Carnivore: Taking a Bite Out of the Fourth Amendment

Frank J. Eichenlaub

Carnivore: Taking a Bite Out of the Fourth Amendment?

INTRODUCTION

The Internet has become an indispensable part of life for Americans in the twenty-first century. Of the 281.4 million individuals living in the United States at the beginning of the new millennium,[1] approximately 123.6 million regularly access the Internet.[2] Americans use the Internet to shop, chat, meet new people, research products or issues, check sports scores or stock prices, and chart their family histories, just to name a few of the uses. The primary use of the Internet, exceeding all other uses by far, is email communication.[3] One study estimates that Internet users will

---

1. MARC J. PERRY & PAUL J. MACKUN, U.S. DEP'T OF COMMERCE, POPULATION CHANGE AND DISTRIBUTION 1990 TO 2000: CENSUS 2000 BRIEF 1 (April 2001), *available at* http://www.census.gov/prod/2001pubs/c2kbro1-2.pdf (last visited Oct. 31, 2001) (noting that the United States' population increased as of April 1, 2000, by 13.2 percent from the 1990 census) (on file with the North Carolina Law Review).

2. Nua Internet Surveys, *How Many Online?*, *at* http://www.nua.ie/surveys/how_many_online/n_america.html (last visited Nov. 12, 2001) (stating that according to NielsonNetRatings, an estimated 166.14 million people had access to the Internet as of August 2000) (on file with the North Carolina Law Review). According to a leading technology industry forecasting firm, "103 million new users will join the ranks of the U.S. online population—a population that will then total 210 million and more closely resemble the overall U.S. populace." International Data Corporation, eBuisness Advisor, *Change in Online Population Will Dictate Changes in eBusiness Market Models* (Aug. 22, 2000), *at* http://www.idc.com/eBusiness/press/EBIZ082500pr.stm (on file with the North Carolina Law Review); *see also* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) (holding unconstitutional several sections of the Communications Decency Act, which prohibited the transmission of obscene or indecent communications sent by telecommunications devices and prohibited sending offensive material to persons under eighteen years of age). In its findings of fact, the district court noted that in 1981 fewer than 300 computers were connected to the Internet. *Id.* By 1993, that number had grown to one million and, when the court handed down its decision in 1996, to 9.4 million. *Id.* The district court noted that by the year 1999 it expected that 200 million individuals would be accessing the Internet. *Id.*

3. *See IDC: Email Deluge Continues with No End in Sight*, SUPPORTINDUSTRY.COM (weekly e.newsletter), Jan. 2, 2001 *at* http://supportindustry.net/newsletter/010201.htm ("E-mail remains the killer [application] for the Internet, evidenced by the many opportunities and challenges facing providers and users of e-mail.") (on file with the North Carolina Law Review) [hereinafter SUPPORTINDUSTRY.COM]. Even during the Christmas 2000 holiday season, more people online used the Internet to communicate than to shop. *See* John Horrigan, *The Holidays Online: Emails and E-greetings Outpace E-commerce*, PEW INTERNET & AMERICAN LIFE PROJECT, Dec. 31, 2000, at 3, http://www.pewinternet.org/reports/pdfs/PIP_Holiday_Report.pdf (pointing out that while fifty-three percent of American Internet users sent e-mail over the holidays, only twenty-

send ten billion e-mail messages over the Internet in 2001, rising to thirty-five billion by the year 2005.[4] Just as Americans employ the Internet for many activities, they also use their e-mail for a multitude of purposes: confirming a dinner plan, conducting business,[5] catching up with a distant friend, selling a product, or soliciting money. Not surprisingly, as Internet and e-mail usage has become common to everyday Americans, it has become common to another, more troubling sector of American society: criminals.[6] According to Donald Kerr, Director of the Lab Division of the Federal Bureau of Investigation (FBI), "In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims."[7]

The law enforcement community has responded in kind by employing the Internet to investigate crimes in which perpetrators use the Internet.[8] Targeting the most popular online use—e-mail—[9]

