South Carolina Law Review

Volume 52
Issue 4 *ANNUAL SURVEY OF SOUTH CAROLINA LAW*

Article 6

Summer 2001

The Software Formally Known as "Carnivore": When Does E-mail Surveillance Encroach Upon a Reasonable Expectation of Privacy?

Manton M. Grier Jr.

THE SOFTWARE FORMERLY KNOWN AS "CARNIVORE": WHEN DOES E-MAIL SURVEILLANCE ENCROACH UPON A REASONABLE EXPECTATION OF PRIVACY?

Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[1]

I. INTRODUCTION

What was once known as "Carnivore" is now called DCS1000, short for digital collection system.[2] It is the FBI's latest e-mail surveillance technology—a software program housed in a computer unit and attached to an Internet service provider, such as America Online.[3] Once attached, Carnivore has the capability of filtering all e-mail sent through a data access point.[4] Theoretically, the software targets and collects only those e-mail communications subject to a court order while ignoring e-mails sent by the public at large.[5] In other words, it gets to the "meat" of a suspect's e-mail communication.[6] However, privacy advocates wonder if some of the meat Carnivore devours is an individual's reasonable expectation of privacy.

Due to the fluid and evolving nature of the FBI's snooping software, this Comment focuses on the Carnivore version reviewed by an independent report in Fall 2000.[7] Because software can evolve virtually overnight, this Comment will focus both specifically on the Carnivore software and generally on e-mail snooping surveillance.

---

1. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

2. This Comment will refer to DCS1000 as Carnivore. The FBI changed the name because "[t]he name Carnivore contributed to some perceptions that the application was a predatory program that could invade citizens' privacy." Matt McLaughlin, *FBI's Upgrade of Carnivore Includes a New Name*, GOV'T COMPUTER NEWS (Feb. 12, 2001), *at* http://www.gcn.com/vol1_no1/ndaily-updates/3661-1.html.

3. *See* FBI, *Carnivore Diagnostic Tool, Large Chart Description*, *in* FBI PROGRAMS AND INITIATIVES, *at* http://www.fbi.gov/programs/carnivore/carnlrgmap.htm (last visited Feb. 21, 2001) [hereinafter *Chart Description*].

4. *Id.*

5. *See* IIT RESEARCH INST., INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT 1-1 (Dec. 8, 2000), *available at* http://www.cdt.org/security/carnivore/00121carniv_final.pdf [hereinafter IITRI REPORT].

6. Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3.

7. *See* IITRI REPORT, *supra* note 5.

This Comment attempts to delineate the expectations of privacy an individual has when using the Internet and determine whether Carnivore or other Internet surveillance software violates these expectations. E-mail "snoopers" possibly violate expectations of privacy in two ways: (1) by collecting too much information while operating in pen-trap mode; and (2) by possessing an inherent potential for abuse. Part II provides an introduction to Carnivore and sketches the Fourth Amendment's reasonable expectation of privacy and how it relates to e-mail. Part III analyzes Carnivore and concludes the following: (1) the current pen-trap mode operation is not statutorily authorized; (2) the pen-trap mode operation intrudes upon a reasonable expectation of privacy by collecting too much information; and (3) although the current software falls short of an Orwellian-type device, it nevertheless should be used only in extraordinary or emergency situations in order to reduce the potential for abuse.

II. BACKGROUND

"*Big Brother Is Watching You . . .*"[8]

A. What is Carnivore?

Carnivore is an e-mail surveillance software created by the FBI "to combat terrorism, espionage, information warfare, child pornography, serious fraud, and other felonies."[9] The software is housed in a computer and connected to an Internet service provider (ISP) such as AOL, Earthlink, or Prodigy. The ISP then provides the FBI with an access point containing all traffic from the suspect.[10] Using a one-way tapping device, all data at the access point is copied.[11] Carnivore then filters this copied data, sniffing out and retrieving "packets" of information that are subject to court orders while theoretically rejecting all extraneous data.[12] FBI administrators have the ability to calibrate Carnivore to capture packets based on Internet Protocol (IP) address or e-mail username.[13] "Packets can be recorded in their entirety (full mode) or recording can be limited to addressing information (pen mode), i.e., IP addresses and usernames."[14]

---

8. GEORGE ORWELL, 1984, at 1 (First Plume Printing 1983) (1949).

9. IITRI REPORT, *supra* note 5, at 1-1; FBI, *Carnivore Diagnostic Tool*, *in* FBI PROGRAMS AND INITIATIVES, *at* http://www.fbi.gov/programs/carnivore/carnivore2.htm (last visited Feb. 21, 2001) [hereinafter *Carnivore Diagnostic Tool*].

10. *See Chart Description*, *supra* note 3 (noting that in some cases, the ISP is able to provide an access point containing only the suspect's traffic).

11. *Id.*

12. IITRI REPORT, *supra* note 5, at 1-1.

13. *Id.*

14. *Id.*

All captured data is saved on a removable Jaz disk.[15] The disk is locked behind a panel in the housing computer and can only be lawfully removed by authorized FBI personnel.[16] When a disk is removed, it is placed in a sealed container and taken to the judge who issued the court order.[17]

The housing computer is installed without a keyboard or monitor.[18] Once installed, it is controlled remotely via a telephone link using a 56-kbps modem.[19] The software is capable of operating in two modes: (1) pen-trap mode, which collects addressing information;[20] or (2) full-content mode, which can capture virtually all the suspect's Internet communications.[21] The legal standards authorizing the different modes vary, with pen-trap authorization being easier to obtain.[22]

The controversy surrounding Carnivore became public on July 11, 2000, through an article published in the Wall Street Journal.[23] The article stated, "[W]hen deployed, [Carnivore] must be hooked directly into Internet service providers' computer networks. That would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing."[24] Not surprisingly, the suggested scope and potential intrusiveness of the technology concerned privacy advocates.[25] The day after the article ran, the Electronic Privacy Information Center (EPIC) filed a lawsuit seeking disclosure under the Freedom of Information Act[26] and an injunction to prevent the use of Carnivore until further review.[27] The FBI countered by claiming Carnivore was authorized to: (1) collect TO and FROM information under the Electronic Communications Privacy Act of 1986 (ECPA),[28] which regulates pen-trap devices; (2) conduct full content searches under Title III of the Omnibus Crime

