention of packages for a reasonable period of time when the packages are of a suspicious character.[113]

While the Supreme Court has had no opportunity to decide whether an individual has a reasonable expectation of privacy in his e-mail transmissions, this issue has been litigated at the appellate level in the United States Court of Appeals

---

104. *Id.* at 466.

105. *Id.* at 464.

106. *See generally* Katz v. United States, 389 U.S. 347 (1967).

107. *See id.* at 348.

108. *Id.*

109. *Id.* at 353.

110. The Supreme Court has not faced the issue whether an individual has a reasonable expectation of privacy in his e-mail transmissions. The seminal e-mail case is *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996).

111. 96 U.S. 727 (1877).

112. *Id.* at 733.

113. *See* United States v. Van Leeuwen, 397 U.S. 249, 253 (1970).

for the Armed Forces.[114] In *United States v. Maxwell*,[115] the FBI obtained a search warrant to search the files of America Online ("AOL") computers while investigating a suspected child pornography ring.[116] The warrant did not authorize the search of the defendant's e-mail files; nevertheless, the FBI seized all file material relating to the defendant, a subscriber to AOL with an e-mail account.[117]

The court found that the key question was whether the defendant had a reasonable expectation of privacy under *Katz*.[118] The court held that the defendant did have a reasonable expectation of privacy in his e-mail transmissions.[119] The court reasoned that the e-mail arrangement was quite analogous to first-class mail, and, like first-class mail, the sender has a reasonable expectation of privacy until the mail is opened by the intended recipient.[120] Once opened, the "destiny of the letter lies in the control of the recipient of the letter, not the sender."[121] The *Maxwell* court also compared e-mail to telephone communications and found that this analogy supported the idea that e-mail should be treated similarly to telephone communications for Fourth Amendment purposes. The court found that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[122] The court did note, however, that e-mail transmissions, once received by another person, are no longer in the control of the transmitter.[123] The *Maxwell* court's treatment of e-mail as analogous to telephone communications lends support to the idea of treating a cyberwiretap (i.e., Carnivore) in the same way as a telephone wiretap for Fourth Amendment purposes.

### 4. Plain View

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement.[124] In *Horton v. California*,[125] the Supreme Court outlined the conditions for search or seizure to fall within the purview of the plain view doctrine.[126] The Court held that the object's incriminating character

---

114. *See Maxwell*, 45 M.J. at 406.
115. 45 M.J. 406 (C.A.A.F. 1996).
116. *See id.* at 411-14.
117. *See id.* at 416.
118. *See id.* at 418.
119. *See id.* at 419.
120. *See id.* at 417.
121. *Id.* at 417.
122. *Id.* at 418.
123. *Id.*
124. *See* Horton v. California, 496 U.S. 128, 129 (1990).
125. 496 U.S. 128 (1990).
126. *See id.* at 136-37.

must be immediately apparent and the officer must have a lawful right of access to the object.[127]

### 5. Exclusionary Rule

The usual remedy for a Fourth Amendment violation is the exclusion of the evidence gathered as a result of that violation.[128] In *Weeks v. United States*,[129] the Supreme Court held that this remedy applied in federal criminal proceedings where the illegal search was conducted by federal officers.[130] The Court declined to extend this rule to the states in *Wolf v. Colorado*;[131] however, the Court later overruled *Wolf* and held that the exclusionary rule applied against the states in *Mapp v. Ohio*.[132] An important issue with regard to the exclusionary rule is that it applies to violations of the Fourth Amendment; consequently, evidence obtained by means other than a search is generally not excluded.[133]

## *B. Statutory Law*

The FBI and the DOJ have claimed that existing statutory provisions, the pen register and trap and trace portion of the Electronic Communications Privacy Act ("ECPA") and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, authorize surveillance conducted via Carnivore's pen and full modes, respectively.[134] Some commentators have questioned this claimed authority;[135] however, such questions about authorization have been rendered moot by legislation enacted in the wake of the September 11, 2001, terrorist attacks on the United States. This legislation, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), explicitly authorizes the electronic surveillance of

---

127. *See id.*

128. *See* SALTZBURG & CAPRA, *supra* note 88, at 444.

