Roger Williams University Law Review

Volume 7
Issue 1 *Symposium: Information and Electronic Commerce Law: Comparative Perspectives*

Article 7

Fall 2001

FBI's Carnivore: Is the Government Eating Away Our Right of Privacy?

Patricia K. Holmes
Roger Williams University School of Law

FBI's Carnivore: Is the Government Eating Away Our Right of Privacy?

INTRODUCTION

With the birth of the Internet has come a virtual reformation of how human society communicates. The exact number of Internet users is nearly incalculable, but recent assessments estimate that nearly 300 million people worldwide are currently online.[1] These users can travel relatively freely among the millions of currently active Internet sites.[2] The growth of this communications medium in the last decade has been tremendous, and promises to continue at such a pace. The United States Department of Commerce has reported that less than 40 million people worldwide had access to the Internet in 1996.[3] This number jumped to more than 100 million people by the end of 1997.[4] Further research by the Department has indicated that the number of people and businesses using the Internet doubles every 100 days.[5] Thus, the Internet presents unprecedented opportunities for global communications and commerce. However, it also poses dramatic risks to personal privacy. Every day Americans use the Internet to access and transfer vast amounts of private data. From electronic mail and business transactions to shopping habits, web surfing profiles can reveal detailed blueprints of how people live.[6] As more of our lives are conducted online and more personal information is transmitted and stored electronically, the result has been a massive increase in the amount of sensitive data available to inter-

1. *See* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 Mich. Telecomm. Tech. L. Rev. 61, 63 (1999).

2. *See id.*

3. *See* Thomas T. Reith III, *Consumer Confidence: The Key To Successful E-Commerce In The Global Marketplace*, 24 Suffolk Transnat'l L. Rev. 467, 486 n.3 (2001).

4. *See id.*

5. *See id.*

6. *See Carnivore's Challenge to Privacy and Security Online: Hearings on Carnivore Before the House Judiciary Subcomm. on the Constitution*, 106th Cong. (2000) [hereinafter *Carnivore's Challenge*] (statement of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology).

ested third parties, including the government.[7] The question thus presented is whether our government has taken advantage of this availability. Although not conclusive, some evidence suggests that the utilization of electronic surveillance for monitoring criminal activity has practically exploded over the past decade, arguably replacing more traditional investigatory tools.[8] Current data indicates that this pace is unlikely to diminish. The FBI alone estimates that over the next decade, given planned improvements in the digital collection and analysis of communications, its requests for electronic surveillance orders will increase 300 percent.[9] It appears that these planned improvements, as well as additional surveillance requests, may well be underway.

During Congressional hearings in April, 2000, Robert Corn-Revere, an Internet and communications lawyer in Washington, D.C., first divulged evidence of the existence of "Carnivore," an electronic surveillance device developed by the FBI.[10] Responding to concerns from various privacy groups and others, former Attorney General Janet Reno ordered that an independent technical review of the system be completed by December 8, 2000, in order to substantiate Carnivore's compliance with both constitutional provisions and federal statutory wiretap laws.[11] The review, completed by the IIT Research Institute (IITRI), a division of the Illinois Institute of Technology, essentially found the system to be legally compliant and determined most concerns over invasion of individual privacy were unsupported.[12]

Despite winning a favorable review by the university, the Carnivore device continues to raise strong concerns about privacy and the legal limits of government surveillance.[13] Many computer experts believe that the scope of the study was too narrow, and that serious technical questions remain about the ability of Carnivore to satisfy Constitutional and statutory thresholds for online secur-

---

7. *See id.*
8. *See id.*
9. *See id.*
10. *See* John Hall, *Privacy Beginning To Be A Top Issue*, Rich. Times Dispatch, July 16, 2000, at F2.
11. *See* Frank James, *U.S. Seeks University Experts to Review FBI's E-Mail Probes*, Chi. Trib., Aug. 25, 2000, at N20.
12. *See Institute's Report on Carnivore Causes Uproar Among Critics*, 4 Telecomm. Indus. Litig. Rep. 12 (2000).
13. John Schwartz, *Computer Security Experts Question Internet Wiretaps*, N. Y. Times, Dec. 5, 2000, at A16.

ity and safety.[14] This note explores some important legal issues raised by the operation of Carnivore, including a brief discussion of the adequacy and conclusiveness of the IITRI analysis as it pertains to each issue.

Part I of this comment provides a basic assessment of the operational aspects of the Carnivore system. Part II explores the fundamental legality of the Carnivore device from a Constitutional perspective. Part III examines Carnivore's likely compliance with current federal statutory wiretap laws as they have been interpreted and applied by the judiciary. Finally, the conclusion offers comments and proposals for how to strike a balance between privacy interests and government objectives.

I. Operational Overview of Carnivore

As an initial matter, to understand the legal implications of utilizing a surveillance system like Carnivore, one must understand its basic operational capabilities. Although a fully detailed description of how Carnivore works has not been made available to the public, the general premise of the system is as follows:

Carnivore is a Windows NT based software program that operates upon connection to a network access point provided by a participating Internet Service Provider (ISP).[15] To install the device, the FBI must present a valid court order to intercept electronic communications of a target suspect.[16] The court order may authorize capture of an entire communication, or it can be limited to addressing or routing information.[17]

The FBI and the ISP install Carnivore at a point on the ISP's network where data from a suspect named in the court order is located.[18] As a technical matter, the FBI has conceded that the ISP cannot provide an access point that can limit the Internet traffic flowing through the Carnivore device to only that of the named

14. *See id.*

15. *See The Carnivore Controversy: Hearings on Electronic Surveillance and Privacy in the Digital Age Before the Senate Comm on the Judiciary*, 106th Cong. (2000) [hereinafter *Hearings 1*] (statement of Sen. Patrick Leahy).

16. *See Big Sister – Janet Reno; An Orwellian Carnivore*, Cincinnati Enquirer, Sept. 13, 2000, at A10.

17. *See Hearings 1*, *supra* note 15 (statement of Sen. Patrick Leahy).