---

15. *Id.* at 3-12.
16. *Id.*
17. *Id.*
18. IITRI REPORT, *supra* note 5, at 3-12.
19. *Id.*
20. *Id.* at 1-1. In the case of e-mail, this addressing information will be the usernames from the TO and FROM fields; in other words, an e-mail address or a list of addresses. *Id.* at viii, 1-1.
21. *Id.* at viii and 1-1.
22. *See* discussion *infra* Part III.B.
23. *See* King & Bridis, *supra* note 6, at A3.
24. *Id.*
25. According to Barry Steinhardt, Associate Director of the ACLU, using Carnivore "is comparable to allowing government agents to rip open Post Office mailbags and scan every piece of mail in search of one specific letter whose address they already know." Press Release, ACLU, ACLU Urges Congress to Put a Leash on "Carnivore" and Other Government Snoopware Programs (July 12, 2000), *at* http://www.aclu.org/news/2000/n071200b.html.
26. 5 U.S.C. § 552 (1994).
27. *See* Elec. Privacy Info. Ctr. v. Dep't of Justice, No. 00-1849 JR (D.D.C. filed July 12, 2000).
28. 18 U.S.C. §§ 3121-3127 (1994); *see generally* IITRI REPORT, *supra* note 5, at 3-1 to 3-3 (setting forth the legal framework which justifies the use of Carnivore).

Control and Safe Streets Act of 1968 (Title III);[29] and (3) conduct surveillance of foreign powers and agents under the Foreign Intelligence Surveillance Act of 1978 (FISA).[30]

In October 2000 the United States Justice Department appointed an independent panel of experts from the Illinois Institute of Technology Research Institute (IITRI) to review Carnivore.[31] On December 8, 2000, the IITRI concluded that when used pursuant to a Title III court order, Carnivore provides no information beyond the scope of a warrant, and when used under pen-trap authorization, it possibly exceeds court-permitted collection.[32] This report, however, failed to close the book on the surveillance software. Indeed, some have questioned just how independent the review actually was[33] and whether the report contained improper conclusions of law.[34]

B. What is a Reasonable Expectation of Privacy?

Although not explicit in the United States Constitution, a reasonable expectation of privacy exists in the context of the Fourth Amendment's right to be free from unreasonable searches and seizures.[35] In *Katz v. United States*,[36]

---

29. 18 U.S.C. §§ 2510-2520 (1994).

30. 50 U.S.C. §§ 1801-1811 (1994).

31. *See* IITRI REPORT, *supra* note 5, at vii.

32. *Id.* at xii.

33. *See* David McGuire, *Positive 'Carnivore' Review Draws Immediate Fire*, NEWSBYTES, Dec. 14, 2000, *at* http://www.newsbytes.com/news/00/159442.html (quoting House Majority Leader Dick Armey, R-Texas, who stated, "[t]his review by a team with clear ties to this administration raises more concerns than it answers"); Barry Steinhart & Christopher Chiu, *ACLU Comments Regarding Carnivore Review Team Draft Report*, *at* http://www.aclu.org/news/2000/carnivore_comments.html (last visited Jan 17, 2001).

34. *See* Letter from David L. Sobel, General Counsel, EPIC, to Carnivore Review Panel, U.S. Department of Justice (Dec. 1, 2000), *at* http://www.epic.org/privacy/carnivore/review_comments.html (arguing that the IITRI team undertook a purely technical review of Carnivore, yet made conclusions regarding both technical and legal issues).

35. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."). In *Olmstead v. United States* Justice Brandeis stated the following:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Although Justice Brandeis's dissenting opinion was ahead of its time, the U.S. Supreme Court in *Katz v. United States* essentially adopted his view that an element of privacy exists in the Fourth Amendment. Katz v. United States, 389 U.S. 347, 353 (1967); *see also* Warden v. Hayden, 387 U.S. 294, 304 (1967) ("We have recognized that the principal object of the Fourth Amendment is the protection of privacy . . . .").

36. 389 U.S. 347 (1967).

the United States Supreme Court accepted this view by declaring "the Fourth Amendment protects people, not places."[37] In *Katz* the Court held that recording Katz's telephone conversations in a phone booth constituted a search under the Fourth Amendment because the conduct "violated the privacy upon which he justifiably relied while using the telephone booth . . . ."[38] Although the *Katz* majority opinion did not mention the phrase "reasonable expectation of privacy," Justice Harlan formulated a test in his concurrence for measuring this expectation.[39]

Under Justice Harlan's test a search violates a person's reasonable expectation of privacy if (1) the person has exhibited an actual (subjective) expectation of privacy and (2) that expectation is one which society recognizes as reasonable (objective).[40] Justice Harlan, however, later de-emphasized the importance of a subjective expectation of privacy.[41] Moreover, he suggested an expectation must be more than merely reasonable; something else was required.[42] He proposed the "something else" was a balancing of "the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[43]

Subsequent Supreme Court cases have held that the reasonableness of a search, and whether a legitimate expectation of privacy exists, is determined by balancing the needs of the government versus the rights of a particular individual.[44] Thus, an individual may possess an expectation of privacy, but this expectation is unreasonable if the court concludes that the governmental interest outweighs the individual's privacy interest.[45] When an individual's expectation of privacy is deemed unreasonable, the Fourth Amendment provides no protection, regardless of whether a warrant was properly

---

37. *Id.* at 351; *see also* Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1756 (1994) (arguing that "[b]y declaring that 'the Fourth Amendment protects people, not places,' the *Katz* Court effectively tied the Amendment's core meaning to the citizenry's 'reasonable expectation[s] of privacy'").

38. *Katz*, 389 U.S. at 353.

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

40. *Id.* (Harlan, J., concurring) ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

41. *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The analysis must, in my view, transcend the search for subjective expectations . . . [because] [o]ur expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.").

42. *Id.*; *see also* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 134-35 (3d ed. 2000) (tracing the development of Justice Harlan's test).

43. *White*, 401 U.S. at 786.

44. *See* Winston v. Lee, 470 U.S. 753, 759 (1985); United States v. Martinez-Fuerte, 428 U.S. 543, 555 (1976); Terry v. Ohio, 392 U.S. 1, 20-21(1968).

