Notre Dame Law Review

Volume 76 | Issue 4 Article 4

6-1-2001

Unrestricted Federal Agent: Carnivore and the Need to Revise the Pen Register Statute

David Hammel Schultz

NOTE

UNRESTRICTED FEDERAL AGENT: "CARNIVORE" AND THE NEED TO REVISE THE PEN REGISTER STATUTE

*Christian David Hammel Schultz**

* Candidate for Juris Doctor, Notre Dame Law School, 2001; M.B.A., Notre Dame Graduate Business School, 2000; B.A. Political Science, B.A. Marketing, Michigan State University, 1995. Many thanks to my family for providing the love, encouragement, and support necessary to achieve my goals. I would like to thank the following people: Assistant Professor Patricia L. Bellia for her insight and encouragement in writing and revising this Note; Professor John Copeland Nagle and Associate Dean Vincent D. Rougeau for their guidance and friendship these past three years; and my colleagues on the Notre Dame Law Review for their dedication, diligence, and friendship. And very special thanks to my wonderful fiancée, Kimberly Bero, for her assistance, patience, and loving support as I worked on this Note. I may be contacted at christian_dh_schultz@hotmail.com.

INTRODUCTION

It is indisputable that the Internet has revolutionized how we exchange information, communicate, educate students, and transact business.[1] In response to this revolution, the United States Government developed the surveillance technologies necessary to keep pace in an ever-changing world where crime unfortunately still takes place. In July 2000, the American public was introduced to one of these new technologies, aptly named "Carnivore,"[2] the latest surveillance tool used by the Federal Bureau of Investigation (FBI) to combat illegal activity on the Internet.

Carnivore is an electronic surveillance system that monitors a targeted user's e-mail, web browsing, and file transfer activity.[3] The

---

1 *See* H.R. REP. No. 106-932, at 4 (2000), *available at* ftp://ftp.loc.gov/pub/thomas/cp106/hr932.txt (last visited May 1, 2001). This Congressional Report indicates that Internet use in the United States alone has grown from 65 million users to over 100 million users between 1998 and 1999 and is expected to reach 177 million users by 2003. *See id.* By that time, the worldwide use of the Internet is expected to exceed 500 million users. *Id.* "Business-to-business electronic commerce totaled over $100 billion in 1999 . . . and is expected to grow to over $1 trillion by 2003." *Id.*; *see also The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. 3 (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology) [hereinafter Dempsey Statement], *available at* http://www.cdt.org/testimony/000906dempsey.shtml (last visited May 1, 2001) ("Individuals, civil society, businesses and governments are all rushing to use the Internet.... The Internet has become a necessity in most workplaces and a fixture in most schools and libraries. Soon, it may converge with the television and wireless phones, and thereby become nearly ubiquitous.").

2 *See* John Schwartz, *FBI's Internet Wiretaps Raise Privacy Concerns*, WALL ST. J., July 12, 2000, at A1 ("The new computer system [is] dubbed 'Carnivore' inside the FBI because it rapidly finds 'meat' in vast amounts of data...."); *see also Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the House Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 1 (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation) [hereinafter July Statement of Donald M. Kerr], *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm (last visited May 1, 2001) (discussing Carnivore's public introduction with Congress). In February 2001, the FBI announced that the name for the system previously called "Carnivore" would be changed to "DCS1000, which stands for Digital Collection System, Version 1." Jeff Fick, *FBI's Carnivore Gets New Name*, USA TODAY, Feb. 12, 2001, at B3. For the purposes of this Note, the name Carnivore will be used to refer to the Carnivore/DCS1000 system.

3 *See* ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM—FINAL REPORT, at viii (2000) [hereinafter IITRI REPORT], *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf (last visited May 1, 2001); FEDERAL BUREAU OF INVESTIGATION, FBI PROGRAMS AND INITIATIVES–CARNIVORE DIAGNOSTIC TOOL 1–3 [hereinafter CARNIVORE DIAGNOSTIC TOOL], *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited May 1, 2001).

system is capable of gathering identification information associated with these activities at two levels. First, in "full collection" mode, Carnivore intercepts the addressing information and content of a targeted user's electronic communication.[4] The Department of Justice (DOJ) and the FBI assert that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)[5] and the Foreign Intelligence Surveillance Act of 1978 (FISA)[6] provide the legal authority for Carnivore's full mode surveillance.[7] Second, in "pen collection" mode, Carnivore primarily gathers only the addressing information associated with e-mail, web browsing, and file transfer activity.[8] The DOJ and FBI argue that the "pen register" provisions of the Electronic Communications Privacy Act of 1986 (ECPA) provide the legal authority for Carnivore's pen mode surveillance.[9]

The use of Carnivore in pen mode has been challenged in Congressional hearings, due to apparent inconsistencies between Carnivore's pen mode collections and the types of information that may be collected under pen register authority.[10] The DOJ and FBI, however,

4 *See* IITRI REPORT, *supra* note 3, at viii, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

5 18 U.S.C. §§ 2510–2522 (1994 & Supp. 1998).

6 50 U.S.C. §§ 1801–1863 (1994 & Supp. 1998).

7 *See* July Statement of Donald M. Kerr, *supra* note 2, at 2, *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm. The DOJ and FBI do not rely on FISA for pen mode surveillance, though a pen register or trap and trace device may be deployed pursuant to FISA authority. *See* 50 U.S.C. §§ 1842–1845 (Supp. 1998). This issue will be discussed in Part II.B.2, Part III.B, and Parts IV.A and D.

8 *See* IITRI REPORT, *supra* note 3, at ix, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

9 *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. 3 (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation) [hereinafter September Statement of Donald M. Kerr], *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm (last visited May 1, 2001); *see also* DEPARTMENT OF JUSTICE COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 80–81 (2001), *available at* http://www.cybercrime.gov/searchmanual.htm (last updated Jan. 10, 2001) (discussing how pen registers and trap and trace devices operate in traditional deployments and explaining why "[in] Internet cases . . . the distinction is less important"). The pen register section of ECPA is codified at 18 U.S.C. §§ 3121–3127 (1994 & Supp. 1998). The IITRI report explains pen register authority, but then discusses judicial oversight, Carnivore's deployment, penalties, and exclusionary recourse only in terms of Title III and FISA. *See* IITRI REPORT, *supra* note 3, at 3-1 to 3-8, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

10 *See* Dempsey Statement, *supra* note 1, at 3, 7, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; *Fourth Amendment Issues Raised by the FBI's "Carni-*

do not detail how the pen register statute governs Carnivore's pen mode surveillance activities. This Note limits its scope to the technical and legal aspects of Carnivore's pen mode operations and concludes that there is no constitutional impediment to law enforcement officials deploying Carnivore in pen mode. In addition, contrary to DOJ and FBI assertions, it determines that the pen register section of ECPA does not control Carnivore's pen mode surveillance. This Note asserts, however, that Carnivore should be used for pure pen mode surveillance only pursuant to pen register authority and proposes the necessary revisions to the pen register statute to provide for such authority.

This Note proceeds as follows: Part I provides a brief overview of the Internet infrastructure, the need for Carnivore, and Carnivore's pen mode surveillance capabilities. Part II reviews the legal environment. First, it presents the reasonable expectation of privacy test used to determine whether government actions implicate the Fourth Amendment. Second, it introduces the relevant statutory scheme under which Carnivore is deployed for full and pen mode surveillance. Part III examines Carnivore's pen mode surveillance against this legal background. First, it determines that Carnivore's pen mode

---

vore" Program: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong. 7–13 (2000) (statement of Robert Corn-Revere, Partner at Hogan & Hartson L.L.P., specializing in First Amendment, Internet, and communications-related issues) [hereinafter Corn-Revere Statement], *available at* http://www.house.gov/judiciary/corn0724.htm (last visited May 1, 2001); *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 3–5 (2000) (statement of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology) [hereinafter Davidson Statement], *available at* http://www.house.gov/judiciary/davi0724.htm (last visited May 1, 2001); *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 7–13 (2000) (statement of Barry Steinhardt, Associate Director, American Civil Liberties Union) [hereinafter Steinhardt Statement], *available at* http://www.house.gov/judiciary/stei0724.htm (last visited May 1, 2001); *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. 2–3 (2000) (statement of Michael O'Neill) [hereinafter O'Neill Statement], *available at* http://www.senate.gov/~judiciary/962000_mo.htm (last visited May 1, 2001); *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. 2–3 (2000) (statement of Jeffrey Rosen, Associate Professor, George Washington University Law School) [hereinafter Rosen Statement], *available at* http://www.senate.gov/~judiciary/962000_jr.htm (last visited May 1, 2001). The House Judiciary Committee recently acknowledged that "the authority for [the use of pen registers to obtain e-mail addresses sent and received] is not without doubt." H.R. REP. No. 106-932, at n.10 (2000), *available at* ftp://ftp.loc.gov/pub/thomas/cp106/hr932.txt (last visited May 1, 2001).

capabilities do not infringe on a reasonable expectation of privacy and thus neither implicate nor violate the Fourth Amendment. Second, it determines that such capabilities are not governed by the requirements and prohibitions of the pen register section of ECPA. Part III proposes revisions to the statute that both encompass the use of Carnivore for pen mode surveillance and allow for developments in communications and surveillance technologies. This Note concludes with a call for Congressional review of the pen register statute and enactment of the recommendations contained in this Note.

I. THE INTERNET AND CARNIVORE

A. *The Internet Infrastructure*

What computer users around the world identify as the "Internet" evolved from the United States Department of Defense's information sharing system called the Advanced Research Project Agency Network (ARPANET).[11] The modern Internet, much like the original ARPANET, is "a network of computers that are connected so they can exchange information amongst each other."[12] Today's computer users rely on the Internet to facilitate different forms of communication and information exchange including e-mail,[13] web browsing, and file transfer activity.[14]

---

11 *See* Robert S. Steere, Note, *Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 246, 246–47 n.89 (1998) (citing ACLU v. Reno, 929 F. Supp. 2d 824, 831 (E.D. Pa. 1996)).

12 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, 190 (2000); *see also* Steere, *supra* note 11, at 246–47 n.89. Mssrs. Sinrod and Reilly provide an excellent summary of how the Internet is structured and how it operates. Their article was particularly helpful for this Section of this Note.

13 E-mail is "a system that lets people send and receive messages with their computers. The [e-mail] system might be over a company's own intraoffice [sic] network or over an external network such as [the] Internet." MICHAEL D. SCOTT, INTERNET & TECHNOLOGY LAW DESK REFERENCE 424 (1995). The typical e-mail message contains the sender and recipient e-mail addresses (for example, TO: student@nd.edu, FROM: professor@nd.edu), a subject header, the date, and the message content. *See* JERRY LAWSON, THE COMPLETE INTERNET HANDBOOK FOR LAWYERS 29–30 (1999). E-mail messages also may include attached files that can be opened by the recipient. *See id.* at 37–38.

14 Web browsing and file transfer activity both entail seeking and obtaining communication and content on the Internet via a web browser like Netscape Navigator or Internet Explorer. *See* SCOTT, *supra* note 13, at 536. Web browsers locate documents using an address called a "Uniform Resource Locator" (URL) and display documents in "hypertext markup language" (HTML). *Id.* at 536–37. The URL is "different than an e-mail address . . . . [It] is a reference to a particular file." *Id.* at 521. URLs

For an exchange of information between two computers, one computer, the "client," requests information from another computer, the "server."[15] This communication process is facilitated by the Transmission Control Protocol (TCP) and the Internet Protocol (IP), collectively the TCP/IP.[16] When the server receives a request for a file from the client, it "locates the file on its computer and breaks the file into tiny pieces . . . [and wraps these pieces] in a bundle of instructions that tells [them] where to go . . . called 'packets.'"[17]

> The TCP assigns a sequence number . . . so it can track what it has sent and eliminate the need to duplicate sending the same packet twice unless the packet is lost somewhere along the line to the client. The "packet header," contains the sequence numbers that also tells the client the next sequence number to expect after each packet, so the client can start arranging the packets and conduct a rolling inventory.[18]

The Internet Protocol "route[s] the packets across the Internet," between the server and client, and does so using "many other servers to reach its final destination."[19] The IP assigns a numerical address to

---

identify the server on which the information sought is located, and the servers "are linked to the Internet through [ ] common communications protocol[s], known as hypertext transfer protocol ('HTTP') [and File Transfer Protocol ('FTP')]." *Id.* at 536–37. The URL consists of three parts: (1) the protocol (http:// or ftp://), (2) the domain at which the file resides (for example, www.nd.edu), and (3) the specific path to the file (for example, basketball/women/2001nationalchampions.html). *Id.* at 521. "[A]n URL will direct a user to a file with a particular protocol, location, and name on a particular server, but it does not assure a user that the named file at a particular location is the same file that earlier was at the same location [or what the user thinks they are going to find]." *Id.*

15 Sinrod & Reilly, *supra* note 12, at 190.

16 *See id.* at 191. E-mail is typically transferred between computers via the Internet using a subset of the TCP/IP family of protocols, the Simple Mail Transfer Protocol (SMTP). *See* Steere, *supra* note 11, at 247 & n.93.