18. *See id.*

suspect.[19] Because the Internet operates by breaking electronic transmissions down into "packets" of data that are reassembled at a destination point, Carnivore must necessarily separate or filter the target suspect's electronic transmissions from other Internet traffic as it flows through the device.[20]

Once the named suspect's data is separated from other traffic, Carnivore routes the information to a second filter.[21] As the data travels through the second filter, the system makes a copy of all of the information and sends the original data to its desired destination.[22] On the basis of authorized search parameters, Carnivore segregates relevant and irrelevant data.[23] Copied data that is not relevant to the FBI investigation is purged.[24] Traffic that is relevant to the investigation and defined under the court order is sent to an archive system for permanent storage at an FBI facility.[25]

With these functional characteristics in mind, the fundamental legality of the Carnivore device can be examined from both a constitutional and federal statutory perspective. Because this comment focuses only on the inherent legitimacy of the system, assuming proper use, these analyses will be made ignoring any possibilities for misuse of the system on the part of the FBI.

II. CONSTITUTIONAL ANALYSIS

A. *Constitutional Issues Presented*

The Fourth Amendment to the United States Constitution provides that:

> [T]he 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,

---

19. *See* James X. Dempsey, *Does Carnivore Go Too Far?*, Network World, Oct. 30, 2000, at 73; *see also* Dan Eggen & David A. Vise, *More Questions Surface about FBI Software; Wiretap Program Can Archive All Internet Communications*, Nov. 18, 2000, at AO3.

20. *See Hearings 1*, *supra* note 15.

21. *Id.*

22. *See The Carnivore Controversy: Hearings on Electronic Surveillance and Privacy in the Digital Age Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter *Hearings 2*] (statement of Donald Kerr, Asst. Director, Federal Bureau of Investigation).

23. *Id.*

24. *Id.*

25. *See Hearings 1*, *supra* note 15.

> 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.[26]

The traditional judicial interpretation of a Fourth Amendment search of persons, houses, papers and effects required some type of physical invasion on the part of the government.[27] However, the scope and interpretation of Fourth Amendment application was broadened in 1967 when the Supreme Court of the United States determined that a search, as defined by the Amendment, could be accomplished via government orchestrated electronic surveillance.[28] Thus, the constitutional implications created by the utilization of the Carnivore surveillance device must be analyzed and reviewed in such context. The primary Fourth Amendment concerns raised by Carnivore can be narrowed to two issues.

Issue 1 – Warrantless Search of Persons Not Named In Court Order

Because the FBI has conceded Carnivore's inability to isolate a target suspect's transmissions as they flow through its first filtering point,[29] is the device able to conduct an unauthorized, warrantless search of communications of persons not subject to the authorized surveillance?

Issue 2 – General Warrant Search of Target Suspect

Because the FBI has stated Carnivore copies and reviews, in some manner, all electronic transmissions attributable to a suspect named in a court order,[30] does the device conduct a general search of the suspect's electronic communications not specified in the order?

1. *Examination of Fourth Amendment Concerns*

The FBI has established that the Carnivore device reads certain "addressing" and "transactional" information for transmis-

26. U.S. Const. amend. IV (emphasis added).

27. *See* Olmstead v. United States, 277 U.S 438 (1928); *see also* Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment:* Knotts, Karo *and the Questions Still Unanswered*, 34 Cath. U.L. Rev. 277, 286 (1985).

28. *See* Fishman, *supra* note 27, at 395.

29. *See* Dempsey, *supra* note 19, at AO3.

30. *Id.*

sions flowing through Carnivore's first filter point.[31] Much of this information is not authorized in a valid court order and has no connection to the approved purpose of the electronic surveillance.[32] The IITRI report seems to confirm that when Carnivore is used for trap-and-trace surveillance to intercept simply the "to" and "from" information on an e-mail, the software gives investigators more information than may be permitted by the court order, including the length of e-mail messages.[33]

Carnivore intercepts such material in one of two ways. First, the device may receive the data without examining the actual body of the transmission.[34] Second, the system may view the addressing information only in conjunction with the body of the communication.[35]

As an initial matter, an individual raising a Fourth Amendment challenge to a government search must show that the actions of the government infringed upon his *legitimate expectation of privacy*.[36] If the individual does not establish this reasonable expectation, no Fourth Amendment search, and therefore violation, has occurred. The judicially created test for determining whether an individual has a reasonable expectation of privacy in an electronic communication is a two-prong application developed in *Katz v. United States*.[37] The first prong of the analysis inquires as to whether the individual has a subjective expectation of privacy in the communication. The second prong focuses on whether society will recognize such expectation.[38] Thus, in order to establish that Carnivore is conducting an invalid warrantless search of information not subject to a court order, both prongs must be satisfied.

Subjective Expectation

Generally, to possess a subjective expectation of privacy, an individual merely has to exhibit that he has some actual desire to

---

31. *Hearings 2*, *supra* note 22.
32. *Id.*
33. Jon Baumgarten, *Official Report on Carnivore Supports E-Mail Surveillance*, 5 Cyberspace Law. 23 (2001).
34. *Carnivore's Challenge*, *supra* note 6.
35. *Id.*
36. *See* Skok, *supra* note 1, at 71.
37. 389 U.S. 347 (1967).
38. *See id.*

keep the communication secluded or away from public access.[39] With respect to most Internet transmissions, electronic mail in particular, one can assume that most people have a strong actual expectation of privacy in the content of messages they send and receive. Safeguards such as login names, passwords and encryption procedures lend credibility to this assumption.

However, the existence of an actual expectation may become less convincing when the communication is what has traditionally been regarded as "addressing" or "transactional" information. The ability of an individual to successfully claim an actual expectation of privacy in electronic addressing and transactional data has been addressed by the Supreme Court on two definitive occasions. In *Smith v. Maryland,*[40] the Supreme Court held that a person "in all probability" does not have an actual expectation of privacy in the telephone digits he dials because he voluntarily conveys such information to a third party, the telephone company.[41] Thus, the individual assumes the risk that such information will be released. Similarly, in *United States v. Miller,*[42] the Court held that an individual has no subjective expectation of privacy in bank records because he freely conveys this information to his bank in the ordinary course of business.[43] The real issue to be addressed here is whether such reasoning is applicable in the Internet arena.

