Carnivore, The FBI's E-mail Surveillance System: Devouring Criminals, Not Privacy

Griffin S. Dunham*

* B.A. 1999, Purdue University; J.D. 2002, Indiana University School of Law – Bloomington. Special thanks to my mother for her valuable assistance during the revising process.

I. INTRODUCTION

"*Carelessness about our security is dangerous; carelessness about our freedom is also dangerous.*"[1] The obvious message of this statement is to be ever-mindful of the fine line between a comfortable co-existence with the government and a pronounced separation from the government. Accordingly, decisions to support or oppose governmental action should contemplate this cautious yet responsible approach. The abstraction of the statement requires its individualized application to specific governmental action to determine whether our decision to endorse or oppose that action is prudent. One such governmental action is the FBI's implementation of Carnivore, an Internet monitoring system introduced on July 11, 2000.[2]

Carnivore was designed, and is used exclusively, to carry out court-ordered surveillance of electronic communications, *e.g.*, e-mail.[3] Carnivore

1. Adlai E. Stevenson Jr., Speech in Detroit, Michigan (October 7, 1952), *in* DANIEL B. BAKER, POWER QUOTES 123 (1992).

2. *The Carnivore FOIA Litigation*, *at* http://www.epic.org/privacy/carnivore/ (updated Aug. 8, 2001).

3. Carnivore can also be used to record Internet sites visited by the suspect for later evaluation, but the FBI insists that usage of Carnivore is restricted to

is a tangible, portable device, tantamount to a phone tap, that acts as a "sniffer," allowing the FBI to intercept and collect criminal suspects' e-mail without their knowledge or consent.[4] Carnivore is used only in limited circumstances—after FBI, Department of Justice, and judicial scrutiny—pursuant to detailed court orders prescribing and proscribing retrieval procedures.[5] The concern that Carnivore transforms George Orwell's fictitious "Big Brother" concept to reality (by allowing the FBI to engage in unfettered e-mail monitoring), however, raises the need to address the system.

Accordingly, this Note addresses competing and parallel interests between the government and society to determine the legitimacy and necessity of Carnivore. The purpose of this Note is twofold: first to demonstrate the need for Carnivore to enable law enforcement to keep up with criminals who utilize cyberspace to communicate criminal plans; and second to dispel privacy concerns associated with the system by allaying misconceptions and fears related to its implementation and usage.

Part II of this Note addresses the catalyzing reasons for Carnivore's design and use. Part III describes the FBI's extensive and mandatory internal procedures that dictate the decision to use Carnivore to pursue a suspected criminal, and addresses the three federal statutes that can empower Carnivore's use. Part IV explains Carnivore's method of operation; i.e., how it works in each of three stages. Part V articulates the privacy concerns raised by privacy advocates, including: (1) the possibility of collecting and storing e-mail in violation of federal law; (2) Fourth Amendment infringement; and (3) a lack of FBI individual accountability by failing to employ tracking mechanisms that allow for independent oversight. Finally, this Note concludes by addressing policy considerations that should shape the future for Carnivore.

II. A BACKGROUND TO CARNIVORE: REASONS FOR IMPLEMENTATION

As computer technology and usage rapidly proliferates within our society, criminals embrace this advancement by capitalizing on the

capturing e-mail transmission. *See* IIT RESEARCH INST., INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM, FINAL REPORT §§ ES.4-5 (2000), *available at* http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf [hereinafter REVIEW].

4. *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing Before the Senate Comm. on the Judiciary: Carnivore Diagnostic Tool*, 106th Cong. (2000) (statement of Donald Kerr, Assistant Director, FBI Laboratory) *available at* http://www.fbi.gov/pressrm/congress/congress00/kerr090600.htm [hereinafter *9/6/00 Hearing*].

5. *Id*.

opportunities and capabilities produced by that technology's increasing pervasiveness.[6] The FBI recognizes cyberspace as an efficient and increasingly popular medium for criminal activity, especially among spies, hackers, and other dangerous criminals.[7] In response to these threats against the safety of the American people, to the security of our communications infrastructure, and to the important commercial and private need for a safe, secure, and vibrant Internet, the FBI has concentrated its technological efforts and resources to fight a broad array of cyber crimes.[8] One of these efforts has been in the design and implementation of Carnivore, which the FBI hopes will increase public safety by reducing the amount of computer-assisted criminal activity. Specifically, the FBI has articulated five types of critically important crimes that Carnivore will target: terrorism, information warfare, child pornography, fraud (including white collar), and virus writing and distribution.[9]

A. Terrorism

Terrorists use information technology and the Internet to formulate plans, to raise funds, to spread propaganda, and to communicate securely.[10] Cyber terrorism—the usage of cyber tools to shut down critical national infrastructures such as energy, transportation, water, telecommunications and other government operations to coerce or intimidate a government or civilian population—is a very real threat with destructive potential.[11] In fact, Director of Central Intelligence George Tenet, testifying on the worldwide threat of terrorism, stated that terrorist groups, including Hizbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida organization are using computerized files, e-mail, and encryption to support their operations.[12] Although none of these groups have successfully

6. *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the House Comm. on the Judiciary: Internet and Data Interception Capabilities Developed by the FBI*, 106th Cong. (2000) (statement of Donald Kerr, Assistant Director, FBI Laboratory), *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm [hereinafter *7/24/00 Hearing*].

7. *9/6/00 Hearing*, *supra* note 4.

8. *Id*.

9. *See id.*

10. *Critical Information Infrastructure Protection: The Threat Is Real: Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. (1999) (statement of Michael Vatis, Director, FBI National Infrastructure Protection Center), *available at* http://www.fbi.gov/ congress/congress99/nipc10-6.htm.