---

four percent bought gifts online) (on file with the North Carolina Law Review). Horrigan, concludes that "Clearly, the online population sees the Internet more as a tool for information gathering and communications than for commercial transactions." *Id.*

4. SUPPORTINDUSTRY.COM, *supra* note 3.

5. This Comment does not address the question of whether employers are allowed to monitor employee e-mail communications. The Fourth Amendment regulates searches only by governmental actors. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1983) (noting that the Supreme Court consistently has applied the Fourth Amendment protections to proscribe only governmental action). Thus, private employers are exempt from Fourth Amendment regulation. Furthermore, private employers often use internal e-mail systems, which they own and thus control. *See* Bill Gates, *A Recap of 1997 Hits and Misses*, SEATTLE POST-INTELLIGENCER, Dec. 31, 1997, at C1 (predicting that most corporations would use e-mail by the end of 1997). Another question altogether is whether the Fourth Amendment permits the monitoring of public employees' e-mail. For a discussion on the right of public employers to monitor e-mail sent by public employees, see Scott A. Sundstrom, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2102 (1998) (urging courts to adopt a "more robust reading" of the Fourth Amendment, which would protect government employees from suspicionless searches of their e-mail).

6. *See Internet and Data Interception Capabilities Developed by FBI: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 11 (2000) (prepared statement of Donald M. Kerr, Director, Lab Division, FBI), *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm (last visited Nov. 12, 2001) (on file with the North Carolina Law Review) [hereinafter Kerr Statement].

7. *Id.*

8. *See id.* According to the FBI, electronic surveillance has helped to secure the conviction of 25,600 felons in the past thirteen years. *See* FED. BUREAU OF INVESTIGATION, CARNIVORE DIAGNOSTIC TOOL, *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited Nov. 12, 2001) (on file with the North Carolina Law Review) [hereinafter CARNIVORE DIAGNOSTIC TOOL]. In many cases, the evidence could not have been discovered without the use of electronic surveillance. *Id.*

9. *See* SUPPORTINDUSTRY.COM, *supra* note 3.

one such specific response to criminal activity on the Internet is the FBI's "Carnivore Diagnostic Tool,"[10] essentially an online version of a wiretap.[11] Subject to internal FBI rules and to laws that predate the emergence of the Internet by more than a decade,[12] Carnivore allows the FBI to monitor a suspected criminal's e-mail communications.[13] The FBI describes Carnivore as something of a magic wand, which, when "waved" over large volumes of e-mail, can be used to identify and separate targeted e-mails from non-targeted messages without violating the rights of those who use e-mail for lawful purposes.[14] Thus, Carnivore allows the FBI to sift through vast amounts of data, probing particular pieces of e-mail sent to or from particular subjects while leaving all other messages virtually untouched.[15]

However, privacy groups, Internet freedom organizations, and civil liberties groups have all raised questions about Carnivore.[16] The

10. The FBI named the system "Carnivore" because it "get[s] to the meat" of an investigation. *See* CNN.com, *FBI Says Carnivore Will Not Devour Privacy*, *at* http://www.cnn.com/2000/TECH/computing/07/21/fbi.carnivore/index.html (July 21, 2000) (on file with the North Carolina Law Review). In light of the controversy surrounding Carnivore, the FBI may regret choosing a name with such aggressive connotations. One unnamed top FBI official told CNN.com that criticism of the name and the system was "somewhat sobering. We'll think further about [the name] in the future." *Id.*

11. The scope of Carnivore's use depends on the scope of the authorizing interception order. *See* Richard F. Forno, *Who's Afraid of Carnivore? Not Me*, *at* http://www.infowarrior.org/articles/carnivore.html (Aug. 2, 2000) (on file with the North Carolina Law Review). A search warrant may authorize a limited interception. *See id.* For example, the FBI can construct the system to intercept only so-called header information, which is the information at the top of an e-mail message that usually includes the names of the sender, recipient, and the subject of the message. *See id.* Alternatively, the FBI can program Carnivore to intercept the content of messages in addition to the header information. *See id.*

12. The Federal Wiretap Act was passed in 1968 as part of the Omnibus Crime Control and Safe Streets Act. Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (1994 & Supp. V 1999)). The Federal Wiretap Act was amended in 1986 and partly renamed the Electronic Communications Privacy Act. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). See 18 U.S.C.A. §§ 2510–2522, 2701–2711, 3117, 3121–3127 (West 2000) for sections pertaining to the Electronic Communications Privacy Act.