Internet addressing and transactional material is generally either Uniform Resource Locator (URL) data or Internet Protocol (IP) addresses.[44] A URL is the "electronic address" a person types when sending an electronic mail message.[45] "JohnDoe@aol.com" is an example of a URL address. An IP address is a computer's personal identification number that accompanies any electronic transmission that is sent over the Internet from that particular computer.[46] An example of an IP address is 207.226.3.43.

As the Internet has become more and more of a pervasive part of everyday life, some discussion has suggested that a traditional

39. *See* Smith v. Maryland, 442 U.S. 735 (1979).
40. 442 U.S. 735 (1979).
41. *See id.* at 742.
42. 425 U.S. 435 (1976).
43. *Id.* at 442.
44. *See Carnivore's Challenge, supra* note 6.
45. *See* Tim Wyatt, *Secure Shopping*, Dallas Morning News, Apr. 27, 2000, at 3J; *see also* J. Timothy Hunt, *Moving Target*, Nat'l Post, Oct. 1, 2000, at 48.
46. *Carnivore's Challenge, supra* note 6.

analysis, such as that invoked in *Smith* and *Miller*, should not be applied to the Internet forum. The basis for such a proposition is the theory that Internet addressing information, unlike more traditional addressing or transactional material, is much more revealing of content. For instance, if an individual logs onto a particular Website and requests information, literature, etc., the request message will be sent to that particular Website's URL address, or mailbox.[47] Therefore, if a person logs onto "WforPresident.com" and requests information about the presidential campaign, how to donate, etc., this request will be sent to the "WforPresident" Website URL. Unlike telephone digits, which when viewed alone and in the absence of further investigation reveal little if any element of content, a simple Internet message such as this could expressly illustrate a person's political affiliations. In fact, unlike telephone numbers, the interception of URL information can give law enforcement a fairly comprehensive picture of the individual's interests and activities online.[48] The FBI could know what type of books an individual reads, his romantic and artistic interests, and much more.[49] Advocates against the application of traditional reasoning argue that such information is more analogous to a telephone conversation than the digits dialed and thus should receive Fourth Amendment protections.[50]

Substantial evidence of this protective approach makes it plausible that Internet users have an actual expectation of privacy in URL information being intercepted by Carnivore. In fact, many privacy groups are concerned about the potential of Carnivore to receive and record such information.[51] For example, Electronic Privacy Information Center (EPIC) filed a Freedom of Information lawsuit against the FBI in July 2000, requesting release of Carni-

47. *Id.*

48. *See* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 Alb. L.J. Sci. & Tech. 65 (1997).

49. *See id.*

50. *See* Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 Va. L. Rev. 1181, 1201 (1995) (discussing how individuals do not assume the risk that the content of their telephone conversations will be disclosed by a third party (e.g. telephone company)).

51. *See* Michael J. Miller, *The Ever-Expanding Browser*, PC Magazine, Oct. 3, 2000, at 7.

vore's capacity to view such information.[52] The organization was successful in obtaining over 2,000 Carnivore related documents from the Justice Department.[53] However, finding the provided information inconclusive, EPIC filed a motion in the District of Columbia in August, 2001 requesting the deposition of several FBI officials in order to acquire further information regarding the device's ability to retrieve such data.[54] Also, private software companies, in response at least in part to Carnivore's ability to intercept URL information, have developed URL blocking software to prevent such access.[55] Similarly, many such companies have developed, or are in the process of developing less invasive surveillance devices, emphasizing a less intrusive procedure and enhancing privacy protections.[56]

Alternatively, it would seem that a strong argument could reasonably be made in favor of a traditional application of the Court's reasoning in *Smith* and *Miller* with respect to Internet addressing information. Although, very few courts have addressed the applicability of such reasoning to the Internet forum, the courts seem to agree that a traditional approach is appropriate. Proponents of this position state that, like telephone digits and bank records, URL information is voluntarily submitted to third parties. Internet users must realize that they "convey" their URL information since this information must travel through the ISP's network to reach whatever destination is desired.[57] Also, ISPs require Internet users to choose a unique URL address in order to facilitate delivery and transmission of electronic communications, much like a telephone company does when it assigns telephone numbers.[58] The analogy can go further. In *Smith*, the Court determined that

52. *See* Maria Mosquera, *Privacy Group Wants Speedier Carnivore Disclosure*, Techweb News, Aug. 18, 2000.

53. *See Epic Wants A Closer Look At 'Carnivore'*, Nat'l J. Tech. Daily, Aug. 13, 2001.

54. *See id.*

55. *See Accelerated Networks Introduces Secure Multiservice Broadband Access; DSLcon*, Bus. Wire, Sept. 19, 2000.

56. *See* Ann Harrison, *Don't Like Carnivore? How About Altivore? Open Source Code Version of E Mail Sniffer in the Works*, Computerworld, Sept. 25, 2000, at 12.

57. *Smith*, 442 U.S. at 742 (reasoning that an individual realizes that he must convey phone numbers he dials to his telephone company since his call is completed through the company's switching equipment).

58. *See* Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 1610-11 (1999).

the individual voluntarily turns over addressing information to the telephone company and thus assumes the risk that the company will reveal the information to law enforcement. This assumption must be made even though telephone companies normally do not record every number dialed by a customer.[59] Thus, although it is quite probable that an ISP would not record every transmission made, every transmission sent by a user must flow through the ISP's server, and therefore the Internet user must assume the risk that such information will be revealed to law enforcement.[60]

Applying the reasoning of *Smith* and *Miller* to IPs, address information may be an easier position to argue for those supporting the traditional approach. Unlike URL information, IP addresses are numerical, therefore much more like telephone numbers and contain little, if any, content element. However, as with URL data, some effort has been made to protect such information from public access. On October 12, 2000, state representative Gene Green introduced a bill that would prohibit ISPs from placing software "cookies," a type of tracking and identification device, on consumer IP addresses.[61] Also, the American Bar Association has created a new website to help consumers avoid cookies as they shop online.[62]

This practical evidence suggests that individuals communicating over the Internet possess some level of a subjective expectation of privacy in the URL and IP information that Carnivore uses to conduct electronic surveillance. However, the real question in the analysis is whether society is ready to recognize such an expectation.