17 Sinrod & Reilly, *supra* note 12, at 191. "A 'packet' is a brief computer message of perhaps a few thousand bits (up to a thousand or so characters) containing some indication of the source of the message and the destination in addition to the content." *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. 2 (2000) (statement of Dr. Vinton G. Cerf, Internet Trustee, The Internet Society), *available at* http://www.senate.gov/~judiciary/962000_vgc.htm (last visited May 1, 2001). Dr. Cerf compares Internet packet-switch communication to sending a book through the mail but doing so using post cards, with the cards numbered for re-ordering and for informing the sender of missing cards. *See id.* at 2–3.

18 Sinrod & Reilly, *supra* note 12, at 191.

19 *Id.* Mssrs. Sinrod and Reilly analogize IP addresses to zip codes.

> Each computer on the Internet has an IP address that tells [other] computers where [it] is located. The IP address is very similar to a zip code. For

every packet before they are sent, "hoping the packet arrives where it is supposed to go. If the server does not receive a response that the packet was received [by the client], the IP can send an error message to the client . . . letting the client know that the packet did not get there."[20] This process continues until the server receives a response from the client for every packet that the server has sent. While this may seem time consuming, the process actually takes only a very small fraction of a second and is virtually seamless to the user.[21]

B. The Need for Carnivore

According to the FBI, "The Nation's communications networks are routinely used in the commission of serious criminal activities."[22] The FBI intends to use Carnivore to combat the various criminal acts that occur via the Internet and "threaten the security of our Nation and the safety of our people."[23] The FBI asserts that it needs Carnivore, because existing technologies—whether available to the FBI or owned and operated by an Internet Service Provider (ISP)—are incapable of satisfying the limitations on information interceptions imposed by existing federal law.[24] In some situations, particularly

---

example, a zip code that begins with a 9, belongs to an address located on the west coast of the United States. If the next number is a 4, the location is in the San Francisco area, and so on until the precise region is located. However, to parallel the IP addresses, each house in the zip code area would be assigned a number, instead of an address.

Id.

20 *Id.*

21 *See* Steere, *supra* note 11, at 247 n.93 (making this assertion regarding e-mail).

22 CARNIVORE DIAGNOSTIC TOOL, *supra* note 3, at 1, *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm. "In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims." *Id.*

23 September Statement of Donald M. Kerr, *supra* note 9, at 1, *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm. The FBI lists terrorism, espionage, information warfare, hacking, child pornography and sexual exploitation of children, fraud, and other serious and violent crimes as the acts that "threaten the security of our Nation and the safety of our people" and justify the deployment of Carnivore. *See id.* at 1–3.

24 *Id.* at 4 (stating that commercial tools that are similar to Carnivore worked "as well as could be expected . . . [but] had never been designed as a law enforcement electronic surveillance tool, and hence had shortcomings"); *see also* CARNIVORE DIAGNOSTIC TOOL, *supra* note 3, at 2. "[T]he complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than older analog communications." July Statement of Donald M. Kerr, *supra* note 2, at 4, *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm.

"where more stringent legal, evidentiary, and law enforcement requirements exist," the FBI asserts that commercially-available tools "collect either too much information . . . or, alternatively, fail to collect the authorized information at all."[25] The Government maintains that Carnivore will be installed only when the FBI and an ISP have determined that the ISP's system is incapable of properly complying with the court order.[26]

C. The Carnivore System

In response to privacy concerns about the use of Carnivore,[27] the DOJ asked the Illinois Institute of Technology Research Institute (IITRI) to conduct an independent review of the system. That review culminated in the December 2000 release of a report on Carnivore's technical capabilities.[28] Almost concurrently, pursuant to Freedom of Information Act (FOIA) requests and a subsequent court order, the DOJ and the FBI released the first installment of documents relating to the Carnivore system.[29] These materials will serve as the primary basis for understanding exactly what the Carnivore system is, what it is expected to do, and what it actually accomplishes.[30]

---

25 September Statement of Donald M. Kerr, *supra* note 9, at 7–8, *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm.

26 *See id.* at 6.

27 *See* Corn-Revere Statement, *supra* note 10, at 8, *available at* http://www.house.gov/judiciary/corn0724.htm; Davidson Statement, *supra* note 10, at 3–7, *available at* http://www.house.gov/judiciary/davi0724.htm; Dempsey Statement, *supra* note 1, at 6, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; Steinhardt Statement, *supra* note 10, at 1–5, 7–9, *available at* http://www.house.gov/judiciary/stei0724.htm.

28 *See* IITRI REPORT, *supra* note 3, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

29 *See* www.epic.org/privacy/carnivore/foia_documents.html (last visited May 1, 2001).

30 The FBI documents released by the DOJ and the FBI pursuant to the FOIA request are merely the first two installments (roughly 400 pages) of the nearly 3000 pages the government maintains on the Carnivore system. *See id.* The FBI plans additional releases every forty-five days until all 3000 documents have been released, however, for security purposes the government has redacted significant portions of the released documents and presently is editing the to-be-released documents for future release. *See* Press Release, Electronic Privacy Information Center (EPIC), *FBI Releases Carnivore Documents to EPIC Privacy Group Says Disclosure Insufficient* (Oct. 2, 2000), *available at* http://www.epic.org/privacy/carnivore/foia_pr.html (last visited May 1, 2001). As of April 2001, EPIC has not posted a third installment of FOIA documents, assuming the DOJ and FBI have released such documents.

1. The Carnivore Architecture

According to the IITRI report, "Carnivore is a software-based tool used to examine all Internet Protocol (IP) packets on an Ethernet[31] and record only those packets or packet segments that meet very specific requirements."[32] The Carnivore system architecture is comprised of:

> (1) a one-way tap into an Ethernet data [stream];[33] (2) a general purpose computer to filter and collect data [i.e., the collection computer];[34] (3) one or more additional general purpose computers to control the collection and examine the data [i.e., the remote computer(s)]; (4) a [Carnivore-dedicated] telephone link to con-

31 Ethernet is a kind of network "that is fast and cheap but limited to a total distance of less than a mile." JOHN R. LEVINE & CAROL BAROUDI, THE INTERNET FOR DUMMIES 25 (2d ed. 1994). "[A] computer is connected to the Ethernet by a . . . cable known as a *drop* cable . . . ." *Id.* It is "[a] wire that looks much like a phone wire with the familiar phone jack . . . [that] plugs into the back of your computer." *Id.* at 27. A modem, on the other hand, "enables data from one computer to travel to another computer by using ordinary telephone lines." *Id.* at 17; *see also* ALLEN C. BENSON, THE COMPLETE INTERNET COMPANION FOR LIBRARIANS 33–46 (1995) (comparing dial-up Internet connections to direct communications); JOHN BURKE, LEARNING THE INTERNET 4 (1996) (comparing directly-connected Internet activity to dial-up connections via modem); LAWSON, *supra* note 13, at 426, 429–30 (defining Ethernet, local area networks, and modems); SCOTT, *supra* note 13, at 184, 302, 325–26 (same).

32 IITRI REPORT, *supra* note 3, at vii, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

33 In a typical Carnivore installation,

> an existing Ethernet data line is disconnected from an Ethernet hub or switch and plugged into the tap. A new line is run from port B [of the tap] to the hub/switch. The tap passes the traffic along [these lines] as if it were a standard cable . . . [while taking] a copy of the . . . data in each direction and feed[ing] it . . . [into Carnivore via a second hub].

Id. at 3-10 to 3-11. The cabling process and the types of cables used ensure that "Carnivore is in a receive-only mode. The transmission lines from the Ethernet adapter are not connected to anything inside the tap." *Id.* at 3-11.

34 "Carnivore employs a generic Pentium-class PC, with a generic 10/100 Mbps Ethernet adapter . . . [and a] removable Jaz disk." *Id.* at 3-11 to 3-12. The collection computer is installed without a keyboard or monitor and is normally controlled remotely. *See id.* at 3-12. "A case agent controlling the Carnivore collection computer from an external computer . . . can . . . start[ ] or stop[ ] collection and download[ ] collected data. An additional password is required to access the advanced setup features and change the filter settings." *Id.* at 3-13. During deployments, the Carnivore collection computer "might not be physically accessible to case agents." *Id.* at 3-12.

nect the [remote] computer(s) to the collection computer;[35] and (5) Carnivore software.[36]

FBI technicians work with ISP personnel to connect the collection computer on the smallest subset of the ISP's network that ensures monitoring and interception of all of the targeted user's communications, in accordance with the court order authorizing the surveillance, while minimizing exposure to other users' communication.[37]

2. The Software Program and Filtering Process

Carnivore is actually the name of the collection software program that filters and records IP packets.[38] The Carnivore software is one component of the "Dragonware Suite," which includes the commercially-available Packeteer and CoolMiner software that reconstruct e-mail and other Internet traffic from the collected packets.[39] Packeteer reconstructs the TCP session from the collected IP packets and creates files that can be viewed using CoolMiner.[40] The FBI case agent conducting the surveillance can use CoolMiner to selectively view certain types of packets; "[t]he agent first might want to look at the HTTP [web browsing] traffic and then later look at the e-mail traffic. By using CoolMiner, the agent doesn't have to look at everything at one time."[41]

Once the Carnivore software is installed on the collection computer, the case agent dials into the system from a remote computer to instruct the collection computer to start and stop collection, cause the collection to start recording to a new file, download the collected data, and change filter preferences.[42] Depending on what the court order authorizes, Carnivore can be programmed to conduct several different types of filtering. "The simplest form of collection is one

35 The telephone line is an analog voice line that is "installed especially for the Carnivore deployment. It does not use one of the modems from the ISP's modem pool, nor is it controllable via the Internet." *Id.* at 3-12. "[E]ach Carnivore [collection] computer is equipped with an off-the-shelf 56-kbps modem allowing it to communicate [with a remote computer] via a standard analog telephone link." *Id.* "[T]he telephone line is protected by an electronic key; only a remote computer with a matching key can connect to [the collection computer]." *Id.*

36 *Id.* at 3-10.

37 *See id.* at 3-9 to 3-10.

38 *See id.* at 3-13.

39 *See id.* at 3-17.

40 *See id.* at 3-17 to 3-18.

41 *Id.* at 3-18.

42 *See id.* at 3-12. Filter preferences are changed on an advanced screen, access to which requires an additional password. *Id.* at 3-13.

based on [the targeted user's] fixed IP address."[43] When the targeted user's computer does not have a fixed IP address, "Carnivore supports the collection of dynamically-allocated IP addresses . . . ."[44] Carnivore can also filter based on the targeted user's e-mail address[45] or exchange protocol—the latter is only used in conjunction with other filters.[46] When operating in full collection mode only, Carnivore can also intercept communication based on specific text strings.[47]

---

43 *Id.* at 3-14.

44 *Id.* at 3-15. Dynamically-allocated IP addresses are addresses that are assigned as the targeted user logs on to the ISP network's Ethernet with a laptop computer—the IP address assigned to the targeted user's computer may change each time the user connects to the network. *See id.* To monitor and record dynamically-assigned IP addresses, the government agent must know the access control address of the machine, the user name, and a range of IP addresses from which the IP address may be dynamically assigned. *See id.*

45 *Id.* at 3-16. "Carnivore can filter [e-mail] traffic based upon the e-mail address. The proper mode must be selected and the e-mail address to be monitored must be entered. If [e-mail] ports are selected and no e-mail address is input, Carnivore collects all packets for those ports." *Id.*; *see also id.* at 3-15, fig. 3-3 (Carnivore Advanced Menu).