13. Kerr Statement, *supra* note 6.

14. *See id.*

15. The messages are virtually untouched in the sense that they are compared against a Carnivore filter, but they are not opened, read, or inspected, if the system operates correctly. *See* CARNIVORE DIAGNOSTIC TOOL, *supra* note 8; *see also infra* notes 69–72 and accompanying text.

16. *See* CNN.com, *supra* note 10 (quoting the Executive Director of the American Civil Liberties Union as saying, "The FBI's position is essentially, 'Trust us. We're the government.' But we have a long history of the FBI abusing its authority."). According to Deborah S. Pierce of the Electronic Frontier Foundation, "Allowing a system such as Carnivore to be used unchecked by law enforcement exacerbates the problem of over collection of data and has the potential to harm our society." *Statement of The Electronic*

questions include whether Carnivore constitutes an illegal search under the Fourth Amendment,[17] whether the FBI can be trusted to comply strictly with court orders authorizing Carnivore searches,[18] and whether sufficient public oversight of the Carnivore system exists.[19]

Frontier Foundation: Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Congress (2000) (statement of Deborah S. Pierce, staff attorney, Electronic Frontier Foundation), *available at* http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html (last visited Nov. 12, 2001) (on file with the North Carolina Law Review) [hereinafter Pierce Statement]. The Electronic Privacy Information Center has likewise been critical of Carnivore. *See* Ann Harison, *Earthline: FBI Won't Monitor Our Network with Carnivore*, COMPUTERWORLD, July 17, 2000, *available at* http://www.computerworld.com/storyba/0,4125,NAV47_STO47214,00.html (on file with the North Carolina Law Review); Michael Meehan, *Is Carnivore Dangerous? Controversy Continues: Researchers Claim Review of Program Doesn't Go Deep Enough To Say For Sure*, COMPUTERWORLD, Dec. 11, 2000, *available at* http://www.computerworld.com/storyba/0,4125,NAV47_STO54998,00.html (on file with the North Carolina Law Review); *see also* Ted Bridis & Neil King, Jr., *FBI's Wiretaps to Scan E-mail Spark Concern*, WALL ST. J., July 11, 2000, at A3 (quoting a former federal computer-crimes prosecutor's statement that "[i]t's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring. You develop a tremendous amount of information.").

17. *See* Pierce Statement, *supra* note 16. The Fourth Amendment provides:

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

U.S. CONST. amend. IV.

18. *See* Forno, *supra* note 11. Forno offers a critical review of Carnivore and then discusses how Internet users can circumvent the surveillance system:

> The FBI's website . . . calls Carnivore a 'diagnostic tool' versus an electronic eavesdropping device. In reality, Carnivore is indeed a network diagnostic tool . . . but to imply that Carnivore's primary use is as a 'diagnostic tool' is stretching the Bureau's already-thin credibility a bit too far. That's like a criminal claiming that the gun he shot someone with was not a gun but a 'tool' to eject hot lead into a wall.

Id.