11. *Cyber Attack: Improving Prevention and Prosecution: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Guadalupe Gonzalez, Special Agent In Charge, FBI Phoenix Field Division), *available at* http://www.fbi.gov/ congress/congress00/gonza042100.htm.

12. *Id*.

employed cyber technology to infiltrate our critical infrastructures, their reliance on information technology and acquisition of computer expertise clearly indicates the knowledge, opportunity, and interest for chaotic destruction.[13]

While the danger from these organizations is currently only a potential threat, the FBI has documented acts of terrorism that were organized and conspired through e-mail and downloaded to computer systems. The FBI, using traditional law enforcement tactics, recently thwarted a terrorist group's plan to break into several National Guard Armories and steal explosives to incapacitate several power transmission sources in the southern United States.[14] FBI intelligence revealed e-mail to be a major communication method among the group in attempting to effectuate their plan.[15] Further, the FBI seized computer evidence that showed the group had downloaded information on Ricin, the third most deadly toxin in the world.[16]

B. Information Warfare

Quite possibly the single greatest cyber threat to our national security lies in "information warfare" by foreign countries and their militaries against U.S. critical infrastructures.[17] Information warfare is a product of other countries' military inferiority in comparison to U.S. forces.[18] In essence, what foreign nations lack in firepower, resources, and training, they attempt to compensate for by waging a "cyber war." This type of war attempts to exploit our "Achilles heel"—a national dependence on information technology in government, commercial, and private operations.[19]

Two Chinese military officers, cognizant of the United States' military stronghold throughout the world, recently published a book that recommended the usage of unconventional measures, including spreading

13. *See id.*

14. *See 7/24/00 Hearing*, *supra* note 6, at 33.

15. *Id*.

16. *Id*.

17. *See* Jim Christy, *Chasing Shadows: The Human Face Behind the Cyber Threat*, 53 F.C.L.J. 185 (2000) (reviewing RICHARD POWER, TANGLED WEB: TALES OF DIGITAL CRIME FROM THE SHADOWS OF CYBERSPACE (2000)).

18. *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing: Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Louis J. Freeh, Director, FBI), *available at* http://www.fbi.gov/congress/congress00/cyber032800.htm [hereinafter *3/28/00 Hearing*].

19. *Id*.

computer viruses to neutralize U.S. advantages.[20] Additionally, the Russian government also recognizes that an attack on the U.S. computer infrastructure, by its catastrophic consequences, could overlap with the use of weapons of mass destruction.[21]

C. Child Pornography

Although exploitation of children is not a national security issue like terrorism and information warfare, its infiltration into our society is analogously detrimental because it reaches deep into the welfare of our communities. It is now overwhelmingly clear that computer and Internet users are using their systems to disseminate child pornography, and to arrange illegal meetings between user and child—an often violent and deadly combination.[22] As a result, the Internet has dramatically increased the access of sex offenders to the population they seek to victimize.[23] These manipulating users take on a "virtual" identity, appealing to a child's impressionable mind while maintaining the saving grace of anonymity. Once a relationship has been established, the trap has been set and the predatory Internet user now must only coerce the innocent child to take the already tempting bait.

To combat sexual predators, the FBI devised "Innocent Images," an initiative designed to capture individuals who travel between states to engage in illegal sexual activity with a child, and those who produce or distribute child pornography via the Internet.[24] The program entails FBI agents going undercover on the Internet by assuming the role of a child, arranging a meeting place with an offender, and arresting the offender(s) upon identification.[25] Capturing these offenders is extremely difficult, however, because the offenders can easily remain anonymous. They use encryption to conceal their illegal activities, which usually consist of communicating with the child and storing pornography files.[26] Innocent Images found it difficult, and sometimes impossible, to defeat the

20. *Id*.

21. *Id*.

22. *See 7/24/00 Hearing*, *supra* note 6.

23. *Online Child Pornography, Innocent Images National Initiative*, *at* http://www.fbi.gov/hq/cid/cac/innocent.htm (last visited Jan. 23, 2002) [hereinafter *Innocent Images*].

24. *Preventing Child Exploitation on the Internet: Hearing Before the Subcomm. on Senate Appropriations of the Senate Comm. on the Judiciary*, 105th Cong. (1998) (statement of Louis J. Freeh, Director, FBI), *available at* http://www.fbi.gov/congress/congress98/sac310.htm [hereinafter *3/10/98 Hearing*].

25. *Id*.

26. *Id*.

encryption.[27]

The FBI is extremely focused on and concerned with sexual predators because they possess distinct character traits. In fact, clinical studies report that a child molester will typically victimize seventy innocent children during his or her lifetime.[28] Between 1995 and 2001, the FBI investigated over 800 cases involving offenders crossing state lines to carry out an illegal sexual relationship and more than 1,850 cases involving the exchange of child pornography over the Internet.[29] All arrests pursuant to these investigations were made using traditional enforcement tactics—before the implementation of Carnivore.

D. Fraud

> Internet fraud is defined as any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms and E-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices or other items of value to the control of the scheme's perpetrators.[30]

Understanding and using the Internet to combat Internet fraud is absolutely essential for law enforcement.[31]

The Internet provides an ideal medium to commit fraud for three reasons. First, access to the Internet essentially means access to thousands of other Internet users through chat rooms, forum discussions, and instant messaging systems. Second, as with sexual predators, fraudsters can retain complete anonymity.[32] "The crucial difference in fraud committed over the Internet is that the perpetrator can 'virtually' vanish, leaving consumers wondering who or where to turn to for help."[33] Third, fraudsters no longer face financial barriers such as mailings, hiring people to reply to the mailings, and maintaining expensive toll-free telephone services.[34]

---

27. *Id*.
28. *Id*.
29. *9/6/00 Hearing*, *supra* note 4.
30. *The Internet Fraud and Complaint Center*, *Bankruptcy Fraud Video*, *at* http://www.fbi.gov/hq/cid/fc/ifcc/about/about_ifcc.htm (last visited March 2, 2001) [hereinafter *IFCC*].
31. *Id*.
32. *Id*.
33. Press Release, U.S. Department of Justice, Federal Bureau of Investigation, Internet Fraud Complaint Center Press Packet (May 8, 2000), *at* http://www.fbi.gov/pressrel/ pressrel00/ifccpr.htm.
34. *IFCC*, *supra* note 30.