129. 232 U.S. 383 (1914).

130. *See id.* at 398.

131. 338 U.S. 25, 33 (1949).

132. 367 U.S. 643, 660 (1961) ("We hold that all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court.").

133. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

134. *See* IITRI DRAFT REPORT, *supra* note 18, at 3-1 to 3-3.

135. *See* Manton M. Grier, Jr., *The Software Formerly Known as "Carnivore": When Does E-Mail Surveillance Encroach Upon a Reasonable Expectation of Privacy?*, 52 S.C. L. REV. 875, 884-86 (2001); *see also* Christian Schultz, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215, 1240-54 (2001).

computer traffic through amendments to ECPA and Title III.[136] Thus, Carnivore should be analyzed in light of the statutory backdrop created by ECPA[137] and Title III.[138] These statutes, as modified by the USA PATRIOT Act, provide a level of protection not required by the Fourth Amendment.[139]

### 1. Pen Register/Trap and Trace Statute—18 U.S.C. §§ 3121-27

Because pen registers do not constitute a search,[140] they do not have to conform to the strictures of Fourth Amendment jurisprudence. Nevertheless, there are some procedural requirements with which law enforcement officials must comply in order to obtain authority to utilize a pen register (or trap and trace) device.[141]

In order to obtain a pen register court order, a law enforcement officer must certify "to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[142] The pen register order must specify:

> (A) the identity, if known, of the person to whom is leased . . . the telephone line to which the pen register . . . is attached; (B) the identity, if known, of the person who is the subject of the criminal investigation; (C) the number and, if known, physical location of the telephone line to which the pen register . . . is to be attached . . . ; and (D) a statement of the offense to which the information likely to be obtained by the pen register . . . relates.[143]

### 2. Title III—18 U.S.C. §§ 2510-22

Title III "places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires."[144] The

---

136. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified in scattered sections of 18, 47, & 50 U.S.C.).

137. 18 U.S.C. §§ 3121-27 (1994 & Supp. V 1999).

138. 18 U.S.C. §§ 2510-22 (1994 & Supp. V 1999).

139. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979); *see also supra* notes 83-133 and accompanying text.

140. *See Smith*, 442 U.S. at 746; *see also supra* notes 95-101 and accompanying text.

141. *See* 18 U.S.C. §§ 3121-27 (1994 & Supp. V 1999).

142. 18 U.S.C. § 3123 (1994).

143. 18 U.S.C. § 3123(b)(1) (1994).

144. Di Gregory Statement I, *supra* note 7.

Fourth Amendment requires a warrant for a wiretap.[145] In addition, Title III requires law enforcement officers to obtain a court order to wiretap communications in the absence of a statutory exception.[146] To obtain such an order, "the government must show that normal investigative techniques for obtaining the information have [failed] or are likely to fail or are too dangerous, and that any interruption will be conducted so as to ensure that the intrusion is minimized."[147]

## IV. AN ANALYSIS OF CARNIVORE AS AN INVESTIGATIVE TOOL AGAINST THE BACKDROP OF LAWS DESIGNED TO PROTECT INDIVIDUAL PRIVACY

### *A. Effectiveness as a Law Enforcement Investigative Tool*

As Internet use becomes increasingly prevalent in society, it is imperative that law enforcement agents have an investigative tool that enables them to keep pace with the enterprising criminals who have and will continue to utilize the Internet as a vehicle for crime. IITRI's recent review of Carnivore indicates that Carnivore should be up to the task. Following their independent technical review of Carnivore, IITRI officials concluded that "Carnivore represents technology that can be more effective in protecting privacy and enabling lawful surveillance than can alternatives."[148] Carnivore places the FBI on a level playing field with cybercriminals. Carnivore's pen and full modes of operation afford the FBI the same or similar investigative techniques and procedures as are available to law enforcement in the telephone context.