45. *See* Chandler v. Miller, 520 U.S. 305, 314 (1997).

obtained.[46] However, if an individual's expectation is reasonable, the Fourth Amendment provides protection from police intrusion absent a warrant supported by probable cause.[47]

Finding bright guidelines for this balancing test has proved elusive. Nevertheless, delineations of what is considered a reasonable expectation of privacy, however vague, can be placed on a spectrum,[48] and the Court will recognize those expectations as either legitimate, diminished, or altogether nonexistent.[49] On one end of this spectrum are situations where an individual experiences the greatest expectation of privacy. Thus, legitimate expectations are found, for example, in the privacy of one's home, especially at night,[50] or in one's personal effects.[51] In the middle of this spectrum are instances where an individual experiences a diminished expectation, such as in a car[52] or at a business establishment.[53] However, perhaps the best way to define a reasonable expectation of privacy is to examine those situations where there is no legitimate expectation. Thus, the Supreme Court has found, for example, there is no reasonable expectation of privacy in the contents of a conversation

---

46. *See White*, 401 U.S. at 748.

47. *See Katz*, 389 U.S. at 361.

48. It should be noted that Fourth Amendment case law is very complex. Indeed, one professor has commented: "Fourth Amendment case law is a sinking ocean liner—rudderless and badly off course—yet most scholarship contents itself with rearranging the deck chairs." Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994). Because this Comment focuses narrowly on the Fourth Amendment in relation to e-mail and an e-mail snooping system, only a very rough sketch of Fourth Amendment jurisprudence is provided.

49. Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1302 (1981) (arguing that the United States Supreme Court has developed a graduated approach based upon degrees of privacy expectations).

50. *See* Gooding v. United States, 416 U.S. 430, 462 (1974) (Marshall, J., dissenting) ("[T]here is no expectation of privacy more reasonable and more demanding of constitutional protection than our right to expect that we will be let alone in the privacy of our homes during the night.").

51. *See* Bond v. United States, 529 U.S. 334, 336-37 (2000) (finding that a traveler's personal luggage is an "effect" protected by the Fourth Amendment, and the individual possessed a privacy interest in his bag).

52. *Compare* Delaware v. Prouse, 440 U.S. 648, 662 (1979) (reasoning that because people experience a greater sense of privacy while in a car than walking on the street, an individual does not sacrifice all expectations of privacy merely because driving a car is regulated) *with* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his *movements* from one place to another." (emphasis added)).

53. *Compare* See v. City of Seattle, 387 U.S. 541, 543 (1967) ("The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property.") *with* Minnesota v. Carter 525 U.S. 83, 90 (1998) ("'An expectation of privacy in commercial premises, however, is different from, and indeed less than, a similar expectation in an individual's home.'" (quoting New York v. Burger, 482 U.S. 691, 700 (1987))).

divulged to a third party,[54] in something knowingly exposed to the public,[55] or in the garbage on the side of the street.[56]

C. *A Reasonable Expectation of Privacy While Using E-Mail*

Electronic mail, commonly known as "e-mail," is a medium of communication transmitted via computers connected over either the Internet (World Wide Web) or an intranet (your office system).[57] In many respects, e-mail is a hybrid of the postal mail and the telephone. Communication via e-mail is similar to postal mail because both (1) are written communications; (2) allow for the attachment of items, such as files or pictures; (3) lack voice inflection, which affects the recipient's ability to judge the tone of the communication; and (4) cannot be retracted once sent. On the other hand, e-mail is similar to a phone call because the communication is virtually instantaneous and is electronic, meaning it is capable of being intercepted by electronic means.

Understanding how an e-mail message is sent and received requires a cursory understanding of how the Internet works. The Internet is basically "a network of networks."[58] Rather than a physical entity, it is "a giant network which interconnects innumerable smaller groups of linked computer networks."[59] Because the smaller networks are owned by various individuals or organizations, public and private, the Internet is essentially a decentralized, global cyberspace that links the entire world.[60]

When an e-mail is sent via the Internet, the message is not sent as a whole entity; rather, it is divided into a series of "packets" which are reassembled at the receiving end.[61] These packets may take many and varying paths to their destination.[62] If certain computers along the path become overloaded, some packets will travel through less congested computers.[63] Because e-mail is not

---

54. *See* United States v. White, 401 U.S. 745, 749 (1971) (reasoning that an individual cannot reasonably assume that the person with whom she is conversing will not later divulge that conversation to the police).

55. *See* Katz v. United States, 389 U.S. 347, 351-52 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (internal citations omitted)).

56. *See* California v. Greenwood, 486 U.S. 35, 40-41 (1988) (reasoning that when a person places garbage on the street, she expressly places it there to be available to the public—such as children, scavengers, or the sanitation department).

57. *See* Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOC'Y 3, *at* http://www.isoc.org/internet/history/brief.html (last modified Aug. 4, 2000).

58. ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996).

59. *Id.*; *see generally* Leiner et al., *supra* note 57 (tracing the development of the Internet and its accompanying technology).

60. *See ACLU*, 929 F. Supp at 831.

61. *Id.* at 832.

62. *Id.*

63. *Id.*

sealed or secure, intermediate computers may be used to access or view the message, unless it is encrypted.[64]

The first federal appellate court to address the issue of an individual's reasonable expectation of privacy in the use of e-mail was the Court of Appeals for the Armed Forces.[65] In *United States v. Maxwell* the appellant had been convicted of knowingly transporting or receiving child pornography in violation of the Sexual Exploitation and Other Abuse of Children Act of 1978.[66] The appellant was discovered by an FBI sting that targeted a child pornography ring operating on the Internet service provider America Online (AOL).[67] On the one hand, the court found that the appellant "possessed a reasonable expectation of privacy, albeit a limited one," in the e-mails he sent via AOL.[68] The court stressed that these e-mail messages were privately stored by AOL,[69] thus affording more protection than, for example, an e-mail transmitted at work. The court, however, also determined that expectations of privacy depend on the type of e-mail used and on the indentity of the intended recipient.[70] Thus, the court found that "[m]essages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent [lose] any semblance of privacy."[71]

In *United States v. Monroe*,[72] the United States Court of Appeals for the Armed Forces, while acknowledging its holding in *Maxwell*, found the appellant had no reasonable expectation of privacy in his e-mail messages that were viewed by Air Force personnel who maintained the network system.[73] In distinguishing *Monroe* from the holding in *Maxwell*, the court noted that in *Maxwell*, AOL contractually agreed not to disclose subscribers' e-mail.[74] Thus, e-mails sent at work or through the Internet itself, absent contractual

64. *Id.*

65. United States v. Maxwell, 42 M.J. 568 (A.F. Ct. Crim. App. 1995), *rev'd in part*, 45 M.J. 406 (C.A.A.F. 1996).

66. *Id.* at 410; 18 U.S.C. § 2252 (1994).