19. *See* Pierce Statement, *supra* note 16. According to Pierce, "Currently, there is little if any public oversight over the FBI's use of its Carnivore system. The FBI has not allowed the [Internet Service Providers] to inspect the device, nor have any of the advocacy groups been allowed to examine it." *Id.* While FBI officials proposed allowing certain universities to conduct audits of Carnivore investigations, those academic institutions rejected the FBI's overture, arguing that the FBI proposals called for strict controls that would prevent a truly independent review. Richard Stenger, *Universities Unwilling to Review FBI's Carnivore System: Agency's Restrictions Seen as Overbearing*, *at* http://www.cnn.com/2000/TECH/computing/09/06/carnivore (Sept. 6, 2000) (on file with the North Carolina Law Review). A computer security expert at the Massachusetts Institute of Technology told CNN.com: "Basically, [the federal government] can edit the report, omit sections of the report, and decide never to release it." *Id.*

Additionally, while technology has advanced at lightning speed over the past decade, the laws governing its use have not always kept pace. Carnivore provides one example of this phenomenon.[20] Carnivore equips law enforcement with powerful technology, enabling it to use the Internet as a law enforcement tool.[21] Yet the law governing the proper use of the Internet for investigative purposes is in its infancy, where it exists at all.[22]

Focusing on the FBI's Carnivore system, this Comment explores the constitutional privacy issues implicated when the nation's law enforcement community uses the Internet to investigate crimes, concluding that while the development of a tool like Carnivore is inevitable, modifications to the current system are necessary. In Part I, after detailing the emergence of the Internet, this Comment discusses the Carnivore system in depth.[23] Part II examines the development of Fourth Amendment law, paying particular attention to the legal system's treatment of traditional forms of communication.[24] Drawing the analogy between Carnivore and traditional electronic surveillance,[25] Part III examines the statutory scheme that has arisen from the Fourth Amendment to regulate traditional electronic surveillance.[26] Part IV applies these traditional rules to Carnivore, and concludes that although Carnivore is an inevitable and useful law enforcement tool, the system requires minor adjustments and the present electronic surveillance statutes must be modified to satisfy the legitimate privacy concerns implicated by the system.[27]

---

20. For example, the primary law governing Carnivore interception orders was amended in 1995, well before the development of Carnivore. *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). See 18 U.S.C.A. §§ 2510–2522, 2701–2711, 3117, 3121–3127 (West 2000) for sections pertaining to the Electronic Communications Privacy Act.

21. *See* Kerr Statement, *supra* note 6.

22. *See id.*

23. *Infra* notes 28–117 and accompanying text.

24. *Infra* notes 118–96 and accompanying text.

25. Traditional electronic surveillance includes wiretapping, pen registers, and trap-and-trace devices. *See* Kerr Statement, *supra* note 6 (discussing the FBI's traditional electronic interceptions). A wiretap is statutorily defined as the interception of the wire, oral, or electronic communication of a third party. *See* 18 U.S.C. § 2511(1)(a) (1994). A pen register refers to a device that interprets electronic impulses that identify numbers dialed on a telephone line. 18 U.S.C. § 3127(3) (1994). A trap-and-trace device interprets the incoming pulses on a telephone line and identifies the originating phone number. *Id.*

26. *Infra* notes 197–241 and accompanying text.

27. *Infra* notes 242–60 and accompanying text.

I. THE INTERNET AND CARNIVORE

A. *The Development of the Internet*

In order to provide an adequate foundation for a discussion of Carnivore, this subsection will discuss the development of the Internet, how the events of the developmental era impacted several choices that the Internet's developers made, and how those choices have resurfaced to play a role in the modern day. The Internet is among the positive developments stemming from the decades-long Cold War between the United States and the former Soviet Union.[28] In many ways, the Soviet launch of Sputnik, the first artificial satellite, triggered the Internet's development.[29] Following the success of Sputnik, Americans worried about a communist satellite orbiting over their heads.[30] Additionally, America and its leaders believed that Sputnik provided hard evidence that the Soviets had a technological advantage over the United States that would prove decisive in war.[31]

In response to this perceived threat, President Dwight Eisenhower challenged the nation's scientists and engineers to answer the Soviet threat.[32] In addition to initiating the American space exploration program, the country's scientists began to consider other issues related to modern war, including how to survive a nuclear battle.[33] Key among survival concerns was communications, particularly how Americans would communicate following a nuclear attack.[34] As early as the 1960s, the Department of Defense[35] sought