46 *See id.* at 3-15. For protocol filtering, Carnivore "can be set to full, pen, or none [the default setting] . . . . If [the default setting] is selected, no packets for that protocol are collected." *Id.* at 3-15 to 3-16. These ports for protocol filtering include, but are not limited to, 110 (POP3, e-mail), 20 (file transfer data), 21 (file transfer control), 25 (SMTP, e-mail), and 80 (HTTP, web browsing). *See id.* at 3-15, fig. 3-3 (Carnivore Advanced Menu). In pen mode, Carnivore "only collects address information appropriate for the protocol (for example, FROM and TO fields of SMTP e-mail or IP address for FTP [file transfer] and HTTP [web browsing] traffic)." *Id.* at 3-15. No packets are collected if Carnivore cannot detect address-only information. *Id.* "Carnivore [also] collects the packets associated with the content of the collected communications, but replaces the actual data with Xs." *Id.* From this information, CoolMiner can "report byte counts for the . . . sessions, even for pen mode collections . . . . [T]he byte counts for the various fields of a protocol (such as Subject) can [also] be determined." *Id.* at 3-15 to 3-16.

47 *Id.* at 3-16. "For example, a setting could be made to collect all TCP packets from a specific IP address that contains [a particular text string]. There is also an option to collect the entire TCP transmission for any packet that contains the given text string." *Id.* "Text filtering capability allows the FBI to capture web-based e-mail such as Hotmail. For example, Carnivore can be set to filter HTTP packets looking for the string '&login=username' where username represents the target of the court order." *Id.* Because text filtering occurs only in full collect mode and thus only occurs pursuant to a Title III or FISA order, it will not be examined in the remainder of this Note. Nonetheless, it seems prudent to provide some information about this capability for informational purposes.

3. Laboratory Tests

In order to fully consider Carnivore's capabilities, IITRI was asked to conduct laboratory test cases of Carnivore in operation.[48] IITRI conducted thirteen separate tests; five tested Carnivore in typical collection cases, while eight tested Carnivore's general capabilities.[49] However, only three of the test cases involved pen mode surveillance.[50] Because this Note only examines Carnivore's pen mode surveillance, the following summary of the test cases will be limited to those wherein Carnivore was set for pen mode collection. These test cases provide insight into precisely what information Carnivore gathers when operating in pen mode—an issue relevant to the analysis of the constitutional and statutory questions addressed in Part III.

a. Non-content E-mail Collection

The test of non-content e-mail collection envisions a scenario where "[a] court order authorizes collecting the noncontent [sic] header fields on e-mail messages sent to and from the target; it [would] not permit collecting the SUBJECT header or the body [content] of the e-mail traffic."[51] IITRI conducted this test to "[v]erify that Carnivore . . . collect[s] [only] the e-mail addresses that were sent from and to a target, and does not collect any of the target's e-mail subject and content."[52] This test showed that Carnivore did not collect any information other than TO and FROM addressing information of the targeted user's e-mail activity, but in some trials failed to

48 The tests are as follows: (1) Non-content E-mail Collection, (2) Non-content Web Browsing Collection, (3) Non-content File Transfer Activity Collection; (4) Full Collection on a Fixed IP Address, (5) E-mail Content Collecuon, (6) Alias E-mail Collection, (7) Filtering Text String on Web Activity Collection, (8) Power Failure and Restoration, (9) Full Mode Collection for All TCP Ports, (10) Collect from a DHCP Assigned IP Address, (11) Filtering on Text String for E-mail Collection, (12) Filtering on Text String and E-mail Address or E-mail UserID for E-mail Collection, (13) Filtering on Text String for FTP Collection. *See id.* at 3-23 to 3-28, C-1 to C-32.

49 *See id.* at 3-23. The three tests of pen mode surveillance are (1) Non-content E-mail Collection, (2) Non-content Web Browsing Collection, (3) Non-content File Transfer Activity Collection. *See id.* at 3-24 to 3-25, C-1 to C-9; *infra* Part I.3.a–c.

50 Tests 1 to 3 are the pen mode tests, while tests 4 to 13 are full collection mode. *See id.* at 3-23 to 3-28.

51 *Id.* at C-1.

52 *Id.* at 3-24. This test should "verify that Carnivore does collect and preserve all of the information authorized by the court order and that no other system user's communication can be collected." *Id.* at C-1.

collect even this information.[53] However, IITRI noted that when operating in pen mode, "Carnivore replaces e-mail header information with Xs. When this data is viewed in CoolMiner it is easy to determine the length of each field in the header and the length of the entire message."[54] Thus, although the IITRI test verified that, when operating in pen mode, Carnivore does not collect any content or header information, it may reveal the size of the header and message.

b. Non-content Web Browsing Collection

The test of non-content web browsing collection envisions a scenario where "[a] court authorizes collecting source and destination information for HTTP [web browsing] activities by [the targeted user]."[55] Specifically, the order would authorize collecting the IP address of the server from which the targeted user seeks to retrieve information. The order would not authorize collecting the full Uniform Resource Locator (URL) generated by the user's browsing activity, which may have specific search terms or other information embedded in it.[56] The purpose of this test is "[t]o verify that Carnivore collects and preserves all of the target's HTTP connection information authorized by the court order, only that information, and not other users' web browsing source and destination information or content."[57]

53 *Id.* at 3-24. IITRI noted that Carnivore "[c]annot effectively collect POP3 e-mail messages in pen mode. It has insufficient capacity to separate allowed versus forbidden information from the messages. It, therefore, collects nothing . . . ." *Id.* at 4-8.

54 *Id.* at C-3.

55 *Id.* at C-4.

56 *See id.* Web browsers locate documents using an address called a "Uniform Resource Locator" (URL). *See* SCOTT, *supra* note 13, at 536–37. The URL is "a reference to a particular file." *Id.* at 521. URLs identify the server on which the information sought is located and consist of three parts: (1) the protocol (http:// or ftp://), (2) the domain at which the file resides (for example, www.nd.edu), and (3) the specific path to the file (for example, basketball/women/2001nationalchampions.html). *Id.* The full URL may have privacy components the interception of which would require greater authority than the pen register statute could provide. For illustrations of this concern, see Davidson Statement, *supra* note 10, at 5–6, *available at* http://www.house.gov/judiciary/davi0724.htm; Dempsey Statement, *supra* note 1, at 6–8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; Steinhardt Statement, *supra* note 10, at 7–8, *available at* http://www.house.gov/judiciary/stei0724.htm.

57 IITRI REPORT, *supra* note 3, at C-4, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf. This test should "[v]erify that Carnivore does collect the target's HTTP web browsing activity source and destination IP address, does not collect the URL [or] content of the target's web activities, and does not collect other users' communication." *Id.* at 3-24.

This test indicated that Carnivore only collected the source and destination IP addressing information of the targeted user's web browsing activity.[58] Like the non-content e-mail collection test discussed above, however, "[t]he CoolMiner analysis results . . . provide information on how many bytes are transferred between the client and the server [and that] data sizes can also be counted from the Carnivore raw data."[59]

c. Non-content File Transfer Activity Collection

The test of non-content file transfer activity collection envisions a scenario where "[a] court order authorizes collecting source and destination information for FTP [file transfer protocol] activity by [a targeted user]. Specifically, the order [would authorize] collecting the IP address to which [the targeted user] opens an FTP connection."[60] The purpose of this test is "[t]o verify that Carnivore collects and preserves all of the target's inbound and outbound FTP traffic . . . information authorized by the court order, only that information, and not other users' FTP source and destination information or content."[61] This test showed that Carnivore intercepted and recorded "only the connections of FTP activities from and to the target . . . ."[62] In other words, it only collected the source and destination IP addresses associated with the targeted user's file transfer activity. However, as in the previous two test cases, "[t]he CoolMiner analysis . . . [indicates] how many bytes are transferred between the client and the server."[63]

58 *See id.* at C-5. Carnivore intercepted and recorded "only the activities of web browsing performed from the target's . . . computer . . . . [N]one of the web browsing content or URL were collected; only the client and server HTTP connection information was collected." *Id.*

59 *Id.* IITRI noted that "[r]ecording this information might be an issue of over-collecting because the court order only authorizes collecting the IP addresses of web activity, but none of the information on data size can be collected." *Id.*

60 *Id.* at C-7.

61 *Id.* This test should "[v]erify that Carnivore does collect the target's file downloading activity source and destination IP address and does not collect the file content and other users' FTP activities." *Id.* at 3-24.

62 *Id.* at C-8.

63 *Id.* IITRI noted that "[r]ecording this information might be an issue of over-collecting because the court order only authorizes collecting the IP addresses of source and destination, but none of the information on message size can be collected." *Id.* at C-9.

II. THE LEGAL ENVIRONMENT

As noted above, the DOJ and the FBI claim that the pen register section of ECPA provides the authority for law enforcement officials to gather information through Carnivore's pen mode surveillance. A pen register order, however, is not the equivalent of the warrant the Fourth Amendment requires when law enforcement officials conduct a search or seizure. The use of Carnivore in pen collection mode, therefore, raises two legal issues: first, whether the collection of certain information in the absence of a full court-approved warrant violates the Fourth Amendment; and second, whether the pen register statute provides the authority to operate Carnivore in pen mode. This Part provides the background necessary to understand the legal implications of Carnivore's pen mode surveillance discussed in Part III.

A. The Fourth Amendment Expectation of Privacy Test

The Fourth Amendment protects against unreasonable searches and seizures.[64] The text indicates that the law specifically protects persons, houses, papers, and effects,[65] and it requires the government to obtain a warrant before conducting a search or seizure.[66] To implicate the Fourth Amendment, however, government activity must rise to the level of either a search or a seizure,[67] which means that it must invade a person's reasonable expectation of privacy.[68] To constitute such an invasion, government action must infringe on an individual's actual or subjective expectation of privacy that is also "one that society is prepared to recognize as 'reasonable.'"[69]

---

64 *See* JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES 82 (1999); STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE 36 (1996).

65 The full text of the Fourth Amendment reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

66 *See* DRESSLER & THOMAS, *supra* note 64, at 82; SALTZBURG & CAPRA, *supra* note 64, at 36.

67 *See* SALTZBURG & CAPRA, *supra* note 64, at 36.

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

69 Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). The Court stated that this was similar to inquiring "whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is 'justifiable' under the circumstances." *Id.* (quoting *Katz*, 389 U.S. at 353).

The Supreme Court first applied this Fourth Amendment expectation of privacy test to pen registers in *Smith v. Maryland*.[70] In *Smith*, a telephone company installed a pen register, at police request, to "record the numbers dialed from the telephone at [Michael Lee Smith's] home."[71] Smith argued that use of the pen register violated the Fourth Amendment because the police failed to obtain a warrant or court order prior to having the pen register installed.[72] In response to this claim, the Court stated that "pen registers do not acquire the *contents* of communications . . . '[and] a law enforcement officer could not even determine from the use of a pen register whether a communication existed.'"[73] The Court doubted that telephone users "entertain any actual expectation of privacy in the numbers they dial," because they transmit these numbers to the telephone company to complete calls and realize that phone companies use technology, including pen registers, for billing purposes.[74] Furthermore, "even if [Smith] did harbor some subjective expectation [of privacy], this expectation is not 'one that society is prepared to recognize as reasonable' . . . [because] a person has no legitimate expectation of

---

70 442 U.S. 735 (1979). The Supreme Court's previous pen register decision, *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), addressed whether Rule 41(b) of the Federal Rules of Criminal Procedure, which authorizes the issuance of a warrant to search for and seize specified types of property, was sufficiently broad to include as a seizure the telephone dial impulses recorded by pen registers. *See id.* at 160.

71 *Smith*, 442 U.S. at 737. In *Smith*, the Supreme Court defined a pen register as "'a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.'" *Id.* at 736 n.1 (quoting *N.Y. Tel. Co.*, 434 U.S. at 161 n.1 (holding that Rule 41(b) of the Federal Rules of Criminal Procedure is sufficiently broad to include pen register recordings as seizable property)). In 1986, Congress enacted the pen register section of ECPA, 18 U.S.C. §§ 3121–3127 (1994 & Supp. 1998), which defines a pen register under existing law. *See id.* § 3127(3). This statute does not, however, alter the importance of *Smith* and its progeny for analyzing the Fourth Amendment implications of the Carnivore system.