67. *See Maxwell*, 45 M.J. at 411-14. The appellant's AOL communications were seized subject to a warrant; however, the warrant was issued to search transmissions by an individual identified by the username "REDDEL," rather than by the actual name the appellant used, which was "Reddel," as in "Ready One." *Id.* at 413. In anticipation of the search warrant, AOL created software to help assist the search. *Id.* In doing so, AOL actually compiled a list of names which included the appellant's name, "Reddel," although this actual name never appeared on the warrant. *Id.* The appellant argued that AOL used its software *before* the search warrant was actually issued, and therefore, had such use not occurred, the FBI would have never identified him, for they only had the name "REDDEL." *Id.*

68. *Id.* at 417.

69. *Id.* (reasoning that "e-mail messages are afforded more privacy than similar messages on the Internet, because they are privately stored for retrieval on AOL's centralized and privately-owned computer bank").

70. *Id.* at 418-19.

71. *Id.* at 419.

72. 52 M.J. 326 (C.A.A.F. 1999).

73. *Id.* at 330.

74. *Id.*

guarantees, experience a diminished degree of protection from the Fourth Amendment.[75]

In sum, the use of e-mail falls into the middle of the spectrum—a diminished expectation of privacy. On the one hand, the use of e-mail is generally subject to the same Fourth Amendment protections found in the use of the telephone and postal mail,[76] and the sender of an e-mail can reasonably expect that the contents will remain private and free from police intrusion, absent a search warrant supported by probable cause.[77] On the other hand, "chat" messages,[78] received e-mails,[79] forwarded e-mails,[80] and e-mails divulged to third parties[81] afford no reasonable expectation of privacy. Thus, in order to implicate the Fourth Amendment, it is necessary to determine how, when, where, and to whom the e-mail was sent.

III. ANALYSIS

"Down With Big Brother"[82]

The year 1984 has come and passed, and yet an Orwellian-type regime has failed to materialize.[83] Nevertheless, technology has, as Justice Brandeis eloquently stated in 1928, continued to advance to the point where a government, or an individual for that matter, can now penetrate our private writings without opening a drawer.[84] Yet the courts have concluded that society is prepared to submit to minimal intrusions for the sake of the collective good.[85] The issue is therefore the degree of Carnivore's intrusiveness.

Theoretically, Carnivore or a similar device may intrude upon a Fourth Amendment reasonable expectation of privacy in the following two ways: (1) by uncovering too much personal information while being used as a pen-trap device pursuant to the Electronic Communication Privacy Act of 1986 (ECPA)[86] and (2) by the software's inherent potential for abuse. In addition to

---

75. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that an employee, in a tort action against an employer, has no reasonable expectation that e-mails sent to a supervisor via the company e-mail system will not be intercepted by management, despite assurances to the contrary).

76. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997).

77. *Id.*

78. United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996).

79. *Id.*

80. *Id.*

81. *See Charbonneau*, 979 F. Supp. at 1184; *see also* Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding that Fourth Amendment fails to protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

82. ORWELL, *supra* note 8, at 16.

83. *Id.* at 14.

84. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

85. *See supra* Part II.B.

86. 18 U.S.C. §§ 3121-3127 (1994).

potentially violating the Fourth Amendment, Carnivore's use may not be authorized by the relaxed standards of the ECPA. Therefore, to address the broad issue of whether Carnivore is unreasonably intrusive, this Comment focuses on three specific issues: (1) whether the pen-trap mode is authorized under the ECPA; (2) whether Carnivore violates a Fourth Amendment reasonable expectation of privacy while operating in pen-trap mode because it over-collects and can easily be misused; and (3) whether Carnivore violates a Fourth Amendment reasonable expectation of privacy because of its inherent potential for abuse.

A. Is the ECPA Broad Enough to Encompass E-Mail?

The ECPA governs the issuance and use of "pen-trap" devices.[87] A pen register is a device that "records the numbers dialed on a telephone" but does not record the content of the phone call.[88] A trap and trace device is similar to a caller-ID system; it records incoming telephone numbers.[89] In *Smith v. Maryland*[90] the United States Supreme Court held that the use of a pen register device does not require a search warrant because an individual has no reasonable expectation of privacy in the numbers dialed from her telephone.[91] The Court reasoned that telephone subscribers must realize the company has the ability to record all dialed numbers, for "they see a list of their long-distance (toll) calls on their monthly bills."[92]

FBI officials have concluded that when Carnivore is modified to limit the collection of content, the ECPA grants the FBI pen-trap authorization to use Carnivore to collect TO and FROM information such as an e-mail address from a suspect's Internet account.[93] Thus, the FBI apparently reasons that a telephone number is sufficiently similar to information sent or received via an Internet account. This reasoning, however, stretches the boundaries of statutory interpretation.[94]

The use of Carnivore does not fit into the statutory language found in the ECPA.[95] This lack of express statutory authorization is important because if the ECPA fails to authorize the use of Carnivore, the Government will likely need

---

87. *Id.*

88. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977); *see also* 18 U.S.C. § 3127.

89. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000).

90. 442 U.S. 735 (1979).

91. *Id.* at 742.

92. *Id.*

93. 18 U.S.C. §§ 3121-3127; *see* IITRI REPORT, *supra* note 5, at 3-1 to 3-2.

94. *See* Ted Bridis, *FBI's E-Mail Suggests Divisions On Legality of Web Surveillance*, WALL ST. J., Dec. 7, 2000, at B9 (noting a candid e-mail obtained under the Freedom of Information Act revealed confusion among at least some FBI agents regarding whether the pen-trap laws were applicable to Carnivore).