The North American Securities Administrators Association estimates Internet-related stock fraud costs investors approximately $10 billion per year, which equals nearly $1 million per hour.[35] In just one case, on March 5, 2000, nineteen fraudsters were indicted in conjunction with a multi-million dollar insider trading scheme that used Internet Service Provider ("ISP") chat rooms as the medium to facilitate and effectuate their scheme.[36] The central "player" in the case passed inside information about clients of several other brokerage firms to two other individuals in exchange for a percentage of the profits subsequently received by acting on the information.[37] This fraudster passed information almost solely through online chats and instant messages for two and one-half years, received $170,000 in kickbacks for his services, and earned $500,000 for his partners.[38] Although the FBI captured these criminals, the traditional tactics used to arrest the individuals involved were inefficient, and keeping up with these types of criminals requires a different approach.[39]

E. Virus Writing

As computer usage increases, so does the number of computer viruses. Throughout the U.S. and other cyber-linked countries, virus writers pose an increasing risk to networks and systems.[40] In the year 2000, viruses such as the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus infiltrated systems worldwide, destroying computer programs and files.[41] Many computer viruses use e-mail as the vehicle for destruction, proliferating through the computer system when the user opens the e-mail file.

35. *9/6/00 Hearing*, *supra* note 4, at 34.
36. *Id*.
37. *Id*.
38. *Id*.
39. *IFCC*, *supra* note 30.
40. *3/28/00 Hearing*, *supra* note 18, at 27 (statement of Louis J. Freeh).
41. *See id.*

III. CARNIVORE USE MUST BE PURSUANT TO FEDERAL STATUTE

Before Carnivore's surgical methods are employed to pursue a suspected criminal, two safeguards fraught with substantive and procedural requirements must be satisfied: The Bureau and Department of Justice ("DOJ") must endorse its usage, and federal law must permit its deployment.

A. FBI and DOJ Approval

Before Carnivore is engaged, the FBI must scrutinize its appropriateness under the circumstances, and obtain DOJ approval.[42] FBI standard operating procedure mandates an eight-step process for determining the appropriateness of Carnivore usage. First, the FBI field agent assigned to the potential case involving Carnivore works in collaboration with the field office principal legal advisor and an attorney from the nearest U.S. Attorney's Office.[43] Together, they revise their documentation of the case's circumstances and particulars, and make comments and suggestions to those involved in the next level of scrutiny.[44]

After approval from field office management, the office submits the case file to the Department of Justice's Office of Enforcement Operations ("DOJOEO") in the Criminal Division, and also to FBI Headquarters.[45] Once received by Headquarters, the documents are processed and analyzed by the Legal Counsel Division and the Criminal Investigative Division.[46] Upon arrival at the Criminal Investigative Division, the case file is appropriated to the program manager in charge of the crime(s) being investigated, *e.g.*, child pornography or terrorism.[47] This program manager thoroughly reviews the case record and file, and determines if the suspect is worthy of pursuit and if interception is appropriate.[48] The interception inquiry ends if the program manager makes a negative determination.

If the program manager decides the suspect and interception is appropriate, the DOJOEO and Legal Counsel Division further refine case

42. Donald P. Delaney et al., *Wiretap Laws and Procedures: What Happens When the U.S. Government Taps a Line*, § 2.1.1, *at* http://www.cpsr.org/cpsr/privacy/wiretap/wiretap.procedure.html (Sept. 23, 1993).

43. *Id*.

44. *Id*.

45. *Id*.

46. *Id*.

47. *Id*.

48. Delaney, *supra* note 42.

findings and forward them to the Deputy Assistant Attorney General (or someone higher).[49] The Deputy Assistant Attorney General reviews the documents and decides whether to approve the case's continuation.[50] If approved, the DOJ authorizes the initial U.S. Attorney's Office to complete and file in court a final version of all documents acquired in conjunction with the investigation.[51] This file includes documents necessary to analyze the interception under federal guidelines (which will be discussed in the following section).[52] After the case is filed, the U.S. Attorney's Office applies for a court order to use Carnivore by submitting the suspect's file and the DOJ authorization to a federal judge.[53] This judge then analyzes the comprehensive record and rules and decides whether Carnivore's use would comport with federal law.[54]

B. Federal Statutory Approval

Even if Carnivore receives the requisite Bureau and DOJ endorsement, its usage must still conform to federal law. The governing federal law will be revealed in the application submitted to the federal judge, but will be either: (1) Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"); (2) the pen-trap provisions of 18 U.S.C. §§ 3121-3124; or (3) the Foreign Intelligence Surveillance Act.[55]

1. Title III of the Omnibus Crime Control and Safe Streets Act of 1968

Title III, as amended by the Electronic Privacy Communications Act of 1986, governs all interception of electronic communications conducted by federal law enforcement investigators.[56] Before Carnivore is granted installation permission pursuant to a Title III investigation, the FBI must be pursuing a recognized Title III suspect and usage of Carnivore must comply with the Title III procedural requirements.