An important characteristic of Carnivore is that it has the capability to perform its collection operations without posing any substantial risks to the integrity of the ISP on whose system it resides.[149] IITRI concluded, following its review of the program, that "Carnivore introduces no operational or security risks to the ISP network where it is installed."[150]

---

145. *See* Katz v. United States, 389 U.S. 347, 358 (1967).

146. *See* 18 U.S.C. § 2511(2)(a)(ii) (1994).

147. Di Gregory Statement I, *supra* note 7.

148. IITRI DRAFT REPORT, *supra* note 18, at xii.

149. IITRI DRAFT REPORT, *supra* note 18, at xii. This statement is undoubtedly denied by Earthlink. *See supra* notes 14-16 and accompanying text.

150. IITRI DRAFT REPORT, *supra* note 18, at xii.

### B. Compliance with Individual Privacy Law

Privacy groups like EPIC and the ACLU must acknowledge the fact that law enforcement plays a critical role in preserving privacy. Although privacy groups are correct in arguing that Carnivore is an intrusion on individual privacy, they neglect the fact that the Fourth Amendment contemplates reasonable searches and seizures, and even authorizes them under the Warrant Clause.

Case law and statutory law stand for the same principle with regard to pen registers and with regard to wiretaps—pen registers are not a search; wiretaps are a search.[151] In general, Carnivore's pen and full modes appear to comply with the applicable law regarding pen registers and wiretaps, respectively.

In order to obtain source or destination information in real time, the government must obtain a trap and trace or pen register court order authorizing the recording of such information.[152] Thus, the FBI must (and does) obtain a court order in order to operate Carnivore in pen mode.[153] Similarly, the government must comply with the warrant requirement and with Title III in order to utilize a wiretap for surveillance purposes or to search and seize letters and packages in the mail. Therefore, the FBI must do likewise when utilizing Carnivore in its full mode, regardless of whether this full mode is more akin to wiretapping a phone or opening someone's mail.

This analysis still leaves a few questions to be answered. Carnivore does record the length of messages when operating in pen mode. It does so by collecting the number of data bytes transferred in an e-mail message and representing each byte by an "X" in the subject field.[154] Such information has no real analog in the pen register context.[155] However, it is unlikely that "society is prepared to recognize as 'reasonable'"[156] an expectation of privacy in the length of e-mail messages.[157]

Some commentators argue that Carnivore's pen mode should be held to stricter standards than pen registers because "e-mail addressing information is more personal, and thus more revealing than a phone number."[158] However, this argument fails for both practical and legal reasons. In practice, e-mail addressing information is not necessary personal. It is only as personal as the user chooses it to be. On the other hand, telephone numbers generally reveal the location of the

---

151. *See supra* notes 95-109 and accompanying text.

152. *See* 18 U.S.C. §§ 3121-27 (1994 & Supp. V 1999).

153. *See supra* notes 95-109 and accompanying text.

154. IITRI DRAFT REPORT, *supra* note 18, at C-3.

155. The IITRI Draft Report noted that recording such data might present an issue of "overcollection." IITRI DRAFT REPORT, *supra* note 18, at 4-2 to 4-3.

156. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

157. *See* Schultz, *supra* note 135, at 1241-42.

158. Grier, *supra* note 135, at 887.

caller by area code and prefix, without any choice made by the caller. More importantly, in legal analysis, the personal nature of an e-mail address is largely irrelevant to the level of protection it may or may not deserve under the Fourth Amendment. Under *United States v. Miller*,[159] a person has no legitimate expectation privacy in information she turns over to third parties. Thus, the individual who discloses her e-mail address to third parties has no legitimate expectation of privacy in her e-mail address regardless of its personal nature.