95. The IITRI report even mentioned that "the language in the pen trap provisions arguably does not clearly apply to electronic communication." IITRI REPORT, *supra* note 5, at 3-2.

to convince a court that, despite the language of the statute, the device still does not violate a reasonable expectation of privacy when used in pen-trap mode. In other words, notwithstanding the ECPA, the Government will likely argue that an individual possesses no legitimate expectation of privacy in the e-mail *addresses* she sends or receives.

Under the ECPA a pen register is defined as a device that identifies "the *numbers* dialed or otherwise transmitted on the *telephone* line to which such device is attached."[96] The statute further defines a trap and trace device as a device that identifies "the originating *number* of an instrument or device from which a wire or electronic communication was transmitted."[97] Carnivore, however, does not record telephone numbers, nor is it attached to a telephone line; rather, it records addressing information, such as e-mail addresses, and is attached to an ISP.[98] Additionally, an e-mail address is unlike a phone number. E-mail addresses provide a greater amount of information than does a mere phone number.[99]

Furthermore, Congress enacted the Communications Assistance for Law Enforcement Act of 1994 (CALEA),[100] which "requires telecommunications carriers and equipment manufacturers to build into their networks technical capabilities to assist law enforcement . . . ."[101] CALEA thus requires phone companies to possess infrastructure that can support surveillance tools such as pen-trap devices. Although CALEA is separate from the ECPA, which allegedly authorizes Carnivore's pen-trap mode, both acts regulate pen-trap devices.[102] In interpreting CALEA, the court in *United States Telecom Association v. FCC*[103] concluded that "CELEA does not cover 'information services' such as e-mail and internet access."[104] Because CELEA has not been extended to cover e-mail addresses, it seems likely that the ECPA will be interpreted in a similar way.

Therefore, the ECPA fails to authorize the use of Carnivore. Congress drafted the ECPA in 1986 when the idea of e-mail communication was in its nascent stages.[105] The ECPA is too narrow to encompass e-mail surveillance because an e-mail address is not a telephone number, nor is it sufficiently similar to such a number. Unless and until Congress passes a statute that

---

96. 18 U.S.C. § 3127(3) (emphasis added).

97. *Id.* § 3127(4) (emphasis added).

98. *See* PRIVACY FOUND., LEGAL ANALYSIS IN RESPONSE TO THE IITRI REPORT ON CARNIVORE, *at* http://www.privacyfoundation.org/pdf/CarnivLT.pdf (last visited Jan. 17, 2001).

99. This argument will be explored further in Part III.B of this Comment.

100. 47 U.S.C. §§ 1001-1010 (1994).

101. United States Telecom Ass'n v. FCC, 277 F.3d 450, 454 (D.C. Cir. 2000).

102. 47 U.S.C. § 1002(a)(2)(B).

103. 277 F.3d at 450.

104. *Id.* at 455. It should be noted that the court concluded this point in dicta and interpreted the words "information services" as including e-mail and internet access. *Id.*; *see also* 47 U.S.C. § 1002(b)(2)(A).

105. 18 U.S.C. § 3127.

addresses e-mail and Internet surveillance, authorization of pen-mode operation should require a Title III court order.[106]

B. Does Carnivore's "Pen-Trap" Mode Collect Too Much Information?

Even if the ECPA could be interpreted to implicitly authorize Carnivore's pen-mode operation, the scope of the information Carnivore collects violates the Fourth Amendment's reasonable expectation of privacy requirement. As discussed in Part II, Carnivore has two modes of operation: pen-trap or full content. Pursuant to wiretapping laws, the legal threshold for obtaining a Title III full content search is more demanding than that required for installing a pen-trap pursuant to the ECPA.[107] In order to tap a phone conversation pursuant to Title III, an agency must obtain a warrant based upon probable cause.[108] In contrast, to install a pen-trap device pursuant to the ECPA, an agent merely must certify that "the information likely to be obtained is relevant to an ongoing criminal investigation . . . ."[109] Thus, the FBI ultimately has a lower threshold to meet if it only operates Carnivore in pen-trap mode. This distinction should not be minimized, for if snooper software over-collects information while operating pursuant to pen-trap authorization, the FBI circumvents the requirements of a Title III court order.[110]

When Carnivore operates in pen-trap mode, it violates an individual's reasonable expectation of privacy in three ways. First, it collects more than mere addressing information.[111] When operating in pen-trap mode, Carnivore captures e-mail addresses sent to and from the suspect's Internet account.[112] While pen-trap mode does not collect the subject heading or content of an e-mail, it does collect the number of bytes transferred in the message.[113] The software represents a unit of data with an "X" in the subject field.[114] Thus, an e-mail sent containing seventeen bytes of data is represented by eighteen *X*s, while an e-mail containing twenty-nine bytes of data is represented by thirty *X*s.[115] This data may seem insignificant, but consider the following

106. 18 U.S.C. §§ 2510-2520.

107. *See* United States Telecom Ass'n v. FCC, 227 F.3d 450, 453 (D.C. Cir. 2000).

108. Before authorizing a wiretap, a judge must find the following: (1) there is probable cause that the suspect committed or will commit a crime; (2) there is probable cause to believe that communications concerning the crime will be obtained through interception; (3) normal investigative procedures have failed, will likely fail, or are too dangerous; and (4) there is probable cause to believe that facilities to be tapped are being used or about to be used to in connection with a specific crime. 18 U.S.C. § 2518(3).

109. 18 U.S.C. § 3122(b)(2).

110. *See supra* note 108.

111. IITRI REPORT, *supra* note 5, at C-3.

112. *Id.* at viii.

113. *Id.* at C-3 ("Recording this information might be an issue of over-collecting because the court order only authorizes collecting e-mail from and to addresses.").

114. *Id.*

115. *Id.*

hypothetical: A judge authorizes FBI agents to use Carnivore to capture e-mail addresses sent to and from a person suspected of violating child pornography laws. While the agents are viewing this information, they notice most messages are small but some are extraordinarily large, perhaps indicating that illegal pictures are being transmitted. Therefore, in some cases the FBI has the ability to ascertain, or at least accurately guess, the nature of an e-mail without first obtaining Title III authorization. If the FBI uses Carnivore as a pen-trap device, the software should at least be configured to capture addressing information only.