a. Subject Must be a Recognized Title III Suspect

To begin the Title III Carnivore inquiry, the FBI must be pursuing a

49. *Id*.
50. *See id.*
51. *Id*.
52. *Id*.
53. *Id*.
54. *See* Delaney, *supra* note 42.
55. REVIEW, *supra* note 3, § 3.1.
56. Electronic Privacy Communications Act, 18 U.S.C. §§ 2510-2522 (2000).

suspect believed to have committed a recognized crime under Title III.[57] Title III exhaustively enumerates these crimes, which are limited to felonies such as murder, kidnapping, child molestation, felony violations of obscenity, crimes against national security, robbery, malicious mischief, extortion, organized crime, and narcotics offenses.[58] If the suspect is not pursued for violation of an enumerated crime, Carnivore cannot be utilized.

b. Case File and Judicial Order Must Satisfy the Act's Requirements

If the subject is a statutorily recognized suspect, Title III still mandates the satisfaction of two procedural requirements before a judge can approve Carnivore's deployment. To satisfy the first requirement, the FBI, in its application for an order, must specify and particularize: (1) facts demonstrating probable cause that statutorily recognized offenses are being committed; (2) a description of the nature and location of the facilities where the communications will be intercepted; (3) a description of the communications sought to be intercepted; and (4) the identity of the suspect.[59] Finally, the FBI must indicate that normal investigative procedures have been insufficient to obtain the desired information, *e.g.*, due to danger or technology restrictions.[60]

If the first requirement is satisfied and the federal judge grants the wiretap request, the judge's wiretap order must contain the following to satisfy the second requirement: (1) the identity of the person whose communication is to be intercepted; (2) the nature and location of the communications facilities to which interception is granted; (3) a particular description of the type of communication sought to be intercepted along with a statement of the particular alleged offense; (4) the identity, and authorizing officer, of the agency authorized to intercept the communications; (5) the authorized time period for interception,[61] which cannot exceed thirty days[62] and which should include "a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained;"[63] and (6) an order requiring the FBI to minimize the interception of communications not

57. 18 U.S.C. § 2516.
58. *Id*. § 2516(l).
59. 18 U.S.C. § 2518(1).
60. Delaney, *supra* note 42.
61. 18 U.S.C. § 2518(4)(a)-(e).
62. *Id*. § 2518(5).
63. *Id*. § 2518(4)(e).

authorized to be intercepted under part three of the order.[64]

2. Federal Pen-Trap Statute

The Federal Pen-Trap Statute provides a less intrusive mechanism for wiretapping than its Title III counterpart, and allows law enforcement to monitor e-mail in two ways: "trap-and-trace" monitoring and "pen-register" monitoring (together, "pen-trap devices").[65] Trap-and-trace e-mail monitoring decrypts the identification of every account attempting to communicate with the suspected felon, whereas pen-register e-mail monitoring tracks all outbound communication from the suspected felon's account.[66] Unlike Title III monitoring, pen-trap devices do not inquire into the content of the communication, or substantively record communication.[67] Instead, the FBI uses the pen-trap statute to obtain destination and origination information of incoming and outgoing e-mail messages. Typically, an e-mail pen-register order will only authorize collection of the source ("FROM field"), destination ("TO field"), date, time, user account address, and duration of the message.[68]

Although a pen-trap device can only be deployed pursuant to a court order,[69] the information it can gather is inherently less intrusive than that gathered under Title III. Accordingly, the requirements to obtain a pen-trap order are less stringent than for Title III wiretap interceptions.[70] Nevertheless, the pen-trap order authorizing collection of Carnivore-monitored e-mail must specify the identity of the person with the e-mail address, the identity of the person under investigation, and the offense for which the person is under investigation.[71] Further, the FBI is precluded from inquiring delving into the e-mail's subject line and "re" information.[72]

64. *Id*. § 2518(5).

65. 18 U.S.C. §§ 3121-3124.

66. Robert Graham, *Carnivore FAQ (Frequently Asked Questions)* § 3.1, *at* http://www.robertgraham.com/pubs/carnivore-faq.html (Oct. 6, 2001).

67. *9/6/00 Hearing*, *supra* note 4, at 37 (statement of Donald Kerr).

68. *Id.*

69. *Id*.

70. 18 U.S.C. § 3121(a). Notice that applications for the usage of pen-trap devices may be made by any federal government attorney or state investigative or law enforcement officer. Also, no special authorization is required. *Id*. § 3122. In fact, any court fulfilling jurisdictional requirements is required to issue a pen-trap order if the court finds that information expected to be obtained would be relevant to an ongoing investigation. *Id*. § 3123(a).

71. *See id.* § 3123(b). Although the language of the statute does not explicitly state that these procedures apply to electronic communication and no case law exists to validate such an application, there have been no constitutional challenges to the FBI's usage of pen-trap devices in such a manner.

72. *9/6/00 Hearing*, *supra* note 4, at 37 (statement of Donald Kerr).