72 *See Smith*, 442 U.S. at 737.

73 *Id.* at 741 (quoting *N.Y. Tel. Co.*, 434 U.S. at 167). The Court further stated:

> "These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by the pen register."

Id. (quoting *N.Y. Tel. Co.*, 434 U.S. at 167).

74 *Id.* at 742.

privacy in information he voluntarily turns over to third parties."[75] The Court's holding in *Smith* will be useful when examining the constitutional aspects of Carnivore's pen mode surveillance in Part III.A.

B. The Relevant Statutory Scheme

As indicated, Congress has enacted several statutes addressing surveillance of communication. For purposes of this Note, the relevant statutes are Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),[76] the Foreign Intelligence Surveillance Act of 1978 (FISA),[77] and the pen register section of the Electronic Communications Privacy Act of 1986 (ECPA).[78] The DOJ and FBI assert that Title III and FISA provide the authority for Carnivore's full collection surveillance, while the pen register section of ECPA provides the authority to use Carnivore for pen mode surveillance.[79] This Note presents the relevant aspects of each of these statutes, but only challenges the propriety of the asserted pen register authority.

1. Title III and FISA

According to the Government, Title III and FISA are only relied on for authority to use Carnivore in full collection mode to acquire the *contents* of e-mail, web browsing, and file transfer activity. Nonetheless, an understanding of what these statutes authorize is worthwhile background information for understanding the FBI's use of Carnivore pursuant to pen register authority to collect non-content information associated with these activities.

a. Title III

Title III is a comprehensive statute covering the subject of wire and electronic surveillance. The statute generally prohibits intentional interception of wire, oral, or electronic communications,[80] but allows for law enforcement interception of such communication pur-

75 *Id.* at 743–44 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)). By using his telephone, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to [the company's] equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744.

76 18 U.S.C. §§ 2510–2522 (1994 & Supp. 1998).

77 50 U.S.C. §§ 1801–1863 (1994 & Supp. 1998).

78 18 U.S.C. §§ 3121–3127 (1994 & Supp. 1998).

79 *See supra* notes 4–9 and accompanying text.

80 *See* 18 U.S.C. § 2511(1)(a) (1994).

suant to a court order.[81] According to Title III, "intercept" is defined to mean the "acquisition of the contents of any wire, electronic, or oral communication."[82]

To acquire a court order authorizing the interception of electronic communication under Title III,[83] "[a]ny attorney for the Government may authorize application to a federal judge of competent jurisdiction . . . [for] an order authorizing or approving the interception of electronic communications . . . when such interception may provide or has provided evidence of [any federal felony]."[84] Title III requires that an application for an intercept order be "made in writing upon oath or affirmation" and state the relevant necessary information to support such an application.[85] The judge may enter an

---

81 *See id.* § 2516 (1994 & Supp. 1998). The statute also provides for the warrantless interception of such information under exigent circumstances (danger of death or serious physical injury to a person, national security, organized crime conspiracy). *See id.* § 2518(7) (1994).

82 *Id.* § 2510(4) ("'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device . . . ."). "Electronic communication" is defined in Title III to mean

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoeletronic or photooptical system that affects interstate or foreign commerce but does not include
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communication system used for the electronic storage and transfer of funds . . . .

Id. § 2510(12) (Supp. 1998).

83 Because Carnivore only intercepts electronic communication, the remainder of this discussion concerning Title III applications will address only those Title III provisions that involve the interception of electronic communication.

84 *Id.* § 2516(3) (1994). For interception of an electronic communication under Title III, the statute permits any attorney for the Government to authorize the application by listing any Federal felony, *see id.*, while for interception of a wire or oral communication the application must come from one of a listed group of Justice Department attorneys or the principal state prosecutor and must indicate a felony from a certain enumerated list, *see id.* § 2516(1)–(2).

85 *Id.* § 2518(1). The application shall identify the investigative or law enforcement officers both making and authorizing the application for a Title III order. *See id.* In addition, the application must state the facts justifying the application including the offense involved, the place where the interception will take place, the type of communication sought to be intercepted, the identity of the person committing the offense and whose communications are to be intercepted, *see id.* § 2518(1)(b), and

order authorizing the intercept only after determining probable cause exists regarding the individual involved, the relationship between the communication to be intercepted and the accused offense, and the appropriateness of the facilities to be targeted or used to intercept the communication.[86] If the judge finds probable cause, the order authorizing the interception of electronic communication must specify the identity, if known, of the person targeted by the surveillance, the facilities to be used, and the time period for interception.[87] The order may direct the provider of the electronic communication service to assist the applicant in completing the surveillance and interception.[88]

b. FISA

FISA permits federal agents to conduct electronic surveillance in order to monitor and retain information that is "evidence of a crime,"[89] provided that special district and appellate court judges determine "there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[90] FISA defines electronic surveillance to mean the acquisi-

"whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(1)(c). The applicant must also disclose any previous applications for such an order "known to the individual authorizing and making the application," *id.* § 2518(1)(e), and the success or failure of such application, when it would involve the same persons, facilities, or places as the present application. *See id.* Furthermore, the applicant may be required by the judge to furnish additional information in support of the application. *See id.* § 2518(2).

86 *See id.* § 2518(1). The judge must also determine that probable cause exists as to the inadequacy of other investigative methods. *See id.* § 2518(3)(c).

87 *See id.* § 2518(4). The order must also particularly describe "the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," *id.* § 2518(4)(c), "the identity of the agency authorized to intercept the communications, and of the person authorizing the application," § 2518(4)(d), and "whether or not the interception shall automatically terminate when the communication has been first obtained." *Id.* § 2518(4)(e).

88 *See id.* § 2518(4). An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

89 50 U.S.C. § 1801(h)(3) (1994); *see* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.3(d), at 365 & n.105 (2d ed. 1999).

90 50 U.S.C. § 1805(a)(3)(A); *see* 2 LAFAVE ET AL., *supra* note 89, at 364. The Act requires the Chief Justice of the United States to designate several district and circuit court judges to review petitions for electronic surveillance of foreign powers or an agent of a foreign power. *See* 50 U.S.C. § 1803(a)–(b); *see also* 2 LAFAVE ET AL., *supra* note 89, at 364–65 & n.103. FISA does not altogether preclude surveillance of United

tion of either the contents of wire or radio communication or "information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[91] FISA also permits the President, acting through the Attorney General, to authorize warrantless electronic surveillance "to acquire foreign intelligence information,"[92] if the Attorney General certifies that the surveillance will acquire only "the contents of communication transmitted by a means used exclusively between or among foreign powers."[93]

FISA also permits the use of pen registers and trap and trace devices for foreign intelligence and international terrorism investigations conducted by the FBI.[94] FISA allows for installation of a pen register or trap and trace device on a telephone line or a "communication instrument or device."[95] While the DOJ and FBI assert that Carnivore is only used pursuant to FISA for full mode surveillance, it appears statutorily permissible to use it for pen mode surveillance as well. However, FISA refers to the pen register section of ECPA for

---

States persons when they are acting as agents of a foreign power. *See* 50 U.S.C. § 1801(b)(2); 2 LAFAVE ET AL., *supra* note 89, at 365 & n.107–08. United States persons include U.S. citizens, permanent resident aliens, unincorporated associations comprised of U.S. citizens or permanent resident aliens, or U.S. corporations, "but does not include a corporation or association which is a foreign power." 50 U.S.C. § 1801(i); *see* 2 LAFAVE ET AL., *supra* note 89, at 365 n.107. FISA does not permit monitoring a US person solely because of the person's First Amendment activities. *See* 50 U.S.C. § 1805(a)(3)(A); 2 LAFAVE ET AL., *supra* note 89, at 365.

91 50 U.S.C. § 1801(f)(4). Contents of communications means "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." *Id.* § 1801(n). Wire communication is defined as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." *Id.* § 1801(*l*).

92 *Id.* § 1802(a)(1); *see* 2 LAFAVE ET AL., *supra* note 89, at 365.

93 50 U.S.C. § 1802(a)(1)(A); *see* 2 LAFAVE ET AL., *supra* note 89, at 365. A copy of the Attorney General's certification, given in writing under oath, is transmitted under seal to the special courts outlined above. *See* 50 U.S.C. § 1802(a)(3); 2 LAFAVE ET AL., *supra* note 89, at 365.

94 50 U.S.C. § 1842(a)(1) (Supp. 1998). The process for obtaining an order to install a pen register or trap and trace device under FISA is substantially similar to the process under the pen register section of ECPA. *Compare* 50 U.S.C. § 1842(b)–(d) (application and issuance under FISA), *with* 18 U.S.C. §§ 3122–3123 (1994) (application and issuance under the pen register section of ECPA).

95 50 U.S.C. § 1842(c)(3).

definitions of pen register and trap and trace device.[96] Because Carnivore does not constitute either of these devices under the present pen register statute, as this Note asserts,[97] the use of Carnivore in pen mode is neither authorized nor constrained by the provisions of FISA. Accordingly, this Note reserves further discussion of this issue to the analysis below.

2. The Pen Register Section of ECPA

As stated, the DOJ and FBI assert that the pen register section of ECPA provides the legal authority to use Carnivore to conduct pen mode surveillance.[98] While this Note asserts that the categories of information collected in such surveillance do not merit constitutional protection,[99] that does not necessarily mean that the pen register section of ECPA governs the gathering of such information. The pen register statute restricts the use of pen registers and trap and trace devices generally, but also authorizes law enforcement use of such devices. Thus, if Carnivore is not a pen register, there are no constraints on its use in pen mode. Before analyzing whether the statute is an appropriate authority for using Carnivore in pen mode, this Subsection provides a general overview of the statute's requirements and proscriptions.

a. Definition of Pen Register

In *Smith v. Maryland*, the Supreme Court relied on an earlier Court precedent when it referred to a pen register as "'a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released.'"[100] The pen register section of ECPA, passed seven years after the *Smith* decision, defines a "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers

96 *See id.* § 1841(2). The Committee Report accompanying the legislation that introduced the pen register section of FISA states that it "establishes a predicate for the use of pen registers or trap and trace devices that is . . . analogous to the statutory standard for the use of such devices in criminal investigations [that is, use under authority of the pen register section of ECPA]." S. REP. No. 105-185, at tit. VI (1998), *available at* ftp://ftp.loc.gov/pub/thomas/cp105/sr185.txt (last visited May 1, 2001).

97 *See infra* Part III.B.1–2.

98 *See supra* note 9 and accompanying text.

99 *See infra* Part III.A.2.

100 442 U.S. 735, 736 n.1 (1979) (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)). "It does not overhear oral communications and does not indicate whether calls are actually completed." *Id.* at 736 n.1 (quoting *N.Y. Tel. Co.*, 434 U.S. at 161 n.1).

dialed or otherwise transmitted on the telephone line to which such device is attached."[101] Law enforcement reliance on pen register authority to install new technologies, or to broaden the range of information that may be intercepted using a pen register, has been controversial.[102] This is due, at least in part, to the "*numbers dialed or otherwise transmitted*" language of the statute and its requirement that pen registers be *attached* to a *telephone line*. The analysis below suggests that the FBI's use of Carnivore to monitor the e-mail, web browsing, and file transfer activity of a targeted user appears comparably controversial. Therefore, a discussion of these concerns will be reserved to the Carnivore analysis in Part III.B.1.b.

b. Definition of Trap and Trace Device

According to the pen register section of ECPA, a "trap and trace device" is "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."[103] Like the pen register definition, the statutory terms used to define a trap and trace device have been controversial; the term "*originating number*" being the most problematic.[104] The use of Carni-

101 18 U.S.C. § 3127(3) (1994). The statute also states that

> such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

Id. Black's Law Dictionary defines a pen register as

> [a] mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed; thus, there is no recording or monitoring of the conversation.

BLACK'S LAW DICTIONARY 1134 (6th ed. 1990).

102 *See* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm; Dempsey Statement, *supra* note 1, at 8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml.

103 18 U.S.C. § 3127(4). The statute cross-references to Title III for the definitions of wire and electronic communication, where electronic communication can easily be read to include e-mail, web browsing, or file transfer activity. *See id.* § 3127(1) (citing *id.* § 2510(12) (Supp. 1998)); *see also supra* note 82 (providing the Title III definition of electronic communication).