Second, the e-mail addressing information is more personal, and thus more revealing, than a phone number. An e-mail address may specifically identify an individual (for example, JohnDoe@aol.com) or at least refer to him in a personal, idiosyncratic manner (for example, BigJohn@aol.com.). A phone number, on the other hand, provides no personal information other than the location from which the phone call was placed. Granted, the FBI can obtain information beyond a mere number by using a tool such as a reverse phone book. However, this additional information will only indicate where the call was placed and who paid the phone bill. It will not necessarily disclose who placed the call. For example, John Doe places a call from work, but FBI agents, using a pen register device on the phone line, may know only that a call was placed from a particular building.[116] However, if the agents were tracing e-mail addresses, they might ascertain that the message was sent from JohnDoe@work.com.[117]

In addition, an e-mail address is more personal than a phone number because that individual has chosen the name for a reason. Perhaps John has a racy side that he only reveals to intimate friends. Thus, he may have an e-mail account which he generally uses, but he may also have an account with a name such as SexyJohn@aol.com. He only uses the latter e-mail account when communicating with certain individuals, wishing to keep this username private from others. In this instance, it is clear how an e-mail address can contain more private information than information accessed with a telephone number. Because an e-mail address is more revealing than a telephone number, obtaining a list of e-mail usernames—many, if not most, of which may belong

116. This hypothetical assumes that John Doe's place of work does not provide personal phone numbers for its employees.

117. For the sake of argument, individuals other than John Doe may actually use the same e-mail address. However, due to an Internet user's relative ease in obtaining a personal e-mail address (for example, setting up a Hotmail account), as opposed to the cost of setting up a personal phone line, it is probably safe to assume that sharing phone numbers is a more common practice than sharing e-mail addresses. *See* Microsoft, Hotmail Registration, MSN Hotmail, *at* http://lc1.law13.hotmail.passport.com/cgi-bin/register?_lang=EN (requiring the following to set up an e-mail account: (1) Internet access from any computer; (2) submission of a name, address, gender, birthday, and occupation; and (3) the selection of a password). Indeed, some people who actually share e-mail addresses may indicate this fact in their username (for example, JohnandJaneDoe@aol.com).

to innocent parties—should not be permitted under the relaxed standards of the ECPA. If Carnivore is operated in pen-trap mode, its scope should be limited to collecting only numerical addressing information such as an IP address.[118] This mode of operation is more closely analogous to operating a pen-trap device on a phone line because only numbers are recorded.

Finally, even assuming *arguendo* that the ECPA authorizes Carnivore's pen-mode operation, the potential for misuse exists. The software is capable of being improperly calibrated and intercepting more information than is lawfully permitted.[119] One of the problems with Carnivore is that both the pen-trap mode and full-content mode are operated using the same software.[120] Indeed, the IITRI report even noted the possible ramifications of this setup: "There is . . . the possibility of unintentional error; for example, clicking the radio button for full collection when the operator meant to click the radio button next to it for pen-trap collection."[121] Perhaps even more remarkable is that there is "no mechanism for detecting or minimizing the likelihood of such an unintentional setup . . . ."[122] Because the government bears a greater burden when obtaining consent for a full content search under Title III,[123] the current pen-trap mode software should be at least separated from the full-content capture software in order to prevent accidental over-collection.[124] Such separation would help eliminate the chance of an accidental or intentional full-content search being performed under mere pen-trap authorization. Furthermore, passwords and authorizations should be different for the separated devices, thereby further removing the possibility of error.

In conclusion, Title III authorization should be required for Carnivore's pen-mode operation because Carnivore collects too much information in this mode.[125] Additionally, an e-mail address is generally identified in connection with an individual, whereas a phone number is more connected to a location. Therefore, an individual possesses a greater expectation of privacy in the e-mail addresses she sends than in the phone numbers she dials.[126] Finally, even assuming statutory authorization, separate software should exist for the pen and full-content modes because the software is capable of being accidentally or

118. *See* MARK A. LEMLEY ET AL., SOFTWARE AND INTERNET LAW 1094 (2000) (defining an IP address as a "numerical identification [such as 1.206.40.130] used to locate a specific computer on the Internet").

119. IITRI REPORT, *supra* note 5, at 4-4.

120. *Id.*

121. *Id.* at 4-10

122. *Id.*

123. 18 U.S.C. §§ 2510-2520.

124. The IITRI Report was sufficiently concerned with accidental over-collection that it recommended separate versions of Carnivore for pen-trap and full content. IITRI REPORT, *supra* note 5, at xiv.

125. *See supra* notes 111-15 and accompanying text.

126. *See supra* notes 116-18 and accompanying text.

intentionally configured to collect full content when only pen-trap collection was authorized.[127]

C. *E-Mail Snooping and the Potential for Abuse*

> *[A]s soon as electronic surveillance comes into play . . . [t]here is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy. . . . Electronic aids add a wholly new dimension to eavesdropping. They make it more penetrating, more indiscriminate, more truly obnoxious to a free society.*[128]

As noted in Part II, in order to have a reasonable expectation of privacy, the individual must possess a subjective expectation of privacy that society deems reasonable.[129] However, despite an expectation of privacy, a search is reasonable if a strong government interest outweighs an individual's privacy interest.[130] Although an individual possesses a legitimate, albeit diminished, expectation of privacy when sending e-mails, Carnivore's use is reasonable if a governmental interest outweighs an individual's privacy interest in cyberspace.[131] On the other hand, Carnivore's use may be inherently intrusive, meaning its very nature intrudes upon all communications passing through the targeted data access point. Therefore, the issue becomes whether an e-mail snooping device capable of being abused is ever reasonable, especially in light of potentially less intrusive alternatives. In other words, is Carnivore inherently too intrusive?