28. Scott Ruthfield, *The Internet's History and Development: From Wartime Tool to the Fish-Cam*, CROSSROADS: THE ACM STUDENT MAGAZINE, Fall 1995, *at* http://www.acm.org/crossroads/xrds2-1/inet-history.html (last visited Oct. 31, 2001) (on file with the North Carolina Law Review). Ruthfield concludes: "The Internet we use today is one of the few positive legacies of Cold War paranoia, providing efficient and inexpensive communications between people around the world." *Id.*; *see also* ACLU v. Reno, 929 F. Supp. 824, 831–38 (E.D. Pa. 1996) (discussing the Internet's origins, its common present-day use, and the various technologies available with respect to the Internet), *aff'd*, 521 U.S. 844 (1997) .

29. *See* PBS, *Networking the Nerds: The Cold War Heats Up*, *at* http://www.pbs.org/opb/nerds2.0.1/networking_nerds/coldwar.html (last visited Nov. 12, 2001) (on file with the North Carolina Law Review) [hereinafter *Networking the Nerds*].

30. *Id.*

31. *See id.*

32. *Id.*

33. *Id.*; *see also* Ruthfield, *supra* note 28 (noting that the United States government sought to develop a secure network of communication that would survive during war).

34. Ruthfield, *supra* note 28.

35. The Advanced Research Projects Agency (ARPA), a branch of the Department of Defense, funded technology and military research projects. *See* BARRY M. LEINER ET AL., *A Brief History of the Internet, Part I*, E-ONTHEINTERNET, May–June 1997, *available*

to determine whether computers at distant locations could communicate with one another.[36]

Using government funding, scientists began to develop a theory called packet-switching, which forms the basis of current e-mail technology.[37] Under the packet-switching theory, a decentralized computer network first splits a message into small chunks, called packets, and then routes messages from one computer location to another at a remote site.[38] The advantage of the decentralized packet-switching method, as opposed to a centralized system, was clear: if one network broke down or was destroyed during war, the packet could be routed to another network.[39] Additionally, if part of the packet were lost or destroyed, other parts would survive and the intended recipient would receive at least those parts of the message.[40] Under the old centralized system, all information was routed through one source, processed, and then sent to the end source.[41] Thus, if any part of the centralized system failed, the message would not reach its destination. Conversely, using packet-switching, "[w]ith every computer having the same routing abilities, an enemy would have to destroy nearly all computers on the network to make sure that communication lines were dead."[42]

The theory of packet-switching underlies modern e-mail technology.[43] When user *A* sends an e-mail message to user *B*, *A*'s message is broken into small packets when it leaves *A*'s machine.[44] Each packet travels a different route to reach *B*.[45] When the packets reach *B*'s e-mail box, the computer reassembles them into one message, which appears as it was written by *A*.[46]

B. How Carnivore Works

In order to discuss the Fourth Amendment implications of Carnivore, one must first attempt to understand how Carnivore

---

at http://www.isoc.org/oti/articles/0597/leiner.html. At various times, the ARPA also has been called the Defense Advanced Research Projects Agency (DARPA). *See* Ruthfield, *supra* note 28.

36. LEINER, *supra* note 35.
37. *See id.*
38. *See Networking the Nerds*, *supra* note 29.
39. *See* Ruthfield, *supra* note 28.
40. *See id.*
41. *Id.*
42. *Id.*
43. *See Networking the Nerds*, *supra* note 29.
44. *Id.*
45. *Id.*
46. *Id.*

works. Using Carnivore, the FBI can monitor millions of packets handled by Internet Service Providers (ISPs).[47] Most users connect to the Internet through an ISP, which maintains a network and communicates with other networks maintained by other ISPs.[48] ISPs use a technology called "packet-sniffing" to monitor and maintain their networks.[49] Packet-sniffing technology allows ISPs to monitor all the packets streaming through their network or to filter out certain packets if the ISP only wants to monitor precise types of data.[50]