104 *See* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm; Dempsey Statement, *supra* note 1, at 8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml.

vore in pen mode raises similar concerns; thus, a discussion of them is also reserved for the Carnivore analysis in Part III.B.2.

c. Application for an Installation Order

The pen register section of ECPA generally states that "no person may install or use a pen register or trap and trace device without first obtaining a court order [under this statute or FISA];"[105] though exceptions exist for the use of such devices under emergency circumstances or by service providers in the course of business.[106] The statute provides that "[a]n attorney for the Government may [apply] for an order . . . authorizing or approving the installation and use of a pen register or a trap and trace device . . . in writing under oath or equivalent affirmation, to a court of competent jurisdiction."[107] The application must identify the attorney making the application and the law enforcement agency conducting the investigation and shall certify "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[108]

d. Issuance of an Installation Order

The pen register section of ECPA provides that, upon receiving an application for an order authorizing the installation of a pen register or trap and trace device, "the court shall enter an ex parte order . . . if the court finds that the attorney for the Government . . . has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[109] The order must specify, if known, the identity of the person who has rights to the telephone line to which the pen register or trap and trace device is to be attached, the identity of the targeted subject

105 18 U.S.C. § 3121(a); *see supra* Part II.B.1.b.

106 *See* 18 U.S.C. § 3125 (1994 & Supp. 1998) (emergency use); *id.* § 3121(b) (1994) (service provider use). The service provider exception may be invoked by the service provider when used to operate, maintain, or test the service or to protect the rights or property of the provider or users, *see id.* § 3121(b)(1); to make a record of a communication to protect the provider, another provider, or a user of the service against fraudulent, unlawful, or abusive use of the service, *see id.* § 3121(b)(2); or with the user's consent, *see id.* § 3121(b)(3).

107 *Id.* § 3122(a)(1). The statute also provides that a state investigative or law enforcement officer may apply for an order under the pen register section of ECPA in the same manner to an equivalent state court. *See id.* § 3122(a)(2). Because Carnivore is only installed by the FBI, this Section will only refer to installations pursuant to a federal court order.

108 *Id.* § 3122(b)(2).

109 *Id.* § 3123(a).

of the investigation, the number and location of the telephone line to be monitored, and a statement of the offense to which the surveillance relates.[110] The liberal nature with which pen register and trap and trace orders are to be given—the court *shall* order *upon certification*—is beyond the scope of this Note. Part III.B.1.b, however, examines the statute's telephone line attachment requirement, and Part IV.A and D propose statutory changes that allow for alternative connections.

e. Limitation on Government Use

The pen register section of ECPA limits the use of pen registers by providing that "[a] government agency authorized to install and use a pen register . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."[111] This limitation on the use of *pen registers* has been analyzed and debated,[112] particularly due to the "*dialing* and *signaling information* used in *call* processing" language, as well as its coverage of pen registers only. Similar issues are implicated by the FBI's use of Carnivore in pen mode; these issues will be examined in Part III.B.3.

III. CARNIVORE AND THE LAW

Part II.A above presented the test for determining whether government action constitutes a search or seizure implicating the protections of the Fourth Amendment. In addition, Part II.B.2 introduced the pen register section of ECPA and indicated that the statute's language has been debated. This Part starts by determining that Carnivore, when operating in pen mode, does not violate a targeted user's expectation of privacy and thus does not implicate the Fourth Amendment.[113] It proceeds by illustrating how, under the present statutory

110 *See id.* § 3123(b)(1). An order to install a pen register under FISA allows for the use of such device on a "communication instrument or device." 50 U.S.C. § 1842(c)(3) (Supp. 1998); *see supra* Part II.B.1.b.

111 18 U.S.C. § 3121(c) (1994).

112 *See* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm; Dempsey Statement, *supra* note 1, at 8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml.

113 The Supreme Court has not confronted the expectation of privacy issue regarding e-mail and Internet activity. While several lower courts have addressed some Fourth Amendment e-mail and Internet issues, these cases are generally inapplicable to this Carnivore discussion due to case-specific facts. *See* United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *11 (4th Cir. May 4, 2000) (unpublished opinion) (holding that no expectation of privacy existed in non-content account in-

language, Carnivore fails to qualify as either a pen register or a trap and trace device and is therefore not governed by the pen register statute for pen mode surveillance. It adds that were Carnivore considered to be a pen register, it nonetheless violates the statutory limitation on government use of such devices. This Part concludes by stating that Carnivore's pen mode surveillance capabilities, while not constitutionally constrained, should be statutorily restricted in a manner comparable to the current regime for pen registers and trap and trace devices.

A. Carnivore's Pen Mode Surveillance Does Not Implicate the Fourth Amendment

In *Smith v. Maryland,* the Supreme Court directed that any Fourth Amendment expectation of privacy inquiry must begin by "specifying precisely the nature of the state activity that is challenged."[114] Accordingly, this section must begin with a quick review of what information is actually acquired by the Carnivore system when operating in pen mode. Only after that brief review can this Note explain why targeted users do not maintain an expectation of privacy in the aspects of their e-mail, web browsing, or file transfer activity that Carnivore gathers and records during pen mode surveillance.

1. Carnivore's Pen Mode Collections

Through the use of filters selected by FBI personnel, Carnivore is set for pen mode collection and programmed to collect certain information regarding e-mail, web browsing, and file transfer activity.[115] Regarding the targeted user's e-mail activity, Carnivore collects TO and FROM information, X'd-out subject header information that indi-

formation given to an ISP in order to establish an e-mail account); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding that no expectation of privacy existed in Internet activity due to a written Internet policy prohibiting personal Internet activity on a government computer and notifying the user of Internet activity audits); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that no expectation of privacy existed in subscriber information, including IP address, voluntarily exposed to the Internet service provider); United States v. Maxwell, No. 95-0751, 1996 CAAF LEXIS 116, at *28 (C.A.A.F. June 25, 1996) (holding that a network subscriber maintains no expectation of privacy as to the business records relating to a network account).

114 Smith v. Maryland, 442 U.S. 735, 741 (1979). This Note only discusses Carnivore in terms of its pen mode collections and only examines the expectation of privacy issue in terms of these collections.

115 *See* IITRI REPORT, *supra* note 3, at 3-11 to 3-14, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

cates the amount of data in the header, and the number of bytes transferred between the client and the server.[116] Regarding web browsing and file transfer activity, Carnivore collects the source and destination IP addresses and the number of bytes transferred between the client and the server.[117] It is important to note that Carnivore does not collect the full header information or URL address.[118]

2. Users Do Not Maintain an Expectation of Privacy in Addressing Information

The aforementioned types of information, collected by Carnivore during pen mode surveillance, are *voluntarily* conveyed to a third party—the ISP—when the targeted user conducts e-mail, web browsing, or file transfer activity.[119] In addition, e-mail and web browsing software typically provides this information to the user,[120] and ISPs

116 *See id.* at 3-24 (TO and FROM information), 3-24 (header information in X'd-out presentation), C-3 (bytes transferred and amount of data in header); *supra* Part I.C.3.a.

117 *See* IITRI REPORT, *supra* note 3, at C-6, C-8 (IP addresses), *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf; *id.* at 3-25 (web browsing: number of bytes transferred); *supra* Part I.C.3.b–c.

118 *See supra* Part II.C.3.b. The results of the IITRI report appear to refute the concerns expressed in recent congressional testimony that such information, which may contain privacy-protected components, is collected by Carnivore's pen mode surveillance. *See* Davidson Statement, *supra* note 10, at 5–6, *available at* http://www.house.gov/judiciary/davi0724.htm.

119 For assertions to the contrary, see Corn-Revere Statement, *supra* note 10, at 10, *available at* http://www.house.gov/judiciary/corn0724.htm; Davidson Statement, *supra* note 10, at 3–7, *available at* http://www.house.gov/judiciary/davi0724.htm; Dempsey Statement, *supra* note 1, at 8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; O'Neill Statement, *supra* note 10, at 2, *available at* http://www.senate.gov/~judiciary/962000_mo.htm; Rosen Statement, *supra* note 10, at 14, *available at* http://www.senate.gov/~judiciary/962000_jr.htm; Steinhardt Statement, *supra* note 10, at 1–5, 7, *available at* http://www.house.gov/judiciary/stei0724.htm. A recent student comment relied on these statements, and those of Government representatives, to echo the concern that Carnivore's pen mode capabilities invade Internet users' privacy rights. *See* Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111, 123–24 (2001). This comment primarily examines the constitutional and statutory framework that surrounds Carnivore's general operations, *see id.* at 111–21, and does not rely on the IITRI report or the FOIA documents for a better technical understanding of how Carnivore operates and what information it gathers during pen mode operations than the aforementioned statements provide. *See id.* at 122–24.

120 Netscape and Internet Explorer indicate the IP addresses associated with the URL locations entered by the user and monitor and update the user as to the size and transfer progress of the information requested.

and e-mail providers usually monitor and/or log this information in the ordinary course of business.[121] Consequently, despite any assertion of a personal or subjective expectation of privacy,[122] this information does not maintain an expectation of privacy that society, or the courts, will accept as reasonable.[123] Accordingly, with no expectation of privacy infringed and the Fourth Amendment not implicated, Carnivore's pen mode surveillance capabilities are constrained, if at all, only by the pen register section of ECPA.

B. Carnivore Is Not Governed by the Pen Register Statute

1. Carnivore Is Not a Pen Register

The pen register section of ECPA defines a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[124] While Carnivore

121 Consider the inclusion of sender information, subject line, date, and file size of e-mail inboxes with software like Eudora and Microsoft Outlook Express and Internet e-mail providers like Hotmail, Juno, Excite Mail, and Yahoo Mail (to name a few). Also consider the frequent and persistent notices from e-mail administrators as to the excessive size of e-mail accounts (I get these when I do not delete old messages quickly enough on Hotmail). Recall that in *Smith*, the Court refuted an expectation of privacy claim in telephone numbers because "pen registers and similar devices are routinely used by telephone companies 'for the purposes of checking billing operations, detecting fraud, and preventing violations of law.'" Smith v. Maryland, 442 U.S. 735, 742 (1977) (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977)).

122 *See* Corn-Revere Statement, *supra* note 10, at 10, *available at* http://www.house.gov/judiciary/corn0724.htm; Dempsey Statement, *supra* note 1, at 8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; O'Neill Statement, *supra* note 10, at 2, *available at* http://www.senate.gov/~judiciary/962000_mo.htm; Steinhardt Statement, *supra* note 10, at 1–5, 7, *available at* http://www.house.gov/judiciary/stei0724.htm.

123 *See Smith*, 442 U.S. at 743 (holding that information voluntarily conveyed to a third party waives expectation of privacy); *see also* United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *11 (4th Cir. May 4, 2000) (unpublished opinion) (holding that no expectation of privacy existed in non-content account information given to an ISP in order to establish an e-mail account); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that no expectation of privacy existed in subscriber information, including IP address, voluntarily exposed to an ISP); United States v. Maxwell, No. 95-0751, 1996 CAAF LEXIS 116, at *28 (C.A.A.F. June 25, 1996) (holding that a network subscriber maintains no expectation of privacy as to the business records relating to a network account).

124 18 U.S.C. § 3127(3) (1994); *see supra* Part II.B.2.a. FISA orders allow for the use of such devices on a telephone line or a "communication instrument or device." 50 U.S.C. § 1842 (Supp. 1998); *see supra* Part II.B.1.b. However, the fact that Carnivore fails to qualify as a pen register due to the information it collects, *see infra* Part

"records or decodes electronic impulses," Carnivore fails to satisfy the other clauses of this definition and thus fails to qualify as a pen register under the current statute. Consequently, its use in pen mode is not governed and cannot be constrained by the pen register section of ECPA.

a. Carnivore's Pen Mode Collections Do Not Identify "Numbers Dialed or Otherwise Transmitted"

According to the statute, a pen register "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[125] Assuming Carnivore were attached to a telephone line,[126] it would nonetheless fail to qualify as a pen register due to the "*numbers dialed or otherwise transmitted*" language of the definition[127] and would thus fall outside the scope of the pen register section of ECPA.