The FBI's current surveillance technology does not foreshadow the coming of the thought police, nor will our communications be relegated to newspeak.[132] Indeed, the Carnivore technology is incapable of making broad sweeps of the entire Internet because the software can monitor only a small group of Internet users for an extended time, or a large group for a short time.[133] In fact, if Carnivore were set to collect all traffic on a link, the 2-Gbyte Jaz disk would be full in eleven minutes.[134] Even if the FBI decided to use an enormous 60-Gbyte disk, it would be full in approximately five to six hours.[135] Furthermore, the FBI currently only taps into a single access point on the ISP's network. This

---

127. *See* IITRI REPORT, *supra* note 5, at xiv (recommending separate versions of Carnivore).
128. Lopez v. United States, 373 U.S. 427, 465-66 (1963) (Brennan, J., dissenting).
129. Katz v. United States, 389 U.S. 347, 353 (1967).
130. Winston v. Lee, 470 U.S. 753, 759 (1985).
131. *See supra* Part II.B.
132. *See* ORWELL, *supra* note 8.
133. IITRI REPORT, *supra* note 5, at 4-4.
134. *Id.*
135. *Id.*

access point will contain only a percentage of the traffic on the ISP's servers.[136] Finally, "Carnivore cannot . . . [b]lock any traffic on the network . . . [s]eize control of any portion of Internet traffic . . . [or] [s]hut down or shut off the communications of any person, web site, company, or ISP."[137]

Despite the fact that Carnivore will not be used to implement an Orwellian regime, the possibility of abuse still exists. For example, (1) overzealous agents or negligent operators may set parameters to collect more information than is subject to a court order;[138] (2) the software is capable of broad sweeps on the access point and, incorrectly configured, can record any traffic it encounters;[139] (3) the software has no mechanism for detecting or minimizing setup error, thus abuse can go undetected and uncorrected;[140] and (4) in the worst case scenario, a rogue FBI agent could use the software to spy on anyone from a suspected criminal to a lover.[141] A reasonable expectation of privacy, however, must contend with the changing nature of our technological society.[142] Thus, the nature of the Internet itself may diminish an individual's privacy interest.[143] In order to determine whether Carnivore's inherent potential for abuse will always make its use unreasonable, it is necessary to apply a Fourth Amendment balancing test that weighs the government's interest in using Carnivore against an Internet user's right to be left alone.

The government's interest behind Carnivore includes the FBI's desire to combat terrorism, computer crime, child pornography, and other felonies conducted or facilitated via the Internet.[144] This is certainly a strong, although broad, interest. However, just as the nature of the Internet may lessen an individual's interest, the government's compelling need also must be diminished by the nature of the Internet.[145] For example, the IITRI report concluded that Carnivore "[c]an be countered with simple, public-domain encryption."[146] If the FBI is targeting criminals such as terrorists, informational warriors, and hackers, then certainly these relatively sophisticated criminals would have the foresight to purchase encryption software, making Carnivore

136. *See Chart Description*, *supra* note 3. The FBI's website did not indicate what percentage of traffic will flow on a given access point, but it did indicate the FBI attempts to filter through as little traffic as possible. *Id.* The FBI claims that an ISP is often able to provide an access point containing only the suspect's transmissions. *Id.* However, "Carnivore can . . . in court authorized counter-cyber-terrorism activities, scan a subset of network traffic." IITRI REPORT, *supra* note 5, at 4-4.

137. IITRI REPORT, *supra* note 5, at xiv.

138. *Id.* at 3-5 ("[T]he potential for human error cannot be discounted—agents must program Carnivore to match the potentially ambiguous information in the court order.").

139. *Id.* at 4-10.

140. *Id.*

141. *Id.* (noting that this type of abuse was beyond the scope of the IITRI report).

142. Sundby, *supra* note 37, at 1758.

143. *See supra* notes 58-64 and accompanying text.

144. *See Carnivore Diagnostic Tool*, *supra* note 9.

145. *See supra* notes 58-64 and accompanying text.

146. IITRI REPORT, *supra* note 5, at 4-8.

completely ineffective as a tool to interpret their communication.[147] As a result, the Carnivore software can only target a smaller percentage of criminals using the Internet.[148] Because Carnivore's effectiveness can be countered by sophisticated criminals, the government's interest is diminished.

On the other hand, the government has a strong interest in effective law enforcement. Using the Carnivore technology is an efficient way to implement e-mail surveillance, especially in the case of national security under the Foreign Intelligence Surveillance Act of 1978 (FISA).[149] For example, if the software is currently being used under a court order, and the suspect sends an e-mail indicating imminent danger such as a bomb, the FBI can quickly intercept the targeted e-mail communication and react appropriately.[150] However, "the mere fact that law enforcement may be made more efficient can never itself justify disregard of the Fourth Amendment."[151] Carnivore's efficiency should, therefore, be measured against current procedures to obtain e-mail, such as issuing a court order to an ISP, who either (1) turns over the contents of a suspect's communications that are stored on the server or (2) creates a clone e-mail account for the FBI's use.[152] Relying on this method could result in a loss of evidence if the content has already been deleted from the server; however, this risk alone should not justify installing a device on an ISP's server, especially when the software's potential for abuse threatens all who share the same data point with the suspect. Therefore, the FBI should refrain from using the device except under the most exceptional circumstances, with the possible exception of a national emergency or a threat to national security. If the FBI does receive authorization to use the software, its use should be limited to the briefest possible amount of time reasonably required to achieve its goal. Such constraints would help to diminish the fear that Big Brother is watching.

Weighed against the government interest is the individual's interest. Although "absolute privacy in modern society is simply unattainable unless one lives the life of a recluse,"[153] one certainly expects that her personal

147. The Carnivore software itself cannot decrypt, but the FBI agents can attempt to decrypt after the encrypted data has been collected. *Id.* at 3-5 to -6.

148. The scope of this Comment is too narrow to discuss implications of FBI decrypting and the procedures and process this would require.

149. 50 U.S.C. §§ 1801-1811.

150. *See* IITRI REPORT, *supra* note 5 at 3-4. Because a field agent may immediately proceed to authorize collection without waiting for judicial approval, the FBI would not have to wait for the ISP to respond to the court order and release information stored on its server. *Id.*

151. Mincey v. Arizona, 437 U.S. 385, 393 (1978). *Mincey* concerned the issue of warrantless searches. *Id.* at 388. The Court's reasoning that efficiency is not a justification to disregard the warrant clause is equally persuasive in determining whether the efficiency of Carnivore helps to justify its use. *Id.* at 393. *Cf.* United States v. Knotts, 460 U.S. 276, 284 (1983) ("We have never equated police efficiency with unconstitutionality . . . .").