Carnivore is a type of packet-sniffing software.[51] As packets stream through an ISP en route to the intended recipient, Carnivore "sniffs out," copies, and stores particular packets for later review by investigators.[52] According to a review conducted by the IIT Research Institute (IITRI) and the Illinois Institute of Technology Chicago-Kent College of Law,[53] Carnivore can accomplish the sniffing,

47. *See* Jeff Tyson, *How Carnivore Works*, *at* http://www.howstuffworks.com/carnivore.htm (last visited Nov. 12, 2001) (explaining how Carnivore works) (on file with the North Carolina Law Review); *see also* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 67 (2000), *available at* http://www.mttlr.org/volsix/skok.html. An ISP is the entry point for users into the Internet. *Id.* at 65 n.14. The user's modem connects with an ISP's modem, and the ISP then hooks the user into the Internet. *Id.*

48. *See* Tyson, *supra* note 47.

49. *Id.*

50. *Id.*

51. *See supra* notes 49–50.

52. *Id.*

53. STEPHEN P. SMITH, ET AL., IIT RESEARCH INSTITUTE AND ILLINOIS INSTITUTE OF TECHNOLOGY CHICAGO-KENT COLLEGE OF LAW, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT (Dec. 8, 2000), *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf (on file with the North Carolina Law Review) [hereinafter IITRI REVIEW]. The *IITRI Review* was much anticipated since news of Carnivore first broke over the spring and the summer of 2000. The IIT Research Institute (IITRI) and the Illinois Institute of Technology Chicago-Kent College of Law released the 117-page report on December 8, 2000. However, criticism of the *IITRI Review* already existed because the FBI released a draft of the *IITRI Review* in on Nov. 17th. *See* Jennifer DiSabatino, *Update: Carnivore Report Mollifies Some, Leaves Others Leery*, COMPUTERWORLD, Nov. 22, 2000, *available at* http://www.computerworld.com/cwi/story/0,1199,nav47_sto54373,00.html (quoting an Internet-company manager as saying, "I believe, at least at a basic level, that the *IITRI Review* established that Carnivore doesn't bite off more than it can chew. Now we need to put a leash on it and make sure that it's only unleashed under a certain set of circumstances") (on file with the North Carolina Law Review). Another, more critical reaction came from the American Civil Liberties Union. *See* Press Release, American Civil Liberties Union, ACLU Slams Biased Review Team Thumbs-Up for Government Snoopware Program "Carnivore" (Nov. 21, 2000), *at* http://www.aclu.org/news/2000/n112100a.html (on file with the North Carolina Law Review). The ACLU called the *IITRI Review* incomplete because the IITRI was unable to review most of the cases in which Carnivore has been used and called the IITRI team biased because it included several people who had ties to the federal government. *Id.* After "further careful review" of the *IITRI Review*, the ACLU appeared to back off

copying, and storing without interrupting the flow of the ISP's traffic and without interfering with the transmission of the message.[54] More importantly, perhaps, Carnivore is able to conduct "fine-tuned searches" in which the FBI can configure the system to search for extremely particularized pieces of data and thus significantly reduce the risk of gathering non-authorized information.[55]

In addition to software that allows the system to sniff out particular packets, the Carnivore system also includes hardware.[56] After receiving approval to use Carnivore in an ongoing investigation,[57] a technically trained FBI agent[58] works with the special agent conducting the investigation and the ISP to set up the hardware, which includes four components: a one-way tap into the ISP's traffic,[59] a collection computer to filter and collect data, a control computer to examine the data, and a telephone link from the FBI office to the collection computer to connect the control and collection computers.[60] After the system has been constructed at an ISP, the collection computer remains on site for the duration of the surveillance. To prevent on-site tampering, the FBI does not leave a keyboard or monitor at the ISP.[61]

---

the position that the IITRI team was biased and noted that the *IITRI Review* included several unfavorable conclusions regarding Carnivore. *See* Press Release, American Civil Liberties Union, ACLU, EPIC Say Further Study of Carnivore Review Proves "Beast Must Be Tamed" (Dec. 1, 2000), *at* http://www.aclu.org/news/2000/n120100.html (on file with the North Carolina Law Review).