Additionally, it is possible to put content-type information in the address fields of an e-mail communication. Some may argue, in light of this fact, that Carnivore's pen mode should be held to the standard of its full mode. However, an FBI agent may have a right to search and seize content-type information in an address field under the plain view doctrine. If the agent has a lawful court order for a Carnivore pen mode collection of data, then that agent may have a lawful right of access to the content-type information.[160] Should the incriminating nature of the information be readily apparent when the agent finds it in his plain view, then the agent is authorized to obtain this information without a warrant.[161]

In addition to complying with the Fourth Amendment jurisprudence and the relevant statutory law, Carnivore is subject to several structural limitations and procedural requirements that limit its potential for misuse. Nevertheless, privacy groups fear the "overzealous" officer or the "rogue"[162] cop "engaged in the often competitive enterprise of ferreting out crime."[163] However, the warrant clause is specifically directed at preventing such behavior.[164] There is also a set of judicial remedies available to address government violations of individual privacy (and to act as a deterrent to such behavior).

## V. CONCLUSION

In light of the relevant jurisprudence and statutory scheme, it seems that the fears of privacy groups are unlikely to materialize. President George W. Bush recognized as much when he signed the USA PATRIOT Act into law on October 26, 2001: "This bill was carefully drafted and considered.... This bill met with an... overwhelming agreement in Congress because it upholds and respects the civil liberties guaranteed by our Constitution."[165] According to IITRI, Carnivore

159. 425 U.S. 325 (1976).

160. *See* Horton v. California, 496 U.S. 128, 136-37 (1990).

161. *Id.*

162. *See* Grier, *supra* note 135, at 890.

163. Johnson v. United States, 333 U.S. 10, 14 (1948).

164. *See id.* at 13-14.

165. President George W. Bush, Remarks at the Signing of the USA PATRIOT Act (Oct. 26, 2001), *available at* 2001 WL 1298919. The USA PATRIOT Act was approved

performs its collection operations fairly efficiently and accurately—"[w]hen Carnivore is used correctly under a Title III order, it provides investigators with no more information than is permitted by a given court order."[165]

Carnivore has the potential to fill a need for law enforcement—the need for a tool that puts law enforcement on a level playing field with cybercriminals. While Carnivore has some administrative deficiencies, it is "evolving to improve its performance [and] enhance its capabilities."[167] If these deficiencies can be improved, Carnivore will allow law enforcement the ability to investigate, apprehend, and prosecute criminals in the cyberworld in the same way that it can do so to perpetrators of traditional crimes.

Carnivore complies with the Supreme Court's current Fourth Amendment jurisprudence. It also complies with the higher standards imposed by the nation's individual privacy statutory scheme. The fact that the statutory scheme has higher standards should be a tip to privacy groups that lobby for tighter controls on Carnivore. If tighter controls are what they want, they should write their representatives in Congress and lobby for stricter statutory provisions, because Carnivore squares with both the ECPA and Title III, as supplemented by the USA PATRIOT Act. There is always the possibility that the Internet Age will continue to evolve in such a way that what "society is prepared to recognize as 'reasonable'"[168] may change and Carnivore may not stand up against future Fourth Amendment jurisprudence. Until then, don't fear Carnivore; it won't devour individual privacy.

---

by an overwhelming margin. In the Senate, ninety-eight of ninety-nine voting Senators supported the bill. *See* Press Release, Federal Document Clearing House, Anti-Terrorism Bill Easily Passes the Senate (Oct. 25, 2001), *available at* 2001 WL 5422733. In addition, the USA PATRIOT Act includes some built-in protection for civil liberties in that it has a sunset provision, which terminates much of the bill on December 31, 2005. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 224, 115 Stat. 272, 295 (2001) (to be codified in scattered sections of 18, 47, & 50 U.S.C.).

166. IITRI DRAFT REPORT, *supra* note 18, at xii.

167. IITRI DRAFT REPORT, *supra* note 18, at vii.

168. *See* Katz v. United States, 389 U.S. 347, 361 (1967).