152. IITRI REPORT, *supra* note 5, at 3-4.

153. *See* Ashdown, *supra* note 49, at 1315-16; *see also* Sundby, *supra* note 37, at 1758-59 ("Technological and communication advances mean that much of everyday life is now recorded by someone somewhere, whether it be credit records, banking records, phone records, tax

communications will remain reasonably private.[154] Expectations of privacy while using the Internet, however, are mixed and often seemingly contradictory. On the one hand, most individuals are aware that their computer is subject to intrusion by hackers, cookies, or otherwise.[155] Indeed, the sale of "firewalls" to protect invasions and encryption software to prevent disclosure indicate that individuals know that using the Internet may require prophylactic measures to protect their privacy.[156] Thus, an individual's expectation of privacy is somewhat diminished due to the inherent openness of the Internet. On the other hand, an individual may feel *more* secure on the Internet than she would otherwise. After all, one of the benefits of the Internet is anonymity, or at least subjective anonymity.[157] Many people enjoy the free expression found in chat rooms, where individual expression is less inhibited because communication is monitor-to-monitor rather than face-to-face.[158] Moreover, the popularity of online shopping provides another example of expectations of anonymity. Thus, individuals may feel more comfortable ordering goods via an anonymous order form, rather than revealing information such as their waist size, taste in music, or choice of lingerie to a salesperson at the store or on the phone.

Individuals also have a strong interest in preventing a "chilling effect" on their communications. Indeed, individuals may actually feel the FBI is intruding upon their privacy, even when no such intrusion actually occurs. After all, an individual's feeling of security is based upon her perception of privacy. If a person feels she is being watched, then she may decide not to send an e-mail she otherwise would have sent. In other words, Carnivore "chills" free communication.

To illustrate this chilling concept, consider the following hypothetical proposed by Professor Lloyd Weinreb:[159] Weinreb considered the effect of deploying surveillance cameras capable of monitoring every segment of Central Park in New York City.[160] Certainly crime would evaporate, but at a cost.[161] As a result of such monitoring, ordinary people would be inhibited from using the park, for fear that whatever they did, however innocent, might

---

records, or even the videos we rent.").

154. *See supra* Part II.B.

155. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN L. REV. 1193, 1196-97 (1998) (citing a study by Alan Westin, a privacy scholar, finding that eighty-nine percent of individuals polled in the United States were concerned about their privacy).

156. One seller of firewalls has the slogan, "We SECURE the Internet." Checkpoint Software Technologies, *at* http://www.checkpoint.com/ (last visited Mar. 27, 2001).

157. *See* Jonathan D. Wallace, *Nameless in Cyberspace: Anonymity on the Internet*, CATO BRIEFING PAPERS, Dec. 8, 1999, at 6, *available at* http://www.cato.org/pubs/briefs/bp-054es.html.

158. Of course, some people are concerned that anonymous speech is more dangerous on the Internet because of lack of accountability. *Id.* at 5.

159. Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47 (1974).

160. *Id.* at 82.

161. *Id.*

embarrass them if captured by television.[162] Weinreb's hypothetical can be analogized to e-mail surveillance. For instance, if people perceived that their e-mails might be read by the government, this alone might inhibit them from sending e-mails of a highly personal nature. The potenteial chilling effect on speech is an important factor to consider when weighing the individual's interest. E-mail use has skyrocketed in the last decade.[163] Because this is a growing and efficient medium of communication, any external effects which may hinder its use should be closely scrutinized.

Finally, the nature of the software may weigh in favor of the individual. Software is capable of evolving at a rapid pace.[164] Indeed, what was formerly known as "Carnivore," when implemented, will likely be an updated version of the software reviewed by the IITRI Report team. Therefore, who monitors the software? Who ensures that the software is not tweaked to intercept data that previously could not be intercepted by Carnivore? Perhaps the FBI programmers will change the program in a good-faith belief that they have statutory authority to broaden the software's interception capabilities. The IITRI report even concluded there are inherent risks in deploying Carnivore.[165] The report recommended that there be "formal development processes to improve traceability of requirements, improve configuration management, and reduce potential errors in future versions of Carnivore."[166]

In conclusion, Carnivore is an effective and efficient means of assisting the FBI in gathering evidence necessary to prosecute criminals. However, often with the good comes the bad, and Carnivore has side effects which can adversely impact the way an individual uses e-mail. In this regard, Carnivore is inherently intrusive even though the degree of intrusiveness is limited due to the restricted scope of the software.[167] Nevertheless, in light of less intrusive alternatives,[168] but with the possible exception of a national emergency, the use of Carnivore unreasonably intrudes upon a Fourth Amendment expectation of privacy.

IV. CONCLUSION

The unique nature of e-mail presents challenges to law enforcement agencies interested in surveilling this medium of communication. The FBI developed Carnivore in order to facilitate the collection of this electronic

---

162. *Id.*

163. *See* Brief of Amicus Curiae Electronic Frontier Foundation at 5, Intel, Inc. v. Hamidi, No. C033076 (Cal. Ct. App. 1999), *available at* http://www.intelhamidi.com/amicusbrief.htm (citing an E-Marketer report that noted eighty-one million Americans use e-mail, and between September 1998 and November 1999, the number of e-mail boxes grew by sixty-six percent).

164. *See* LEMLEY ET AL., *supra* note 118, at 30.

165. *See* IITRI REPORT, *supra* note 5, at xiv.

166. *Id.* at xv.

167. *See supra* notes 132-37 and accompanying text.

168. *See supra* note 153 and accompanying text.

evidence. An individual, however, possesses a legitimate expectation of privacy in the e-mails she sends. Carnivore violates this expectation by over-collecting information in pen-trap mode and by its inherent potential for abuse. Additionally, the FBI is currently operating in pen-trap mode under questionable statutory authority. Sergeant McGruff tells us to "[t]ake a bite out of Crime."[169] Carnivore may indeed help take a bite out of crime; unfortunately, however, Carnivore's large appetite for devouring crime is supplemented by healthy doses of individual expectations of privacy. When an animal's large appetite causes it to become a threat to humans, it should be put back in the pen or left alone in the wild. Similarly, unless and until the intrusiveness of Carnivore's appetite can be curbed, it should be put back in its cage, only to be removed in case of national emergency.

Manton M. Grier, Jr.

169. *See* Nat'l Crime Prevention Counsel, *McGruff's 20th Anniversary Tour Cities*, *at* http://www.ncpc.org/tour20/eia.htm (last modified Nov. 11, 2000).