Any law enforcement agent that uses a pen-trap device without first acquiring a court order is subject to a fine and up to a year in prison.[73]

3. The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) allows the federal government to monitor electronic communication of foreign powers, and agents of foreign powers located in the United States, to obtain foreign intelligence information.[74] If the focus of the surveillance is not a U.S. citizen, no court order is required and only authorization from the Attorney General is necessary.[75] If the subject of surveillance is a U.S. citizen, the usage of Carnivore must be approved through a special foreign intelligence surveillance court that determines its appropriateness by using standards analogous to those used to obtain permission under Title III.[76]

IV. METHOD OF OPERATION

Relative to the most technologically current computer hardware, Carnivore is considered, by experts, to be systemically unsophisticated; the computer program has been around since 1992.[77] The system configuration is comprised of: a four- to eighteen-gigabyte hard drive with 128-megabytes of RAM; a Pentium III processor; Windows NT or Windows 2000; and a two-gigabyte Jaz drive—all of which can be readily purchased through a local computer retailer.[78]

There are, however, fundamental differences between Carnivore and the typical "off-the-shelf" system. First, the Carnivore computers exclude a TCP/IP identifier, which virtually obviates the possibility of being hacked into by a network user, and include "network isolation devices," which prevent the computer from transmitting data in the unlikely event that hackers hijack Carnivore's system.[79] Secondly, the Carnivore computers are equipped with a hardware authentication device, which prevents ISP personnel or law enforcement agents from obtaining post-programming access to the contents of the computer without producing visible signs of forced entry.[80]

73. 18 U.S.C. § 3121(d).
74. *See* 50 U.S.C. § 1802 (1994).
75. *Id*. § 1802(a)(1).
76. *See id.* § 1805(b).
77. Graham, *supra* note 66, § 1.5.
78. *Id*.
79. *Id*.
80. *Id*.

A. Background of Internet Communication

Unlike telephones, which work through a circuit-switching process that allocates one phone line for use between the two communicating parties, the Internet delivers messages (e-mail) via a process known as "packet switching."[81] Packet switching refers to a transmission process in which entire messages are divided into tiny packets of information before they are sent.[82] These packets consist of binary code—simply a numeric stream of many "0s" and "1s" that will eventually be reorganized into a readable message.[83] After the packets are divided, they are transmitted separately, and can follow one of thousands of different possible routes before passing through an ISP and on to its desired destination.[84] After all the packets forming the message arrive at the destination, they are recompiled into the original message.[85]

B. Carnivore's Installation and Filtering: A Process of Stages

After the FBI receives judicial approval to initiate Carnivore's setup, the physical deployment and information retrieval process begins. Specifically, the process consists of four stages: installation, filtration, segregation, and collection.

1. Stage One: Installing Carnivore

After the FBI has obtained an authorization to capture information pursuant to one of the three previously mentioned statutes, they will turn to the suspect's ISP to determine if the ISP has the technology to comply with the court order.[86] If the ISP can comply, Carnivore is not used. If the ISP cannot, the FBI engages in a cooperative effort with the ISP technicians to position Carnivore in the network where the suspect's communication packets can be isolated.[87]

81. Webopedia, *Packet Switching*, *at* http://www.webopedia.com/TERM/p/packet_switching.html (last modified May 1, 2001).

82. *See id.*

83. *See 9/6/00 Hearing*, *supra* note 4, at 37 (statement of Donald Kerr).

84. Marilyn McKinley Parrish, *The Internet for Church Librarians*, *at* http://www.mph.org/plan/planspr96b.htm (April-June 1996).

85. Systemnews, *Digital Journey, The Human Origins of the Internet*, *at* http://sun.systemnews.com/system-news/jobdir/submitted/2002.02/5154/5154.html (last visited March 12, 2002).

86. 9/6/00 Hearing, *supra* note 4, at 37.

87. *Id*.

2. Stage Two: Initial Filtering

Carnivore's first action is to "take a glimpse" of the ISP's traffic, which includes traffic from non-targeted individuals, and filter the packets of "0s" and "1s" at the ISP's designated speed, usually 40 mega-bits per second or much higher.[88] Carnivore filters this binary code in "real time," which means it processes at least 40 million "0s" and "1s" each second, depending on the speed of the packets.[89] This initial filtration serves to determine whether the suspect's identifying information, in accordance with the court order, is present in the binary code.[90] Carnivore essentially takes a picture each second, searching for the suspect's information. If the suspect's information is not present, every packet of information is vaporized, and not collected, stored, or saved, and Carnivore analyzes the next second's data.[91] If the suspect's information is present, Carnivore proceeds to Stage Three.[92]

3. Stage Three: Segregating the Suspect's Information

If Carnivore detects the suspect's identifying information, the packets of the suspect's communication are segregated for additional filtration and storage.[93] This filtration and storage is effectuated entirely within the Carnivore device, without known FBI or ISP technician interference.[94]

4. Stage Four: Following Collection Orders

After the Stage Two filtration and Stage Three segregation occurs, the suspect's information is filtered again to comport with the court order.[95] Carnivore checks its programming to see what it should filter and collect for processing, as determined by court order, and discards nonretrievable information.[96] For example, Carnivore determines whether the collection is for purposes of Title III, pen-trap collection, or the Foreign Intelligence Surveillance Act. Once again, this process is done entirely within Carnivore, without known FBI or ISP technician interference.[97]

88. *Id*.
89. *Id*.
90. *Id*.
91. *Id*.
92. 9/6/00 Hearing, *supra* note 4, at 37.
93. *Id*.
94. *Id*.
95. *Id*.
96. *Id*.
97. *Id*.