The IITRI report indicates that Carnivore acquires information during pen mode surveillance depending on what type of electronic communication it has been programmed to monitor—e-mail, web browsing, or file transfer activity. When monitoring e-mail activity, Carnivore acquires the e-mail addresses of recipients to whom e-mail has been sent or files have been transferred.[128] As all e-mail users know, e-mail addresses are, at best, alphanumeric designations (for

---

III.B.1.a, obviates the connectivity discrepancy between FISA and the pen register section of ECPA. Recall that the Committee Report accompanying FISA's pen register section intended the pen register section of ECPA to provide the statutory definition and standard for the use of such devices under FISA. *See* S. REP. No. 105-185, at tit. VI (1998), *available at* ftp://ftp.loc.gov/pub/thomas/cp105/sr185.txt (last visited May 1, 2001). Accordingly, since Carnivore is not a pen register under the pen register section of ECPA, as this Note asserts, it is not a pen register under the pen register section of FISA.

125 18 U.S.C. § 3127(3). The Committee Report accompanying FISA's pen register section makes no attempt to otherwise define a pen register and intends such a device be used in conformity with the pen register section of ECPA. *See* S. REP. No. 105-185, at tit. VI (1998), *available at* ftp://ftp.loc.gov/pub/thomas/cp105/sr185.txt (last visited May 1, 2001).

126 This assumption will be refuted in Part III.B.1.b.

127 For similar assertions, see Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm; Dempsey Statement, *supra* note 1, at 8, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; Steinhardt Statement, *supra* note 10, at 3–4, 7–8, *available at* http://www.house.gov/judiciary/stei0724.htm. The statute does not define what "numbers dialed or otherwise transmitted" means. *See* 18 U.S.C. § 3127(3).

128 *See* IITRI REPORT, *supra* note 3, at 3-24, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

example, student.18@nd.edu), but in many cases are purely alphabetical (for example, student@nd.edu).[129] Consequently, such addresses cannot reasonably be interpreted to mean "numbers dialed or otherwise transmitted."[130] With respect to pen mode surveillance of web browsing and file transfer activity, however, Carnivore does limit interceptions to the purely numeric IP addresses associated with these activities (for example, 255.255.255.255),[131] which appears to conform to the statutory language "numbers . . . otherwise transmitted." This necessarily creates, however, an inconsistency for Carnivore deployments—the pen register section of ECPA governs the gathering of web browsing and file transfer IP addresses but not e-mail addresses. Consulting the legislative history behind the pen register section of ECPA mitigates this inconsistency.[132]

The Committee Report accompanying ECPA addresses the subject of pen register use and states, "the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for the purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached."[133] The Committee Report also states that pen registers record "the telephone numbers to which calls have been placed from a particular telephone,"[134] "only the telephone numbers dialed,"[135] and "merely the electronic switching signals that connect two telephones."[136] In addition, one of the bill's sponsors, Senator Patrick Leahy, referred to pen registers as

129 These are imaginary e-mail addresses, but illustrative of what alphanumeric and alphabetical addresses look like.

130 18 U.S.C. § 3127(3). For a compelling argument that rejects the acquisition of header information under pen register authority, see Chris J. Katopis, *"Searching" Cyberspace: The Fourth Amendment and Electronic Mail*, 14 TEMP. ENVTL. L. & TECH. J. 175, 196–99 (1995).

131 *See* IITRI REPORT, *supra* note 3, at C-5, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

132 *See* S. REP. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

133 S. REP. No. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3603; *see* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm.

134 S. REP. No. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564; *see* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm.

135 S. REP. No. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3603; *see* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm.

136 S. REP. No. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564; *see* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm.

"devices used for recording which phone numbers have been dialed from a particular phone" in the legislative summary accompanying the bill's introduction.[137] To be sure, this legislative history is not dispositive of what constitutes "numbers dialed or otherwise transmitted," but it clearly supports a narrow interpretation of these terms to which IP addresses would not be included.[138] According to legislative history, therefore, Carnivore is not a pen register, because it does not record telephone numbers and is not constrained by the pen register section of ECPA when used for pen mode surveillance.

The understanding of what information pen registers actually record, as reflected in the statutory text and the legislative history, has been similarly adopted in judicial precedent. In *United States v. New York Telephone Co.*, the Supreme Court stated that pen registers "disclose only the telephone numbers that have been dialed—a means of establishing communication."[139] In *Smith*, the Supreme Court quoted this language when it held that the use of pen registers did not violate an expectation of privacy and thus did not implicate the Fourth Amendment.[140] Numerous lower court decisions subsequent to *Smith*, including a case decided in 2000, have used this language or sufficiently similar language, to support the proposition that pen registers only acquire telephone numbers.[141] Consequently, judicial interpretation provides further support for this Note's conclusion that the IP addresses gathered by Carnivore when operating in pen mode are not within the ambit of the "*numbers dialed or otherwise transmitted.*" Thus,

---

137 131 CONG. REC. 24,370 (1985).

138 For a similar assertion, see Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm, and Katopis, *supra* note 130, at 198 (regarding e-mail addresses).

139 United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977).

140 442 U.S. 735, 741 (1979).

141 *See* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) (citing 18 U.S.C. § 3127(3) (1994)) ("Pen registers record telephone numbers of outgoing calls . . . ."); Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995) (citing S. REP. No. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3603) (stating that a pen register's "only capability is to intercept [telephone] numbers"); *In re* Grand Jury Proceedings, 654 F.2d 268, 277 n.3 (3d Cir. 1981) (citing United States v. N.Y. Tel. Co., 434 U.S. 161 at n.1) (stating that "a pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released"); United States v. Michigan, 122 F. Supp. 2d 785, 789 (E.D. Mich. 2000) (defining pen register parenthetically as "tracking numbers dialed from a particular phone"); Jefferson v. Winnebago County, No. 94-C50151, 1995 U.S. Dist. LEXIS 2425, at *18 n.3 (N.D. Ill. Mar. 2, 1995) (citing *In re* Application of the United States of America for an Order Authorizing the Installation of a Pen Register, 610 F.2d 1148, 1152–53 (3d Cir. 1979)) (stating that "a pen register identifies what numbers were dialed from a subject telephone").

judicial precedent also accords with this Note's assertion that Carnivore is not a pen register under the statutory definition and is therefore not constrained by the pen register section of ECPA when operating in pen mode.

b. Carnivore Is Not Attached to a Telephone Line

The statutory definition of a pen register requires installation of a pen register device on a telephone line,[142] and other statutory provisions are predicated on a telephone line connection by such a device.[143] The IITRI report indicates, however, that Carnivore is not attached to a telephone line; rather, it is installed as a tap directly onto an ISP's Ethernet using an Ethernet adapter.[144] Consequently, because Carnivore does not attach to telephone lines, it does not fit within ECPA's definition of a pen register and, thus, is not governed by the pen register section of ECPA.

The legislative history of ECPA supports this narrow interpretation. In the Committee Report accompanying ECPA,[145] the Committee refers to pen registers only as devices that are installed on telephone lines to record telephone numbers. Specifically, the Committee Report states,

> [T]he term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or

142 *See* 18 U.S.C. § 3127(3) (1994). The statutory definition of a trap and trace device does not require connection to a telephone line, *see id.* § 3127(4), and the legislative history that is discussed below makes no indication that such a connection is required. *See* S. REP. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555. It can be argued that the other sections of the statute require indication of the telephone line to which a pen register or trap and trace device is to be attached. *See* 18 U.S.C. § 3123(b)(1)(C) (An installation order must indicate "the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached."); *see also Waddell*, 50 F.3d at 290–91 (making this determination). However, because the statutory definition of a trap and trace device lacks this requirement, this Section will only contend that Carnivore fails to qualify as a *pen register* due to the lack of such a connection.

143 For example, a pen register order must indicate "the number and, if known, physical location of the telephone line to which the pen register . . . is to be attached," 18 U.S.C. § 3123(b)(1)(C), and also the "identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register . . . is to be attached," *id.* § 3123(b)(1)(A). *See also id.* § 3123(d)(2) (stating that the order must indicate "the person owning or leasing the *line* to which the pen register or a trap and trace device is attached"); Corn-Revere Statement, *supra* note 10, at 9, *available at* http://www.house.gov/judiciary/corn0724.htm.

144 *See* IITRI REPORT, *supra* note 3, at 3-10, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf; *supra* Part I.A.

145 S. REP. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

> otherwise transmitted for the purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached.[146]

This legislative history indicates that Congress understood pen registers to be directly attached on telephone lines; it should not be argued that the statute means otherwise. Consequently, the legislative history supports this Note's determination that Carnivore does not operate as a pen register in the statutory sense and thus is not constrained by the statute's restrictions.

Subsequent legislation provides additional support for this assertion. The sections of FISA that authorize the use of pen registers do not limit the use of such devices to a telephone line, but allow for their use on a "communication instrument or device."[147] The Committee Report accompanying these FISA provisions does not account for this deviation from the provisions of the pen register statute, though it states that the Committee intends such devices be defined by and used in conformity with the pen register section of ECPA.[148] This suggests that Congress recognized the inadequacy of the pen register statute's telephone line connection requirement and made the necessary adjustments in the appropriate sections of FISA. Accordingly, because Carnivore is not attached to a telephone line, it is not a pen register under the pen register section of ECPA and is thus not governed by the statute's regulations.

A recent judicial interpretation of this language also held that the statute requires a device be attached to a telephone line to qualify as a

---

146 *Id.* at 49, *reprinted in* 1986 U.S.C.C.A.N. at 3603; *see id.* at 42, *reprinted in* 1986 U.S.C.C.A.N. at 3600 ("Briefly, a pen register is a device which can be attached to a telephone line for the purpose of decoding and recording the numbers dialed from that line."); Corn-Revere Statement, *supra* note 10, at 9, *available at* http://www.house.gov/judiciary/corn0724.htm.

147 50 U.S.C. § 1842(c)(3), (d)(2) (Supp. 1998).

148 *See* S. REP. No. 105-185, at tit. VI (1998), *available at* ftp://ftp.loc.gov/pub/thomas/cp105/sr185.txt (last visited May 1, 2001). Attorney General Janet Reno and FBI Director Louis Freeh testified before the Senate Appropriations Committee on the subject of Fiscal Year 1999 Appropriations for Counterterrorism, the legislative source of the pen register section of FISA, and made no mention of pen registers, other than Director Freeh's closing remark renewing a request for authorization to use such devices for foreign intelligence and international terrorism investigations. *See Fiscal Year 1999 Budget Request for Counterterrorism: Hearing Before the Commerce, Justice, State and Judiciary Subcomm. of the Senate Appropriations Comm.*, 105th Cong. (1998), *at* LEXIS Federal Document Clearing House Congressional Hearing Summaries database (Federal News Service, May 31, 1998) (testimony of Janet Reno, Attorney General of the United States, and Louis Freeh, Director of the Federal Bureau of Investigation).

pen register. In *Brown v. Waddell*,[149] the United States Court of Appeals for the Fourth Circuit reviewed the aforementioned legislative history and found that a digital display pager clone was not a pen register under the statute. In doing so, the Court quoted the statutory definition of a pen register and held,

> As a matter of plain textual meaning, a digital display pager clone does not itself fit this definition—in the critical sense that it is not a device [that is] attached to a telephone line. It receives (and "intercepts") electronic impulses transmitted by radio waves, and is "attached" to no transmission device. Hence, it is not defined *into* the category of pen registers by the statutory definition of that device.[150]

Like the digital display pager clone in *Waddell*, Carnivore is not a device attached to a telephone line—it is connected to an ISP's Ethernet via an Ethernet adapter—and a telephone line is not used to maintain its connection to the Ethernet.[151] While Carnivore arguably is attached to a "transmission device," the Ethernet itself, such a connection also is not facilitated or maintained via a telephone line. Consequently, under the Fourth Circuit's rationale in *Waddell*, Carnivore cannot be considered a pen register in the critical sense of the statutory definition and thus cannot be constrained by the pen register section of ECPA.

2. Carnivore Does Not Qualify as a Trap and Trace Device

The pen register section of ECPA defines a "trap and trace device" as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."[152] Computers clearly qualify as instruments or devices from

149 50 F.3d 285 (4th Cir. 1995).

150 *Id.* at 290–91 (quoting 18 U.S.C. § 3127(3) (1994)).