54. IITRI REVIEW, *supra* note 53, § 4.2.7, at 4-7.

55. *Id* § 4.2.3, at 4-4.

56. *Id.* § ES.4, at viii.

57. *See infra* notes 232–41 and accompanying text (describing the steps necessary to obtain such approval).

58. The agent trained in technical matters is not the same agent conducting the investigation. *See* IITRI REVIEW, *supra* note 53, § 3.2.1, at 3-3. The FBI separates the responsibility of configuring the electronic surveillance from the responsibility of conducting the actual investigation. *Id.* § ES.4, at viii.

59. The one-way tap is also called a read-only tap. *See id.* § ES.4, at ix. A read-only tap fulfills the function of allowing the agents to read only the information with which they come into contact, rather than to alter the packets or to initiate a new packet. *Id.* The one-way tap appears to be designed to satisfy the minimization requirements set forth in the Federal Wiretap Act, which require agents "to accomplish the interception unobtrusively and with a minimum of interference." 18 U.S.C. § 2518(4) (1994).

60. *See* IITRI REVIEW, *supra* note 53, § ES.4, at viii. The telephone link allows the FBI to monitor the surveillance from a remote site where the control computer operator is located. *See id.* § ES.4, at ix. The control computer operator can alter the surveillance, start and stop the collection of data, and retrieve collected information. *See id.*

61. *See id.* § ES.4, at viii–ix. Similar to the one-way tap, the coordination between the agents and the ISP is designed to meet the statutory minimization requirements that require wiretapping investigations to be conducted with "a minimum of interference." 18 U.S.C. § 2518(4) (1994); *see also* IITRI REVIEW, *supra* note 53, § 3.2.2, at 3-4 to 3-5. The

Working with the ISP, the FBI agents determine the best location to insert the one-way tap to minimize exposure to non-targeted users.[62] Depending on the scope of the FBI's authority in a particular investigation,[63] the FBI creates filters that allow for the collection of targeted data while preventing collection of other data.[64] At its most restrictive end, Carnivore's default setting rejects all packets.[65] At its least restrictive end, the selection of "a single radio button"[66] switches Carnivore from collecting nothing—its default setting—to collecting all the traffic passing through the data stream.[67] At an intermediate setting, Carnivore is designed to allow for the collection of specifically targeted data, based on a variety of different criteria.[68]

When targeted packets pass through the ISP's data stream and by the FBI's access point, the packets are copied immediately and routed to the collection computer.[69] The copied information then is "compared against" the filter authorized by the court order.[70] But the Carnivore filter is not an everyday filter. According to the FBI, only the information authorized by the interception order actually passes through the Carnivore filter.[71] This seems counter-intuitive. An ordinary filter takes all of one thing, and passes it through the filter,

---

coordinated efforts allow the ISP to offer less intrusive and more precise options for conducting the investigation. *See id.* § ES.4, at viii.

62. *See* CARNIVORE DIAGNOSTIC TOOL, *supra* note 8.

63. Internal FBI rules and informal practice require agents to obtain a court interception order before using Carnivore in an investigation. *See* IITRI REVIEW, *supra* note 53, § ES.4, at viii.

64. *See id.* § ES.4, at ix.

65. *See id.* § ES.4, at xi.

66. The "single radio button" refers to the Carnivore hardware setup, which effectively turns on or off the data collection. *Id.* Among its various conclusions and recommendations, the IITRI was concerned particularly with the "single radio button" aspect of Carnivore. *See id.* § ES.5, at xiii. A simple mistake in configuring a filter has the potential to lead to the collection of information beyond the scope of a court order. *See id.* § 3.2.2, at § 3-5. Although creating the filters is "usually straightforward... the potential for human error cannot be discounted...." *Id.* Possibly complicating the problem is the fact that agents create filters based on information contained in court orders. *Id.* If the court order is ambiguous and the agent converts the ambiguity into a less restrictive filter than the court intended, an over-collection of data may occur. *See infra* notes 107–10 and accompanying text (discussing the shortcomings in Carnivore software with respect to auditing and accountability). When an identified over-collection occurs, the data is sealed and given to a judge. *See* IITRI REVIEW, *supra* note 53, § 4.2.3, at 4-3.