V. PRIVACY CONCERNS

Since its inception, Carnivore has been scrutinized as an over-infringing device that "devours" the privacy rights of every non-targeted individual whose information passes through the system. While activist groups and individuals have verbally denounced Carnivore and have established websites[98] to collaboratively oppose its use, the two most prominent opponents are the American Civil Liberties Union ("ACLU") and the Electronic Privacy Information Center ("EPIC"). Many of their concerns are technical in nature, rooted in Carnivore's general operation—they want to know the system's capabilities, what goes on inside the "black box," and whether the installation could expose or cause ISPs to malfunction or crash.[99]

The DOJ recognized this widespread ignorance and distrust of the system, and consequently contracted with the IIT Research Institute and the Illinois Institute of Technology Chicago-Kent School of Law ("IITRI") to address the technical concerns of the system.[100] However, the IITRI "expressly declined to address the significant legal issues surrounding the use of the Carnivore system."[101] As a result, EPIC, the ACLU, and other privacy advocates have articulated three continuing legal concerns: (1) the possibility that Carnivore conducts broad sweeps over the ISP's transmissions; (2) Carnivore's ability to transmit more than the suspect's data violates the Fourth Amendment; (3) the lack of FBI personnel accountability for Carnivore further creates a concern for over-collection through agent impropriety.[102] Until these issues have been sufficiently resolved, privacy advocates urge the FBI to suspend Carnivore deployments.[103]

A. Concern #1— Can Carnivore Spy on Every Internet User?

Many privacy advocates are concerned that Carnivore collects more

98. *See, e.g.*, *Stop Carnivore NOW*!, *at* http://www.stopcarnivore.org (last visited Jan. 26, 2002).

99. Mario Figueroa, *Carnivore—Diagnostic Tool or Invasion of Privacy*?, *at* http://rr.sans.org/legal/carnivore.php (Sept. 1, 2000).

100. REVIEW, *supra* note 3. The report analyzed the process assessment, system architecture, software source code, and laboratory tests. *See id.* §§ 2-1, 2-3. However, the nature of IITRI's findings enabled them to answer questions that were not strictly technical. *See id.* § 4-9.

101. E-mail from David L. Sobel, General Counsel, EPIC, to Carnivore Review Panel, U.S. Department of Justice, *at* http://www.epic.org/privacy/carnivore/review_comments.html (Dec. 1, 2000) [hereinafter *EPIC Review*].

102. *See id.*

103. *Id*.

data than is allowed by court order. They fear that Carnivore can read the content of all individuals' e-mails over an ISP.[104] In fact, David Sobel, General Counsel for EPIC, stated that Carnivore could easily conduct a "broad sweep" of transmission data.[105]

If so programmed, the FBI concedes that Carnivore could conceivably be able to collect and archive all unfiltered traffic from an extremely small ISP.[106] Such a notion will probably remain strictly theoretical, however, because a court order would never allow for such a broad sweeping collection, regardless of ISP size.[107] But even if a court granted such an order, there is not a realistic possibility that such a sweep would occur because of Carnivore's intrinsic storage limitations.

> Carnivore does not have nearly enough power 'to spy on almost everyone with an e-mail account.' In order to work effectively, it must reject the majority of packets it monitors. It also monitors only the packets traversing the wire to which it is connected. Typically, this wire is a network segment handling only a subset of a particular ISP's traffic.[108]

However, withstanding intentional mis-programming, which will be discussed in Part V.C., this issue is moot because a court would never authorize such a broad sweep.

When programmed for a Title III or FISA collection, Carnivore provides the FBI with no more information than is permitted by the court order.[109] In cases involving a pen-trap order, however, Carnivore does collect "more than would be permitted by the strictest possible construction of the pen-trap statute."[110] The over-collected data is essentially useless to the FBI. Instead of only collecting the contents from the "TO" and "FROM" fields, Carnivore also replaces characters in the other fields, for example putting an "X" in the subject line.[111] Therefore, the FBI could ascertain the length of the subject line by counting the number of "Xs." Aside from these character replacements in pen-trap mode, "there was no evidence of over-collection during any of the tests."[112]

104. *Stop Carnivore NOW*!, *at* http://www.stopcarniovre.org/what_can_carnivore_do.htm (last visited Jan. 26, 2002).

105. *See EPIC Review*, *supra* note 101.

106. Letter from Donald Kerr, Director, FBI, to Senator Patrick J. Leahy, Senate Comm. on the Judiciary (Jan. 23, 2001), *available at* http://www.epic.org/privacy/carnivore/kerr_letter.html.

107. *Id*.

108. REVIEW, *supra* note 3, § ES.5.

109. *Id*. § 4.3.1.

110. *Id*. § 4.2.3.

111. *Id*.

112. *Id*.

To further allay the concern of collecting more data than authorized, Carnivore has been configured to "err on the side of caution." When programmed in accordance with the court order that unequivocally prescribes the programming, Carnivore provides investigators with less information than can legally be obtained if a suspect's privacy right can be potentially infringed.[113]

B. Concern #2 – Is Carnivore Eating the Fourth Amendment?

Carnivore's purpose is to capture criminal suspects' Internet transmissions, notwithstanding the suspects' knowledge or consent. That purpose necessarily results in the clandestine acquisition of non-suspects' electronically transmitted data. Consequently, many privacy advocates question whether Carnivore comports with the Fourth Amendment when processing both the non-suspects' data as well as the suspects' information.

1. Non-Suspects' Fourth Amendment Rights

EPIC and other privacy advocates claim that much of the controversy surrounding Carnivore is derived from its ability to access and process a great deal of ISP transmissions.[114] This concept particularly concerns the organization because users not named in the court order and not targeted by the FBI have their transmissions processed through Carnivore.[115] "It is this unique aspect of Carnivore that gives rise to fundamental privacy risks,"[116] and creates a Fourth Amendment concern because the court order is a warrant for collection of the suspect's data, not the non-targeted individual's data.[117]

The central purpose of the Fourth Amendment is to protect the public's privacy and security from arbitrary governmental invasion.[118] Accordingly, law enforcement must obtain advance judicial approval of searches and seizures by obtaining a warrant.[119] While warrants are preferred, there are certain undefined, limited circumstances that allow law enforcement to conduct searches without probable cause or individualized suspicion.[120] A government action falls within these limited circumstances