151 For an explanation of Carnivore and its connection to an Ethernet, see *supra* notes 31–33 and accompanying text.

152 18 U.S.C. § 3127(4) (1994). The statute cross-references to Title III for the definitions of wire and electronic communication, where electronic communication can easily be read to include e-mail, web browsing, or file transfer activity. *See id.* § 3127(1). According to Title III, electronic communication means "any transfer of signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12) (Supp. 1998); *see* Corn-Revere Statement, *supra* note 10, at 9, *available at* http://www.house.gov/judiciary/corn0724.htm. As with the pen register definition, the Committee Report accompanying FISA's trap and trace section makes no attempt to otherwise define a trap and trace device and intends such a device to be used in conformity with the pen

which electronic communications are transmitted; e-mail, web browsing, and file transfer activity clearly qualify as "incoming electronic or other impulses" and "electronic communication." Therefore, the use of Carnivore in pen mode under trap and trace authority appears partially supported by the statutory language. However, the requirement that the captured information identify the "originating *number*" of the transmitting device causes Carnivore to fall outside the statute's governance.

The IITRI report indicates that Carnivore, when operating in pen mode, acquires the information it is programmed to monitor with regard to e-mail, web browsing, or file transfer activity. When operating as a trap and trace device, Carnivore acquires the e-mail addresses of computer users from whom e-mail has been sent to the targeted user[153] and the source IP addresses of the web browsing or file transfer activity directed to the targeted user.[154] Carnivore's gathering of e-mail sender information clearly cannot qualify as "originating *numbers*" due to the at-best alphanumeric nature of the information acquired.[155] The intercepted IP addresses, on the other hand, are completely numeric means of identifying the instrument or device transmitting the electronic communication[156] and thus initially appear to fall within the statutory qualification. The legislative history of ECPA and judicial interpretations of the statutory language, however, belie this understanding.[157]

The Senate Judiciary Committee Report accompanying ECPA uses the statutory language to describe a trap and trace device.[158] However, the Report *defines* a trap and trace device in its glossary as a device which "records the numbers of *telephones* from which calls have been placed to a particular telephone."[159] While this definition does

---

register section of ECPA. *See* S. REP. No. 105-185, at tit. VI (1998), *available at* ftp://ftp.loc.gov/pub/thomas/cp105/sr185.txt (last visited May 1, 2001). Therefore, since Carnivore is not a trap and trace device under the pen register section of ECPA, as this Note asserts, it is not a trap and trace device for the purpose of FISA.

153 *See* IITRI REPORT, *supra* note 3, at 3-24, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

154 *See id.* at C-6 (web browsing activity), C-8 (file transfer activities).

155 *See supra* notes 128–30 and accompanying text; *supra* Part I.A.

156 *See* IITRI REPORT, *supra* note 3, at C-6, C-8, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf; *supra* note 131 and accompanying text; *supra* Part I.A.

157 *See* Corn-Revere Statement, *supra* note 10, at 8–9, *available at* http://www.house.gov/judiciary/corn0724.htm.

158 *See* S. REP. No. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3603.

159 *Id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. at 3564; Corn-Revere Statement, *supra* note 10, at 9, *available at* http://www.house.gov/judiciary/corn0724.htm.

not dispose of the ambiguity of the "originating number" language, it suggests that Congress understood trap and trace devices to record only telephone numbers. Accordingly, Carnivore's pen mode capabilities appear to fall outside the statute's regulation. However, because this prior legislative history only discusses what constitutes a trap and trace device briefly, and does so inconclusively, the legislative history of subsequent legislation should be considered for additional clarification of these terms before such an assertion can be made.

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA),[160] which requires communication providers to assist law enforcement officers in conducting electronic surveillance. Among other things, CALEA compels these providers to assist law enforcement acquisition of "call-identifying information,"[161] which the legislative history of CALEA explains to include information acquired by a trap and trace device.[162] The Committee Report accompanying CALEA states, "In trap and trace investigations, [call-identifying information] are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed."[163] While this language is no more dispositive of the issue than was the ECPA legislative history, it supports this Note's assertion that Congress understood trap and trace devices to record only telephone numbers. No other statutory text or legislative history, prior or subsequent to ECPA or CALEA, indicates that Congress understands or intends trap and trace devices to operate otherwise.[164] Consequently, because Carnivore's pen mode operations cannot be considered operations of a trap and trace device under the pen register statute's definition, Carnivore cannot be constrained as such by the statute's regulations.

160 H.R. 4922, 103d Cong., Pub. L. No. 103-414, 108 Stat. 4279 (1994) (enacted).

161 H.R. 4922, 103d Cong. § 108(a)(1), Pub. L. No. 103-414, 108 Stat. 4285 (1994) (codified as amended at 47 U.S.C. § 1007(a)(1) (1994)).

162 *See* H.R. REP. No. 103-827, pt. 1, at 21 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3501.

163 Id. This same language was used in the section-by-section analysis Senator Leahy provided when he introduced CALEA in 1994. *See* 140 CONG. REC. 20,448–49 (1994). The Committee Reports add that "[o]ther dialing tones that may be generated by the sender . . . are not to be treated as call-identifying information." H.R. REP. No. 103-827, at 21 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3501.

164 *See, e.g.*, H.R. REP. No. 104-383, pt. 3, § 302 (1995), *available at* ftp://ftp.loc.gov/pub/thomas/cp104/hr383.txt (last visited May 1, 2001) ("Section 302 grants the FBI authority to utilize 'pen registers' (which record the numbers dialed on a telephone) and 'trap and trace devices' (which record the number from which a call originates), such as through so-called 'caller ID.'").

Judicial opinions interpreting and applying the statutory definition of a trap and trace device further echo the assertion that such devices only record telephone numbers.[165] In 2000, the D.C. Circuit specifically examined ECPA and CALEA and discussed the use of trap and trace devices under these acts in *United States Telecom Ass'n v. FCC*.[166] Comparing Title III warrants to ECPA orders, the court noted in dicta that ECPA "establish[ed] less demanding standards for capturing telephone numbers through the use of . . . trap and trace devices."[167] Additionally, the court cited the statutory definition and stated, "trap and trace devices record telephone numbers from which incoming calls originate."[168] While this decision, like the legislative history, is not dispositive of the intended meaning of the term "originating number," it suggests that courts, like Congress, understand trap and trace devices to record only telephone numbers.

These judicial opinions, coupled with the legislative history of the statute and subsequent legislation, substantiate this Note's assertion that trap and trace devices, as presently defined, only intercept incoming telephone numbers. As discussed, when operating in pen mode as a "trap and trace device," Carnivore intercepts the sender information for e-mail activity, which is at best alphanumeric, and the purely numeric source IP addresses for web browsing and file transfer activity. Because these clearly are not telephone numbers, in any sense of that term, Carnivore is not operating as a "trap and trace device" within the statutory definition and thus cannot be constrained as such under the pen register section of ECPA.

165 *See, e.g.*, U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) (citing 18 U.S.C. § 3127(4) (1994)) ("[T]rap and trace devices record telephone numbers from which incoming calls originate, much like common caller-ID systems."); United States v. deLay, Nos. 92-30090 & 92-30091, 1993 U.S. App. LEXIS 4911, at *5 n.3 (9th Cir. Nov. 18, 1993) (unpublished opinion) ("A pen register tracks outgoing phone calls, and a trap and trace device tracks incoming calls."); United States v. Swinburne, No. 90-10492, 1993 U.S. App. LEXIS 11594, at *3 n.1 (9th Cir. Mar. 9, 1993) (unpublished opinion) ("A trap and trace identifies the originating points of incoming calls to a telephone number . . . ."); Jefferson v. Winnebago County, No. 94-C50151, 1995 U.S. Dist. LEXIS 2425, at *18 n.3 (N.D. Ill. Mar. 2, 1995) (stating that "a pen register identifies what numbers were dialed from a subject telephone whereas a [trap and] trace identifies from where a particular call is being made"). I found no cases that interpreted the statutory definition of a trap and trace device to mean anything other than a device that captures only telephone numbers.

166 227 F.3d 450 (D.C. Cir. 2000).

167 *Id.* at 454.

168 *Id.*

3. Carnivore Does Not Comply with the Government Limitation

ECPA's pen register section limits government use of pen registers to reasonably available technology "that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."[169] This limitation was enacted as part of the 1994 CALEA legislation.[170] Accordingly, to determine if Carnivore complies with this limitation—assuming it constituted a pen register in the statutory sense and was thus governed by the pen register section of ECPA—CALEA's legislative history should be examined to determine what Congress meant by the terms "*dialing* and *signaling* information utilized in *call* processing."

The Committee Report accompanying CALEA reports that the limitation restricts the use of a pen register device to technology that, when reasonably available, "restricts the information captured by such device to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured."[171] The Report also discusses the dialing and signaling information associated with "call-identifying information" and states, "In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order [or other lawful authorization]."[172] Not only does this legislative history indicate that the amendment was intended to limit the acquirable information to that which relates to a telephone call, but also, it indicates that Congress specifically excluded the interception of numbers entered after the initial telephone number is dialed.

The IITRI report indicates that Carnivore, when operating in pen mode, collects the addressing information for e-mail activity and the source and destination IP addresses for web browsing and file transfer activity.[173] These types of information definitively are not "*dialing* information," and while they could be construed as "*signaling* information," they do "*identify the numbers dialed*," and they are neither "used

169 18 U.S.C. § 3121(c) (1994).

170 *See* H.R. 4922, 103d Cong. § 207(c), Pub. L. No. 103-414, 108 Stat. 4292 (1994).

171 H.R. REP. No. 103-827, pt. 1, at 32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3512.

172 *Id.* at 21, *reprinted in* 1994 U.S.C.C.A.N. at 3501. This same language was used in the section-by-section analysis Senator Leahy provided when he introduced CALEA in 1994. *See* 140 CONG. REC. 20,448 (1994).

173 *See* IITRI REPORT, *supra* note 3, at 3-24 (e-mail), C-6 (web browsing activity), C-8 (file transfer activities), *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

in *call* processing" nor "necessary to direct or process a *call*." Furthermore, IP addresses are numbers transmitted after any initial telephone numbers are dialed—assuming the communication was sent by a user who initially connected to a communications provider via telephone line—in direct contravention of what the statute authorizes and the legislative history confirms. As such, even if Carnivore qualifies as a pen register under the statutory language and was therefore governed by the pen register section of ECPA, the use of Carnivore for pen mode surveillance does not comply with the statutory limitation on government use of such devices.

C. *Carnivore's Pen Mode Surveillance Is Not Constrained by Existing Law*

As this analysis indicates, Carnivore's pen mode surveillance does not implicate the Fourth Amendment[174] and is not restricted statutorily.[175] Accordingly, despite the DOJ's and FBI's contrary understanding, the FBI may deploy Carnivore for pen mode surveillance without any legal constraints.[176] However, because Carnivore, when operating in pen mode, gathers information of which individuals may maintain a personal or subjective expectation of privacy[177]—even if that expectation is not reasonable by Fourth Amendment standards—Congress

---

174 *See supra* Part III.A.2.

175 *See supra* Part III.B.

176 Without legal restraints, state governments might also use Carnivore-like devices in a similar manner. Consider that the pen register section of ECPA provides for state government use of pen registers and trap and trace devices under authority of the statute. *See* 18 U.S.C. § 3122(a)(2) (1994). If Carnivore is neither a pen register nor a trap and trace device under this statute, state governments do not need to consider the federal statute before using a Carnivore-like device. The only deterrent, assuming there is not a more restrictive state statute, would be the possibility of prosecution for violating the federal statute. *See id.* § 3121(d) ("Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both."). Rather than wait for a court to interpret the pen register statute in such a prosecution, it seems more appropriate for Congress to statutorily address the use of new surveillance technologies by implementing recommendations like those outlined in Part IV of this Note.

177 *See* Corn-Revere Statement, *supra* note 10, at 8, *available at* http://www.house.gov/judiciary/corn0724.htm; Davidson Statement, *supra* note 10, at 3–7, *available at* http://www.house.gov/judiciary/davi0724.htm; Dempsey Statement, *supra* note 1, at 6, *available at* http://www.cdt.org/testimony/000906dempsey.shtml; Steinhardt Statement, *supra* note 10, at 1–5, 7–9, *available at* http://www.house.gov/judiciary/stei0724.htm.

should revise the pen register section of ECPA to provide some statutory restrictions on Carnivore's pen mode surveillance capabilities.[178]

IV. RECOMMENDATIONS

The FBI's rationale for designing and implementing Carnivore is convincing,[179] and Carnivore is an invaluable tool for satisfying the government's needs.[180] Part III indicated that Carnivore is neither proscribed constitutionally nor restricted statutorily. While the FBI should continue to use Carnivore to conduct pen mode surveillance, it should not be able to do so without any legal constraints. Accordingly, Congress should revise the pen register section of ECPA to encompass Carnivore's pen mode surveillance capabilities.[181] In addition, the revised statute should accommodate future developments in communications and surveillance technologies. This Part

178 Congress followed a similar rationale when it enacted the original pen register section of ECPA in 1986. *See* S. REP. No. 99-541, at 1–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–57.