Society's Expectation

This second, and more difficult prong of the two part *Katz* test to satisfy, addresses whether society is prepared to recognize a reasonable expectation of privacy in the electronic communication. The Supreme Court has stated that society is not willing to recog-

59. *Smith*, 442 U.S. at 735.

60. *See* Skok, *supra* note 1, at 67.

61. *See* Drew Clark, *Privacy: Green Introduces Online Privacy Policy Measure*, Nat'l J. Tech. Daily, Oct. 12, 2000.

62. *See* Sara Hazlewood, *ABA Offers Tips to Help Consumers Protect Themselves on the Internet*, 17 Bus. J. 7 (Dec. 3, 1999).

nize an individual's expectation of privacy unless that expectation is "objectively reasonable."[63]

The *Katz* court defined objective reasonableness in the form of a two-factor application. The first factor addresses whether the individual attempted to deny public access to his communication.[64] The second factor focuses on whether law enforcement has intercepted the content of the individual's transmission.[65]

Katz involved the warrantless recording of a telephone conversation an individual had in a public phone booth that had been bugged by law enforcement officials. Applying these two factors, the Court determined that the individual subjected to the surveillance had an objectively reasonable expectation of privacy in using the phone booth because he had taken steps to *deny public access* to his conversation.[66] Also, law enforcement had full access to the *content* of the individual's phone conversation because they had placed a recording device on the exterior of the booth itself.

In the years since *Katz*, at least with respect to those cases where the Court has been presented with more traditional parameters,[67] the Supreme Court's reasoning and application of determinative factors has been further verified.[68] Where there is little, if any established parameters, such as the Fourth Amendment's application regarding the Internet, the analysis has tended toward a narrow application of the *Katz* reasoning.[69] In fact, the few judicial decisions expressly addressing Internet transmissions have applied the *Katz* reasoning very narrowly.[70] For instance, in *United States v. Charbonneau*,[71] the court held that an individual's expectation of privacy in electronic mail was significantly less than that held in posted mail.[72] Also, in *United States v. Kennedy*,[73] the

63. California v. Greenwood, 486 U.S. 35 (1988).

64. *Katz*, 389 U.S. at 351.

65. *Id.* at 354.

66. *Id.* at 347.

67. *See* Allegra Knopf, *Privacy and the Internet: Welcome to the Orwellian World*, 11 J. Law & Pub. Pol'y 79, 83 (1999) (discussing how the *Katz* framework has applied nicely to situations where society holds conventional notions of public and private places).

68. *See* Minnesota v. Carter, 525 U.S. 83 (1998); *see also* O'Connor v. Ortega, 480 U.S. 709 (1987).

69. *See* Knopf, *supra* note 65, at 83.

70. *See* Skok, *supra* note 1, at 72.

71. 979 F. Supp. 1177 (S.D. Ohio 1997).

72. *Id.* at 1184.

court established that society would not recognize an expectation of privacy in information a user passes online to an ISP when contracting for Internet service.[74]

Thus, the judicial decisions addressing personal privacy on the Internet strongly suggest that a narrow interpretation of the *Katz* analysis will be applied to determine if society will recognize an expectation of privacy in URL and IP information. The first inquiry would undoubtedly address whether Carnivore enables access to the content of the electronic communications of persons not named in a court order. It is very improbable that, under a narrow *Katz* application, a court would determine URL and IP information to be "content" because each serves a function similar to that of a telephone number. Also, if the judiciary is not willing to recognize an equal expectation of privacy in electronic mail to that of posted mail, the probability of successfully arguing that the protection of information can be intercepted by law enforcement without intrusion into the body of the electronic communication it accompanies is minimal.

The second inquiry in the *Katz* analysis would certainly focus on whether the individual attempted to restrict third party access to his URL or IP information. Again, the judiciary will likely conclude that users of the Internet must realize that they "convey" their URL information since this information must travel through the ISP's network to reach whatever destination is desired.[75] The court will likely, as it has often done when addressing Fourth Amendment applicability to technological advances, attempt to analogize the situation with a more traditional setting. In this case, that traditional setting will undoubtedly be that established in *Smith* and *Miller*.

From this examination, it seems unlikely that, even if an individual can establish that he has a subjective expectation of privacy in URL and IP information attached to his electronic transmissions, the judiciary will determine that society is prepared to recognize such expectation. Thus, Carnivore's interception of URL and IP information relating to individuals not named in a court order is

---

73. 81 F. Supp. 2d 1103 (D. Kan. 2000).

74. *Id.* at 1110.

75. *See Smith*, 442 U.S. at 742 (reasoning that an individual realizes that he must convey phone numbers he dials to his telephone company since his call is completed through the company's switching equipment).

not likely a search as determined under Fourth Amendment principles.

If, in the alternative, the judiciary were to find the existence of both a subjective and societal reasonable expectation of privacy in URL and IP data, Carnivore would undoubtedly be conducting a search of such information, and the next step in the constitutional analysis would be to determine whether the search was a valid one.

2. *The Viewing of Addressing Information Inside Body of Transmission*

a. *Is the Governmental Action a Fourth Amendment Search?*

Electronic addressing information, such as URL or IP data, can generally be intercepted by Carnivore without entering the body of the accompanying electronic transmission.[76] However, there may be certain instances in which such information is located *only* within the body of the communication, such as the "TO:" line within an electronic message. This situation may occur when the particular software used to transmit the communication does not reveal the URL address to the ISP, but merely transmits the IP address, or computer identification number.[77] For example, if the FBI has a court order to search for a particular URL, the device may have to locate this information on the "TO:" line of the transmission if the only information sent from the computer to the ISP is its numerical IP address. Thus, in these cases it is highly probable that Carnivore will enter the body of transmissions sent or received by people not subject to a court order as they flow through the first filter point.