113. *Id*. § 4.3.1.
114. *See EPIC Review*, *supra* note 101.
115. *Id*.
116. *Id*.
117. *See id.*
118. S. Dakota v. Opperman, 428 U.S. 364, 377 (1976) (Powell, J., concurring).
119. Terry v. Ohio, 392 U.S. 1, 20 (1968).
120. Chandler v. Miller, 520 U.S. 305, 308 (1997) (citing Treasury Employees v. Von Raab, 489 U.S. 656, 668 (1989)).

when the privacy interest implicated by the search is minimal, and the action serves an important governmental interest that would not be promoted if individualized suspicion of each non-targeted subject is required.[121]

Assuming non-targeted individuals have a privacy expectation in their packets of information, the standards for warrantless intrusions clearly permit Carnivore's processing. Since Carnivore is used only to pursue felons, the government obviously has an important interest in their apprehension. Non-targeted suspects have only a minimal privacy interest in their packets of information because each packet contains very little information and the intrusion—a brief, one-second processing of data—is negligible. If, however, the government opts to collect, store, and analyze a non-targeted subject's information, there is a much lower governmental interest because the non-targeted subject is not a criminal suspect, and there exists an obvious increase in the degree of intrusiveness because the packets are being analyzed. Thus, the evidence would be barred from usage by the exclusionary rule.[122] But so long as Carnivore only processes the non-targeted subject's information, the system does not violate these non-targeted subjects' Fourth Amendment rights.

2. Targeted Suspects' Fourth Amendment Rights

Privacy advocates also express concern for the suspect's Fourth Amendment rights when Carnivore is used pursuant to a pen-trap order.[123] Since pen-trap devices are less intrusive than Title III interceptions, acquiring a suspect's information does not require a showing of probable cause. Thus, advocates argue the collection of the "TO" and "FROM" fields constitutes an unjustified search and seizure of the suspect's data.[124] This argument fails, however, because the Supreme Court has determined that a suspect does not have a reasonable expectation of privacy in the information collected pursuant to a pen-trap order.[125] Even if the suspect had a reasonable expectation of privacy, the Fourth Amendment challenge would fail due to the same balancing test applied above for non-targeted subjects: the governmental interest of solving the particular crime far outweighs the minimal privacy interest the suspect has in the "TO" and

121. Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 624 (1989).

122. Weeks v. United States, 232 U.S. 383 (1914).

123. *Stop Carnivore NOW!*, *Why Carnivore is Bad for You (Reason # 1)*, *at* http://stopcarnivore.org/whyitsbad/reason1.htm (last visited Jan. 29, 2002).

124. *Id*.

125. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979). Although this case addressed telephonic interception, the same reasoning can be applied to e-mails because essentially the same information is obtained.

"FROM" fields.

C. Concern #3 – Who's Spying on the Spiers?

The purpose of Carnivore is to process ISP transmissions in strict adherence to the empowering court order, which allows gathering and storing the suspect's data, but mandates instantaneous purging of a non-suspect's data. Theoretically, this gathering and purging is effectuated after the Carnivore box is programmed in *exact* accordance with the court order. Since theory is not reality, privacy advocates worry that Carnivore is susceptible to programming in violation of the court order.[126] This is possible because Carnivore lacks "audit functions," which results in the absence of an individual user accountability mechanism.[127]

> Auditing is crucial in security. It is the means by which users are held accountable for their actions. There is no auditing in Carnivore. The Carnivore version 1.3.4 collection computer is always logged in as the "Administrator" rather than using individual user IDs. This Administrator log-in means that every user of the system has full control over all the resources of the system . . . Since everyone with Administrator access has full control, there is nothing to prevent someone from using a Hex editor or other tool to [access Carnivore's advanced filter setting menu]. Therefore, it is not possible to determine who, among a group of agents with the password, may have set or changed filter settings.[128]

This deficiency is Carnivore's most troubling attribute. Without individual user accountability, there exists no system-intrinsic disincentive for FBI agents to unlawfully program Carnivore. A simple click of a mouse (whether intentional or unintentional) changes Carnivore's configuration settings from a pen-trap collection to a full collection under Title III.[129] "There is no mechanism for detecting or minimizing the likelihood of such an unintentional setup error."[130]

The implementation of an auditing system would almost certainly reduce both intentional and unintentional violations; it may cause a potentially unintentional violator to more carefully select the proper setting, and may cause a corrupt FBI agent to abate intentions of mis-programming.

126. *See EPIC Review*, *supra* note 101.

127. REVIEW, *supra* note 3, § 4-9.

128. *Id*. § 4.2.4.

129. *Id*. § 4.3.3. There is also the possibility of improperly setting Carnivore to comply with the court order. *Id.* However, this "chance of error . . . is low because of the large number of individuals involved in framing the court order and determining the feasibility of its implementation by Carnivore." *Id*.

130. *Id*.

Nevertheless, until an auditing system is implemented, mis-programming can occur, resulting in collection of more data than allowed by the court order.[131] Although this excessively collected data may be subject to judicial suppression, privacy advocates could claim the mis-programming infringed on the subject's privacy right and the possibility remains of unlawfully initiating an investigation based on information learned as a result of the over-collection. It is natural to assume that privacy advocates would be unwilling to rely on the FBI's assurance that any information inadvertently gathered beyond the scope of the court order is disposed of in conformity with federal statutory and constitutional law.

Quite simply, there need to be safeguarding mechanisms in place to counteract Carnivore's systematic pitfalls. Fortunately, federal statutes and rules exist that not only protect subjects who have fallen victim to over-collection, but also deter intentional and unintentional mis-programming.