179 *See supra* Introduction.

180 *See supra* Part I.B.

181 On April 13, 2000, Senator Leahy introduced The Internet Security Act of 2000, a bill that would have greatly expanded the pen register section of ECPA and that served as the foundation for the statutory changes proposed in this Note. *See* S. 2430, 106th Cong. § 7 (2000), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.2430: (last visited May 1, 2001). This Note expands on the language proposed in that Act in order to provide further clarity and breadth to the pen register statute. In addition, Senator Leahy's amendment sought to provide for greater judicial discretion in authorizing pen register or trap and trace device applications, *see id.* § 7, an idea that is neither proposed nor endorsed in this Note. Another piece of legislation from the 106th Congress initially sought to amend the statute and allow broader pen register or trap and trace surveillance, but it only sought to add "e-mail addresses" to the scope of collectable information. *See* Electronic Communications Privacy Act of 2000, H.R. 5018, 106th Cong. § 4, *available at* http://thomas.loc.gov/cgi-bin/query/D?c106:1:./temp/~c106BtXONk:: (last visited May 1, 2001) (allowing for judicial discretion in approving applications). This Note does not rely on this Act because the term "e-mail addresses" is not sufficiently broad to avoid some of the problems outlined in this Note (for example, IP addresses are not "e-mail" addresses and thus would not be covered under House Resolution 5018). The other legislation proposed in the 106th Congress did not address the changes proposed in this Note. *See* Internet Integrity and Critical Infrastructure Protection Act of 2000, S. 2448, 106th Cong. § 301, *available at* http://thomas.loc.gov/cgi-bin/query/D?c106:2:./temp/~c106o8e7Us:: (last visited May 1, 2001) (requiring description of facts underlying certification and additional reporting of pen register and trap and trace usage); Electronic Rights for 21st Century Act, S. 854, 106th Cong. § 103 (1999), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.854: (last visited May 1, 2001) (granting courts discretion to determine if the information sought is relevant to an ongoing criminal investigation).

proposes statutory language that accomplishes both of these objectives.

A. Revise the Statutory Definitions

The pen register section of ECPA does not cover the use of Carnivore as a pen register, because Carnivore collects more information than the "the *numbers dialed or otherwise transmitted*" and because it is not *attached* to a *telephone line*.[182] In addition, the pen register statute does not cover the use of Carnivore as a trap and trace device, because Carnivore collects information that is inconsistent with the "originating number" limitation, as understood from the statutory text, legislative history, and judicial interpretations.[183] The following definitions of pen register and trap and trace device bring Carnivore within the ambit of the pen register section of ECPA and, also, are broad enough to accommodate the inevitable developments in communications and surveillance technologies.

Adopting the proposed changes to the pen register definition, the amended § 3127(3) would read as follows (proposed changes italicized):[184]

> (3) the term "pen register"—
>
> (a) means a device *or process* that records or decodes electronic or other impulses *that identify the telephone numbers, electronic addresses, other electronic routing information, or other identifiers dialed or otherwise transmitted by an instrument or device or facility from which a wire or electronic communication is transmitted and used for purposes of identifying the destination or termination of such communication; and*
>
> (b) does not include any device *or process* used by a provider *or* customer of a wire *or* electronic communication service for billing, or recording as incident to billing, for communications services provided by such provider or any device *or process* by a provider or customer of a wire communications service for cost accounting or other like purposes in the ordinary course of business.

---

182 *See supra* Part III.B.1. Accordingly, Carnivore also is not a pen register for FISA purposes. *See supra* notes 119–20, 143 and accompanying text.

183 *See supra* Part III.B.2. Likewise, Carnivore also is not a trap and trace device for FISA purposes. *See supra* note 146 and accompanying text.

184 Subsection (b) is identical to what Senator Leahy proposed in Senate Bill 2430, but subsection (a) contains language beyond what was proposed in that bill. *See* The Internet Security Act of 2000, S. 2430, 106th Cong. § 8(b)(1), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.2430: (last visited May 1, 2001). Adopting these changes will also bring the use of Carnivore within the ambit of the FISA provisions governing the use of pen registers. *See* 50 U.S.C. §§ 1842–1844 (Supp. 1998).

Adopting the proposed changes to the trap and trace device definition, the amended § 3127(4) would read as follows (proposed changes italicized):[185]

> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating *telephone numbers, electronic addresses, other routing information, or other identifiers* dialed or otherwise transmitted by an instrument *or device or facility* from which a wire or electronic communication is transmitted.

These definitional changes encompass Carnivore's pen mode collection of sender and recipient addresses in e-mail activity, which clearly qualify as "electronic addresses," and the IP addresses associated with web browsing and file transfer activity, which clearly qualify as either "electronic addresses" or "other routing information." Therefore, these proposed changes provide statutory governance for future Carnivore deployments, as it presently operates. In addition, the breadth of these new terms—and the additional phrases "or other identifier" and "or device or facility"—allows for developments in communications and surveillance technologies.

B. Revise the Government Limitation

The pen register statute's current government limitation section confines the information acquired by *pen registers* to "dialing and signaling information utilized in call processing."[186] As outlined, even if Carnivore constitutes a pen register, the information Carnivore gathers does not satisfy this limitation as understood from the statutory text and its legislative history.[187] In addition to this Carnivore-specific problem, however, the existing statutory limitation is deficient because it only applies to pen registers, rather than to pen registers and trap and trace devices alike.[188] As such, any proposed change must expand the limitation to cover trap and trace devices, must encompass the information that Carnivore currently intercepts, and must provide for developments in communications and surveillance technologies. Adopting the following recommendations, the amended § 3121(c)

185 This proposes changes beyond what Senator Leahy offered. *See* The Internet Security Act of 2000, S. 2430, 106th Cong. § 8(b)(2), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.2430: (last visited May 1, 2001). These changes also will bring Carnivore within the ambit of the FISA provisions governing the use of trap and trace devices. *See* 50 U.S.C. §§ 1842–1844 (Supp. 1998).

186 18 U.S.C. § 3121(c) (1994).

187 *See supra* Part III.B.3.

188 *See* 18 U.S.C. § 3121(c).

would satisfy these objectives and would read as follows (proposed changes italicized):[189]

> (c) Limitation. A government agency authorized to install and use a pen register or *trap and trace device* under this chapter (18 U.S.C. §§ 3121 et seq.) or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to *those authorized in this chapter (18 U.S.C. §§ 3121 et seq.).*

This language not only encompasses trap and trace devices and Carnivore, but also changes the limitation from "dialing and signaling information utilized in call processing" to "those authorized in this chapter." Doing so binds the limitation statute to the language of the authorizing provisions and avoids the interpretation problems that previously existed when the limiting and authorizing clauses utilized different terminology.[190] If the authorizing provisions conform to this Note's definitional proposals,[191] the government limitation section will cover Carnivore's pen mode capabilities and will not limit such surveillance—or that of similar future technologies—any further than such use is limited by the new definitions.

C. Add a Limitation Notice to Issued Orders

The Issuance of Court Order section should be revised to reflect the language of the new government limitation as well. Adopting the following recommendation, the amended § 3123(b) would require that an order authorizing the use of a pen register or trap and trace device[192]

> *(3) shall direct that the use of the pen register or trap and trace device be conducted in such a way as to minimize the recording or decoding of any electronic or other impulses that are not related to the telephone numbers,*

---

189 This proposes changes that were not offered by Senator Leahy. *See* The Internet Security Act of 2000, S. 2430, 106th Cong., *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.2430: (last visited May 1, 2001).

190 *Compare* 18 U.S.C. § 3127(3) ("[T]he term 'pen register' means a device which records or decodes electronic or other impulses which identify the *numbers dialed or otherwise transmitted on the telephone line* to which such device is attached . . . ." (emphasis added)), *with id.* § 3121(c) ("A government agency authorized to install and use a pen register . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the *dialing and signaling information used in call processing.*" (emphasis added)).

191 *See supra* Part IV.A.

192 This proposes changes beyond those of Senator Leahy. *See* The Internet Security Act of 2000, S. 2430, 106th Cong. § 7(2)(C), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.2430: (last visited May 1, 2001).

electronic addresses, other electronic routing information, or other identifiers dialed or otherwise transmitted by an instrument or device or facility for use in wire or electronic communication processing or transmission.

The inclusion of this clause accomplishes two goals. First, it reminds those relying on the statute—government attorneys, state investigative or law enforcement officers, and judges—of the existing limitations on the use of pen registers, trap and trace devices, and other surveillance tools, such as Carnivore, in a section of the statute that they are likely to review on a regular basis. Second, it requires that the actual order authorizing the use of such a device contain language that specifically tracks the statutory limitations, thereby giving clear and direct notice to those acting pursuant to the order of what is and is not permitted and proscribed under the law.

D. Modify the Statute's Attachment Requirement

The statute's current Issuance of Order section, § 3123, consistently refers to telephone lines and requires the attachment of pen registers and trap and trace devices to such lines.[193] As discussed, Carnivore is not attached to a telephone line and therefore cannot comply with an order issued under existing law.[194] Accordingly, the relevant subsections of § 3123 must be amended to allow for the attachment, *application*, or *connection* of pen registers or trap and trace devices to telephone lines *and other facilities*.[195] These changes not

193 *See* 18 U.S.C. § 3123(b), (d); *see also supra* notes 137–38 and accompanying text.

194 *See supra* Part.III.B.1.b.

195 This proposal is substantially similar to what Senator Leahy offered, but adds "or connected" before his legislation added "or applied." *See* The Internet Security Act of 2000, S. 2430, 106th Cong. § 8(a), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.2430: (last visited May 1, 2001). This Note rejects the FISA language that allows connection of a pen register or trap and trace device to a "communication instrument or device," *see* 50 U.S.C. § 1842(c)(3) (Supp. 1998), because such terms appear open to interpretative attack (for example, an argument that the instrument or device is not to be used for "communication"). Accordingly, § 3123(b), as amended by this Note's proposals, would read as follows (proposed changes italicized):

(b) Contents of order. An order issued under this section—
  (1) shall specify—
    (A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line *or other facility* to which the pen register or trap and trace device is to be attached, *connected, or applied*;
    (B) the identity, if known, of the person who is the subject of the criminal investigation;

only encompass and accommodate the manner in which the FBI currently connects Carnivore to an ISP's Ethernet, but also allow for connectivity developments in communications and surveillance technologies.

CONCLUSION

The development of the Internet as a general communications tool has provided new means for criminals to conduct illegal activities. Carnivore is an impressive and important surveillance tool that the FBI should use to monitor illegal activity occurring via the Internet. Because the current law is "hopelessly out of date" with modern technology,[196] there are no constitutional or statutory proscriptions on the FBI's use of Carnivore to conduct pen mode surveillance. To accommodate privacy concerns and ensure appropriate use of Carnivore and future surveillance technologies, it is imperative that Congress amend the pen register section of ECPA at the earliest opportunity. This Note presents the necessary statutory changes to accomplish this objective. It is time for Congress to act.

> (C) the number and, if known, physical location of the telephone line *or other facility* to which the pen register trap and trace device is to be attached, *connected, or applied* and, in the case of a trap and trace device, the geographic limits of the trap and trace order . . . .

In addition, the amended § 3123(d), which prohibits disclosure of pen register or trap and trace device installation, would read as follows (proposed changes italicized):

> (d) Nondisclosure of existence of pen register or trap and trace device. An order authorizing or approving the installation and use of a pen register or trap and trace device shall direct that—
>
> (1) the order be sealed until otherwise ordered by the court; and
>
> (2) the person owning or leasing the line *or other facility* to which the pen register or trap and trace device is attached, *connected, or applied, or who is obligated* by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

196 The Senate Judiciary Committee Report accompanying the ECPA used the same language to describe the pre-ECPA state of the law. *See* S. REP. No. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (quoting Senator Leahy, 132 CONG. REC. 14,600 (1986)).