Some argue that this invasion, however slight, is an unauthorized warrantless search. Those who support this position rely on the Supreme Court's reasoning in *Arizona v. Hicks*.[78] In *Hicks*, the Court held that a warrantless search premised on no judicially cre-

76. *See Hearings 2*, *supra* note 22.

77. *See Carnivore's Challenge*, *supra* note 6.

78. 480 U.S. 321 (1987) (concerning a situation where law enforcement officers were legally on private premises investigating a shooting when an officer noticed and certain stereo equipment within the home that he suspected was stolen. The officer slightly moved the equipment in order to obtain its serial number. The Supreme Court held that although law enforcement was legally on the premises, the movement of the equipment constituted a warrantless search because an action was taken by the officer to obtain information not otherwise available to

ated exception will be deemed violative of the Fourth Amendment *even if the governmental intrusion is minimal.* The Court based its decision in part on the fact that such intrusions may give law enforcement access to information that they would not otherwise be legally entitled. Applying the *Hicks* reasoning, when Carnivore is searching for URL information in the body of an electronic transmission, although the intrusion is slight, the FBI may have access to information within the communication that it would not otherwise be legally entitled.

Although this reasoning has not yet been applied by the courts to Internet communications, there is some evidence that suggests that the judiciary would not favor this approach. In 1997, the Communications Assistance for Law Enforcement Act of 1994 (CALEA)[79] was amended to allow telecommunications companies, in certain instances, to provide the full content of customer communications to the government. This is true even when the government is only authorized to intercept addressing information.[80] The amendment relies on law enforcement to segregate the addressing information from the content of the messages. No court has yet deemed the provision to be unconstitutional.[81] Although CALEA is not applicable to ISPs, the amendment and its judicial acceptance is significant in that it illustrates again the trend of the judiciary to place a lower value on, not only addressing information, but electronic communications in general. Therefore, based on the current inclination of the courts, Carnivore's invasion into the body of communications not subject to investigation is not likely to be considered a search for Fourth Amendment purposes.

b. *Assuming the Government Action is a Search, is it a Valid Search?*

Generally, a search is valid under the Fourth Amendment if it is conducted via a warrant based on probable cause, or if it is rea-

---

him.); *see also Carnivore's Challenge*, *supra* note 6 (statement of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology).

79. 47 U.S.C. § 1001 (1994 & Supp. V 1999) (imposing a statutory obligation on telecommunications providers to provide assistance to law enforcement when presented with valid legal authorization; although CALEA regulates telecommunications, it has not yet been amended to include Internet Service Providers).

80. *See* Dempsey, *supra* note 46, at 97-98.

81. *See id.*

sonable.[82] In implementing Carnivore, the FBI obviously has no warrant authorizing the interception of electronic communications of persons not named in a court order. Thus, the inquiry becomes whether the FBI's intrusion on the individual's expectation of privacy is reasonable.[83] In determining whether a governmental search is reasonable, courts will generally first attempt to determine whether the Framers of the Fourth Amendment would regard such action as unlawful.[84] Where this inquiry yields no definitive answer, the judiciary will ordinarily evaluate the search under standards of reasonableness that have been developed though judicial determinations in the area of Fourth Amendment jurisprudence.[85]

Determining the reasonableness of the FBI's action regarding Carnivore based on standards considered by the Framers may prove to be extremely difficult, if not impossible. The concept of searches of electronic communications was not a consideration of the drafters of the amendment. Under standards that have been delineated through numerous Fourth Amendment judicial decisions, however, warrantless searches are generally recognized as reasonable in a limited number of situations. Without enumerating all possible circumstances, the most plausible exception to the warrant requirement likely to be presented by the FBI to justify the operation of Carnivore is the existence of exigent circumstances.[86] The judiciary has identified an exigent circumstance to be one in which there is the danger that evidence will be destroyed if law enforcement takes time to obtain a warrant.[87] Also, an exigent circumstance exists if law enforcement have a reasonable belief that the safety of an agent or other innocent individuals is an issue.[88] An argument suggesting exigent circumstances in an elec-

82. *See* Frank W. Miller, et al., The Police Function 260 (6th ed. 2000).

83. *See* Skok, *supra* note 1, at 71.

84. *See* Florida v. White, 526 U.S. 559, 562-63 (1999); Wilson v. Arkansas, 514 U.S. 927, 931 (1995); California v. Hodari, 499 U.S. 621, 624 (1991); Carroll v. United States, 267 U.S. 132, 149 (1925).

85. *See* Wyoming v. Houghton, 526 U.S. 295, 299-300 (1999); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652-53 (1995); *see also Carroll*, 267 U.S. at 149 ("The Fourth Amendment is to be construed in light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.").

86. Miller, *supra* note 73, at 261.

87. *Id.*

88. *Id.*

tronic surveillance situation is weakened by the Supreme Court's determination that such surveillance can be accomplished without prior notification to the individual under investigation.[89] Thus, the risk that a suspect subject to surveillance by Carnivore will destroy, or in this case, fail to transmit, electronic communications in anticipation of FBI intervention is not likely to be viewed as "reasonable" under the current interpretation of the Fourth Amendment.

Further, as an alternative to searching for a suspect's data by identifying certain URL information, law enforcement could obtain a warrant to conduct a search solely using IP information. This type of information always accompanies electronic transmissions and is always present in the header address location. Thus, the need to enter the body of the transmission is eliminated. However, such an alternative may not be a practical one. Most IP addresses are temporary, and are assigned to a device when it is connected to an ISP's network.[90] These addresses frequently change and thus likely cannot be electronically monitored for any significant period of time.[91]

c. *General Warrant Search of a Target Suspect*

The second constitutional concern presented by the operation of Carnivore focuses on the interception and collection of electronic data attributable to the target suspect of the electronic surveillance. Carnivore functions by copying all electronic data relating to a target individual that is sent through a particular ISP's network. When intercepting and copying such data, Carnivore can employ an "Internet pen register function" or an "Internet wiretapping function."[92] The constitutional issue presented is whether either of these functions present the risk of creating a general warrant search of the target individual's communications.