1. Title III and FISA Post-Collection Judicial Review[132]

Both Title III and FISA provide for judicial oversight when Carnivore is used. Specifically, Title III mandates the recording of the contents of the electronic communication intercepted by Carnivore.[133] Further, "[i]mmediately upon the expiration of the period of the order, . . . such recordings shall be made available to the judge issuing such order and sealed under his directions."[134]

FISA provides similar oversight language when the subject is a United States citizen, but adopts a judicially permissive, though not mandatory, review.[135] The statute provides in relevant portion:

> At or before the end of the period of time for which electronic surveillance is approved by an order . . . the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.[136]

Thus, each Title III and FISA order-issuing judge has the opportunity to compare the captured information with the court order to independently determine the legality of the obtained information, and accordingly

131. *Id.*

132. As stated, the FBI receives less information when Carnivore is configured for a pen-trap collection than for a Title III or FISA collection. Therefore, mis-programming from a Title III or FISA collection to a pen-trap collection seems highly unlikely because more information is retrievable by following the court order.

133. 18 U.S.C. § 2518(8)(a).

134. *Id*.

135. 50 U.S.C. § 1805(e)(3).

136. *Id*.

suppress all deemed "over-collection."

2. Federal Rule of Evidence 901

Evidence must be authenticated to be admissible against a defendant at trial.[137] "[This] requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[138] To comport with section 901, Carnivore appends to an event file for each collection in which the filter configuration is used.[139] This information makes explicit to the FBI, judge, and jury what mode controlled Carnivore's use during the collection process and what it was programmed to collect.[140] Since over-collection of the suspect's transmissions would violate the court order and the defendant's Fourth Amendment rights, the trial judge could apply the exclusionary rule to suppress illegally seized information.[141]

3. Criminal and Civil Liability; Employment Termination

Any FBI agent that engages in the illegal, unauthorized conduct of electronic surveillance commits a federal criminal offense punishable by imprisonment for up to five years, a fine, or both.[142] In addition, an individual victimized by unlawful over-collection or interception can recover damages in a civil action including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.[143] Although the culpable FBI agent may not be personally liable for damages, the impending disciplinary action for causing the government liability certainly serves as a deterrent. In fact, every law enforcement agent who illegally conducts electronic surveillance is subject to immediate termination.[144]

VI. CONCLUSION

Internet technology has evolved exponentially over the past few years, and the future will certainly continue to realize the same growth. The accessibility to such an immense audience, coupled with a criminal's ease

137. FED. R. EVID. 901.
138. *Id*.
139. *9/6/00 Hearing*, *supra* note 4.
140. *Id*.
141. Weeks, 232 U.S. 383.
142. 50 U.S.C. § 2511(4)(a).
143. *Id*. § 2520.
144. *9/6/00 Hearing*, *supra* note 4.

of anonymity, requires an approach to accommodate the growing threats made possible by the Internet.[145] Carnivore represents a permissible and responsible approach. It enables law enforcement to take one small step to level a playing field currently dominated by criminals who can routinely break the law by using an extremely evasive and criminally propitious medium.

We live in a world where criminals can remain undetected or vanish with the mere click of a mouse. Terrorists, whether foreign or U.S. citizens, are undoubtedly plotting to bomb more American structures with the intent of producing results like those witnessed on September 11th or in Oklahoma City. Pedophiles are pursuing and encroaching on innocent children every day by assuming the most clandestine identities to manipulate the child's every unsuspecting move. The governments of foreign countries are deploying intelligence teams to crack the computer codes that harbor our most important resources—such as our electrical and water supplies, gas and oil reserves, and telecommunications—to exploit our vulnerabilities and to potentially cause catastrophic and deadly results. College students are writing computer viruses solely for the thrill of destroying others' computer files. Although these hypothetical situations seem disconnected in nature, they all share a commonality—the use of electronic communication to facilitate their collusive, maniacal acts of depravity.

The government inevitably faces a "Catch 22" when deciding how to address these types of cyber criminals. If it uses investigative and surgical methods such as Carnivore, privacy advocates criticize the action as overly invasive of privacy rights. If it fails to pursue every avenue to eliminate potential threats, advocates for crime control criticize the lack of action as irresponsible policing and a failure to serve the interests of societal welfare. Unfortunately, no governmental action will ever be uniformly supported. Therefore, the government should initiate only those programs that adhere to the statement offered in this Note's first sentence—act in the interests of security while maintaining the utmost possible level of freedom. Carnivore successfully furthers this goal by increasing security while not compromising freedom.

The manner in which Carnivore collects transmissions is abstractly analogous to a law-enforcement roadblock, instituted to search for an escaped convict, that stops every vehicle (packet) traveling down a certain road (ISP). If law enforcement is not 100 percent certain the traveler is the convict (targeted suspect), the traveler is processed through the roadblock

145. *IFCC*, *supra* note 30.

(Carnivore) and continues to the intended destination. If law enforcement is 100 percent certain, however, the traveler is detained. Privacy concerns are alleviated when considering this entire electronic "roadblock" is nondiscretionary in that decisions are made within the confines of the acutely accurate Carnivore system, and not by a human police officer, who, even if the paradigm example of objectivity, is still fraught with fallibility.

This is not to say Carnivore is perfect. Its lack of individual accountability, as well as the potential to accidentally mis-program the device, are flaws that should be remedied. As technology-based crime increases, however, so does society's need to embrace governmental action aimed at safeguarding society from this increased threat facilitated through electronic communication.

With FBI and DOJ internal policy to bureaucratically determine whether Carnivore should be used; Title III, Pen-trap, and FISA statutory prescriptions; judicial oversight coupled with federal rules to deter unlawful electronic communication interception; and continued necessary pressure from privacy advocates, Carnivore is an appropriate, prudent, and necessary law enforcement mechanism that balances the values of freedom and security that predicate and underlie this Note.