Internet Pen Register Function

Carnivore's pen register function operates by copying and storing only authorized source and destination data, otherwise termed

89. *See Katz*, 389 U.S. at 355 n.16; *see also* Ker v. California, 374 U.S. 23, 37-41 (1963).

90. *See Latest IP Prompts Net Privacy Fears*, Computing, Oct. 28, 1999, at 14.

91. *See id.*

92. *See Carnivore's Challenge*, *supra* note 6.

addressing information.[93] This information, such as "to" and "from" electronic mail addressing material, is expressly described in a court order, and the FBI must store only such specified information.[94] All other copied data must be purged.[95]

As with communications relating to persons not named in a court order, there are certain situations where Carnivore may enter the body of a transmission pertaining to a named suspect to facilitate the search for URL information. Privacy groups and others are concerned that these circumstances transform an otherwise valid court order into a general warrant because the FBI can now search practically all of the communications sent to or from the suspect.[96] This is an important function when one considers the extremely low standards for acquiring court authorization to intercept source and destination information for electronic communications.[97] The standard, analogous to that of a subpoena or telephone pen register, holds that a judge must approve practically any surveillance request that can reasonably be expected to produce evidence relevant to an ongoing criminal investigation.[98] However, to obtain authorization to intercept the content of certain electronic communications, the FBI must meet the much higher standard applicable to wiretaps.[99] It is therefore plausible that Carnivore's pen register function allows the system to operate under the impermissive authority of a general warrant.

Originally, Fourth Amendment protections were designed primarily to protect individuals from the intrusive power wielded by general warrants.[100] However, modern judicial interpretation of the Amendment has seemed to dilute these principles.[101] Nowhere in Fourth Amendment jurisprudence is this more apparent than in the judiciary's lenient interpretation of the minimization require-

93. *See Hearings 2, supra* note 22.

94. *Id.*

95. *Id.*

96. *See* Donna Howell, *Security & Privacy Studies Set to Flesh Out FBI's Carnivore*, Investor's Bus. Daily, Aug. 28, 2000, at 8.

97. *See* 18 U.S.C. §§ 3122-23 (1994).

98. *See id.*

99. *See* 18 U.S.C. § 2510 (1994 & Supp. V 1999).

100. *See* Christopher E. Torkelson, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 Seton Hall L. Rev. 1142, 1175 n.90 (1995).

101. *See id*; *see also* Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics,"* 7 Harv. J. Law & Tech. 239, 278 (1994).

ments mandated in the federal wiretap laws.[102] Substantial evidence suggests that the interception of unauthorized information attributable to a target suspect during the conduct of an electronic surveillance is rarely even frowned upon by the courts.[103] In fact, law enforcement is often afforded judicial tolerance when certain technical or practical difficulties inhibit their ability to minimize the interception of such data.[104] Reasoning from this perspective, Carnivore's inability to consistently intercept addressing or routing information without entering the body of an electronic transmission is likely to be allowed by the courts and not viewed as an unconstitutional general warrant search of the target suspect's communications.

Internet Wiretap Function

Carnivore's wiretapping function operates by searching all of the target suspect's Internet communications for key words or phrases that are described in a court order.[105] Although the FBI copies all transmissions pertaining to the suspect, it must store only communications containing such key words or phrases, and purge all other information.[106] This "stored" data is sent to an FBI facility for subsequent examination by FBI agents.[107]

Similar to the Internet pen register function, advocates of greater privacy protections on the Internet are worried that this procedure may also present a danger of a general warrant.[108] Those promoting this position believe there is a risk that a transmission could contain the specified "key word or phrase" but not be relevant to the government's investigation.[109] For example, if a key word such as "drugs" is authorized, the FBI might collect and review a target suspect's communication consisting of anything from a request submitted to a website concerning new drugs available for AIDS patients, to cures for the common cold. The IITRI report seems to concede this possibility. It states that while the

102. *See* Dempsey, *supra* note 46, at 77.
103. *See* Scott v. United States, 516 F.2d 751 (D.C. Cir. 1975); *see also* United States v. Ozar, 50 F3d. 1440 (8th Cir. 1995).
104. *See id.*
105. *See Carnivore's Challenge*, *supra* note 6.
106. *See id.*
107. *See Hearings 2*, *supra* note 22.
108. *See Carnivore's Controversy*, *supra* note 6.
109. *See id.*

system is designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps.[110] Incorrectly configured, Carnivore can record any traffic it monitors.[111] The report goes on to state that this possibility may be increased due to the lack of adequate audit trail provisions or safeguards against common configuration errors.[112]

However, like the pen register function, the relaxed minimization requirements applied by the judiciary to more traditional wiretap investigations are likely to be similarly applied to Internet taps. Therefore, the FBI's erroneous collection and storage of target suspect material not relevant to the surveillance is probably constitutionally permissible.

Upon analysis, it appears that the FBI's implementation and utilization of Carnivore is in compliance with Constitutional principles, at least so far as these principles are currently interpreted. The next stage of the legal analysis addresses whether or not the application of Carnivore complies with federal statutory wiretap laws.

III. Federal Statutory Analysis

The legitimacy of the Carnivore surveillance system can also be analyzed in a statutory context. The focal points of such an analysis are the privacy protections included in such provisions that add to the constitutional minimum. Once these added safeguards are determined, an assessment of how the judiciary is likely to interpret and apply such provisions must be made. The following presents a commensurate examination of the federal statutory provisions applicable to Carnivore, as well as the probable judicial opinion as to Carnivore's compliance with such requirements.

In 1968, one year after *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act.[113] This act permitted non-consensual wire or oral eavesdropping by the government as long as the surveillance was done pursuant to the requirements

110. *See* Brian Krebs, *Study Calls For Stronger Audit Trail In FBI's Carnivore*, Newsbytes, Nov. 21, 2000.

111. *See id.*

112. *See id.*

113. 18 U.S.C. § 2510 (1994 & Supp. V 1999).

delineated in the act.[114] In 1986, Congress amended Title III by passing the Electronic Communications Privacy Act (EPCA).[115]

The ECPA was intended to enhance Title III by establishing definitive rules for electronic surveillance.[116] In drafting the ECPA, Congress included certain privacy "protections" that underlie the essential purpose of the statute. These protections can be grouped into three categories.[117] First, any attempted electronic surveillance is subject to stringent ex parte judicial review. Second, those conducting the electronic surveillance must minimize the interception of non-pertinent information during the surveillance. Third, the conduct of and results derived from an authorized electronic surveillance may be subject to a stringent adversarial review after the surveillance has been completed.[118]

An analysis will show that these protections, although embodied in the language of the ECPA, have been significantly diminished through judicial interpretation and action. Thus, the utilization of Carnivore, arguably an extremely invasive investigative tool, is likely to be in full compliance with the federal statutory requirements of the ECPA.

Ex Parte Judicial Review

EPCA Section 2518 provides that upon an application for a surveillance order, the issuing judge may enter an ex parte order authorizing interception of the electronic communications.[119] In issuing such order, the judge must determine primarily that (1) there is probable cause for belief that an individual is committing, has committed, or is about to commit a specific offense enumerated in the statute; (2) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; and (3) *normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or may be too dangerous.*[120]

---

114. *See id.*

115. *See* Christopher Slobogin, Criminal Procedure: Regulation of Police Investigation 190 (2d ed. 1998).

116. 18 U.S.C. § 2518 (1986).

117. *See* Dempsey, *supra* note 46, at 85.

118. *See id.*

119. 18 U.S.C. § 2518 (1994 & Supp. V 1999).

120. *Id.; see also* Dempsey, *supra* note 46, at 85.

The FBI has applied for and received approximately twenty-five court orders approving the use of Carnivore in the past two years.[121] Although it is unclear what information was presented to obtain such surveillance orders, the majority of courts have generally applied the same sufficiency of evidence standard for establishing probable cause for electronic surveillance warrants as required for more traditional warrants.[122] Thus, it is likely that all twenty-five surveillance requests were supported by sufficient probable cause.

The judicial application of Section 2518 (3) presents a more elusive question. Although the statutory language expressly mandates that normal investigative procedures generally be tried and failed before electronic surveillance should be authorized, in many jurisdictions, evidence strongly suggests this procedure is not adhered to. Some courts authorize electronic wiretapping before all other investigative techniques have been exhausted. In these jurisdictions, in order to obtain a warrant authorizing interception of such communications, the government need only show that other techniques would be "impracticable under the circumstances."[123] In other jurisdictions, law enforcement only has to state a "likelihood of failure" of other investigative techniques in their affidavit for a search warrant.[124]

This trend is also reflected statistically. Between 1968 and 1995, federal and state courts approved 20,107 surveillance applications and denied only 27, with none denied since 1988. Further, from the 349 federal taps authorized in 1991, 1022 persons were arrested and 292, or about .08% of the total number under surveillance, were convicted.[125]

Thus, based on this persuasive data, it is possible that so long as the FBI can establish probable cause for a particular investigation, it can obtain an order to implement Carnivore without

121. *See Hearings 2*, *supra* note 22 (statement of Donald Kerr, Asst. Director, Federal Bureau of Investigation).

122. *See generally* United States v. Clements, 588 F.2d 1030 (1979) (finding probable cause existed based on information provided by three informants and independently corroborated by police); United States v. Wagner, 989 F.2d 69 (1993) (finding probable cause existed based on information provided by informant that had made eight previous drug purchases under police supervision).

123. United States v. Cooper, 85 F. Supp. 2d 1 (2000).

124. United States v. Caruso, 415 F. Supp. 847 (1976).

125. *See* Slobogin, *supra* note 112, at 190.

presenting evidence of an attempt to utilize more conventional investigative techniques, and still be in full compliance with the statutory requirements.

Major Crimes Only

In drafting the original Title III, Congress recognized that wiretapping created a significant opportunity for abuse, and therefore should be limited in its use. Thus, the Legislature expressly stated that "interception of . . . communications should . . . be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused."[126]

However, the list of offenses for which wiretapping and electronic surveillance are permitted under Title III and the EPCA has increased from 26 in 1968 to 95 in 1996.[127] The list has expanded from espionage, treason, violent crimes, and offenses typically associated with organized crime, to include such cases as those involving false statements on passport applications and loan applications.[128] Further, by and large, electronic surveillance is primarily used in drug cases. In 1996, 71% of wiretaps nationwide were issued for drug cases.[129]

The FBI has stated that its use of Carnivore has complied with the "major crimes" requirement of Title III, primarily focusing on cases such as those involving the illegal solicitation of sex with minors and security issues concerning illegal bomb making activities.[130] The Bureau has also acknowledged possible use of the device in narcotics investigations.[131] In light of the expanded list of legislatively approved uses for electronic surveillance, the FBI's assertion of compliance with the statute is correct, and Carnivore is being utilized well within the statutory guidelines.

---

126. Omnibus Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801, 82 Stat. 211 (1968).

127. 18 U.S.C § 2516 (1994); *see also* Dempsey, *supra* note 46, at 76-77.

128. *See* Dempsey, *supra* note 46, at 76.

129. *Id.*

130. *See* Qaisar Alam, *E-Mail Surveillance: Carnivore Cornered*, Computers Today, Oct. 31, 2000, at 48.

131. *See* Danny A. Defenbaugh, *FBI's Carnivore Software*, Dallas Morning News, Aug. 27, 2000, at 4J.

Minimization of Non-Pertinent Information

The EPCA requires that electronic surveillance "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[132] However, similar to the other two statutorily enumerated protections, the minimization requirement has not been strictly enforced by the courts.[133] It appears that any explanation for law enforcement's failure to minimize will suffice to justify their actions. For instance, in *Scott v. United States,*[134] the D.C. Circuit held that the complete recording of all conversations on a phone line used by a suspect was acceptable despite the fact that 60% of calls were not pertinent to the investigation. The court accepted the failure to minimize on law enforcement's explanation that the suspect often used coded language in brief conversations. Thus it was necessary for law enforcement to listen to all calls to determine their relevancy.[135]

Similarly, in *United States v. Ozar,*[136] the Eighth Circuit upheld the FBI's method of listening to two out of every three minutes of every phone conversation. In *Ozar*, the government intercepted a total of 8,126 minutes of the suspect's telephone conversations, of which 223 minutes, or 2.75% were deemed pertinent to the investigation.[137] The FBI explained that it was necessary to listen to a large number of conversations to determine their relevancy, not because they were short and coded, as in *Scott*, but because they were lengthy and contained complicated subject matter.[138]

The Carnivore system cannot be implemented without intercepting electronic transmissions unrelated to the target suspect.[139] Also, the system operates by intercepting and copying all communications sent to or received by an individual under surveillance.[140] Thus, a situation requiring effective minimization of information not pertinent to the investigation is very much

132. 18 U.S.C. § 2518(5) (1994 & Supp. V 1999).
133. *See* Dempsey, *supra* note 46, at 77.
134. 516 F.2d 751 (D.C. Cir. 1975); *see* Dempsey, *supra* note 46, at 77.
135. *Scott*, 516 F.2d at 755.
136. 50 F.3d 1440 (8th Cir. 1995); *see* Dempsey, *supra* note 46, at 77.
137. *Ozar*, 50 F.3d at 1448.
138. *Id.; see also* Dempsey, *supra* note 46, at 77.
139. *See Hearings 1*, *supra* note 15 (statement of Sen. Patrick Leahy).
140. *See Hearings 2*, *supra* note 22 (statement of Donald Kerr, Asst. Director, Federal Bureau of Investigation).

presented. However, based on the collective reasoning applied by the judiciary, it appears improbable that a failure by the FBI to adequately minimize the interception of such data while implementing Carnivore would have any significant statutory ramifications.

Post-Surveillance Judicial Review

EPCA provides that that an individual who is subject to government conducted electronic surveillance is entitled to an after-the-fact judicial review of the authorization and conduct of the surveillance.[141] However, the EPCA currently contains no exclusionary provision for illegally obtained electronic transmissions *in transit.*[142] Arguably, this would be the type of electronic information Carnivore expressly targets. A proposed amendment to the EPCA suggests the implementation of such a provision,[143] but judging from the application of exclusionary provisions applicable to wire and oral communications, it is not encouraging that such a provision would be effective. Statistics indicate that a defendant's after-the-fact challenges to the authorization or conduct of oral and wire surveillance are rarely sustained.[144] Between 1985 and 1994, judges nationwide granted 138 suppression motions while denying 3,060, for a 4.3% suppression rate.[145] In light of this data, it seems highly improbable that even after the enactment of an applicable exclusionary provision, any party attempting to challenge the conduct of an electronic surveillance utilizing Carnivore would be successful. From this analysis, it is presumable that the use of

141. *See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 103rd Cong. 6 (1994) (testimony of Louis J. Freeh).

142. *See Hearings on H.R. 5018, Electronic Communications Privacy Act of 2000; H.R. 4987, Digital Privacy Act of 2000; and H.R. 4908, Notice of Electronic Monitoring Act*, 106th Cong. (2000) (statement of Gregory T. Nojeim, Legislative Counsel, American Civil Liberties Union).

143. *See Hearings on H.R. 5018, Electronic Communications Privacy Act of 2000; H.R. 4987, Digital Privacy Act of 2000; and H.R. 4908, Notice of Electronic Monitoring Act*, 106th Cong. (2000) (statement of Robert Corne-Revere).

144. *See* Robert Plotkin, *Breaking the Code: Excluding Illegal Wiretap Evidence*, 10 BNA Crim. Prac. Manual 432 (1996).

145. *See* Dempsey, *supra* note 46, at 77.

Carnivore would not be deemed to violate the privacy protections embodied in Title III and the EPCA.

CONCLUSION

The information and analysis presented in this comment supports the conclusion that the FBI's Carnivore surveillance device is likely to be in compliance with both constitutional and federal statutory requirements. However, in light of citizen concern and uncertainty concerning the utilization of Carnivore, I briefly propose two plausible solutions that would likely quell, or at least diminish, these fears and concerns while still achieving the government objective. These proposals are as follows:

First, the FBI could replace Carnivore with a less invasive surveillance system. Since the existence of Carnivore was made public last year, several software companies have developed alternatives. One such alternative, "Altivore,"[146] works much like Carnivore. However, unlike Carnivore, Altivore allows for the collection of just one stream of data as the information flows through the device, thus reducing some fear that unauthorized data is being intercepted.[147]

Second, ISPs should be given some collaborative role in the conduct of the surveillance. Carnivore, in departure from ordinary telephone taps, inserts the FBI into the ISP's network.[148] In fact, the ISP has no role in the surveillance once the ISP assists the FBI in connecting to its network.[149] Like CALEA, the EPCA should be amended to require ISP assistance in the collection of data from its network. In addition, the FBI should make the technology of Carnivore, including the source code and the right to modify it, available to any ISP that needs to comply with a surveillance order. The involvement of the ISP would serve to confirm exactly what the operating capabilities of the system really are.

Obviously, these recommendations are not all of the possible solutions that could effectively balance the interest of Internet users with that of the Government. Yet, whatever resolution is se-

146. *See* Ann Harrison, *Security Software Vendor Develops Carnivore E-Mail Monitoring Alternative*, Infoworld Daily News, Sept. 21, 2000.

147. *See id.*

148. *See* Dempsey, *supra* note 19, at AO3.

149. *See id.*; *see also Hearings 1*, *supra* note 15 (statement of Sen. Patrick Leahy).

lected, American society must act quickly if it wishes to preserve fundamental Fourth Amendment protections as it moves further and further into the technology age. Without a doubt, in light of the uncertain and inadequate legal and judicial guidance currently applicable to the Internet forum, we have a very long way to go.

Patricia K. Holmes