67. *See* IITRI REVIEW, *supra* note 53, § ES.4, at xi.

68. *See id.* § ES.4, at x; *see also infra* notes 91–95 (discussing tests run by the IITRI).

69. *See* CARNIVORE DIAGNOSTIC TOOL, *supra* note 8.

70. *Id.*

71. *See id.*

separating part of the whole from the rest. For example, consider an air filter. An air filter takes all of the air, passes all of the air through a filter, and separates the good from the bad. The Carnivore filter, on the other hand, eliminates what it does not require *before* it reaches the filter.

This distinction may have constitutional implications. If the non-targeted information passes through the Carnivore filter (rather than simply being "compared with" the filter), then the FBI arguably is conducting a search of the information. Under the Fourth Amendment, a government search generally requires probable cause and a warrant.[72] If the non-targeted information does not pass through a filter but instead is picked out before it reaches the filter, as the FBI argues,[73] then a search may not have occurred. This issue could be resolved by reconceptualizing the way a filter works. Perhaps a filter does not need to first search through material before rejecting it. Of course, resolving the question requires a closer review of the Carnivore filter's operation, something the FBI has not yet allowed.[74]

Once the Carnivore filter identifies targeted packets, they pass to permanent storage on the FBI's collection computer.[75] The FBI has stated that non-targeted data is never stored on permanent media, nor is any other information from non-targeted data ever collected.[76] Every day or two, an FBI agent retrieves the captured information with a disk and replaces the disk in the collection computer with another.[77] The information is then used in the investigation of the targeted party and sealed by court order.[78] Under federal law, data collected in violation of federal regulations may be excluded from use

72. *See* Katz v. United States, 389 U.S. 347, 355–59 ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."). The *Katz* test protects citizens from governmental searches when a reasonable expectation of privacy exists. *Id.* at 361 (Harlan, J., concurring). Under the *Katz* tests, courts must determine whether the defendant had a reasonable expectation of privacy and, if so, whether society is prepared to protect that expectation. *Id.* (Harlan, J., concurring).

73. *See* CARNIVORE DIAGNOSTIC TOOL, *supra* note 8.

74. *Supra* note 19 (discussing the FBI's reluctance to allow a detailed examination of Carnivore's source code).

75. *See* CARNIVORE DIAGNOSTIC TOOL, *supra* note 8.

76. *Id.* ("No other data is ever stored to permanent media, nor is any information recorded about the traffic that does not match the filters.")

77. *See* Tyson, *supra* note 47.

78. CARNIVORE DIAGNOSTIC TOOL, *supra* note 8.

at trial.[79] Additionally, federal law provides criminal and civil penalties for violations of electronic surveillance regulations.[80]

C. *Carnivore's Operational Strengths and Weaknesses*

Despite strenuous arguments from privacy groups and civil libertarians,[81] the FBI so far has declined to make available the source

79. 18 U.S.C.A. § 2515 (West 2000). *See also* Gelbard v. U.S., 408 U.S. 50–51 (1972) (permitting grand jury witnesses to refuse to answer questions based on illegal interceptions). *But see* U.S. v. Chavez, 416 U.S. 562, 568–69 (1974) (holding that the government could use information obtained by wiretap even though the government did not fully comply with statutory requirements). In *Chavez*, the defendant sought to suppress wiretap evidence because the wiretap application misidentified the high-level official who approved the wiretap. *Id.* at 569. The Supreme Court held that when the application identified the official as the Assistant Attorney General as the person who approved the order, when in fact the Attorney General had approved the order, that the evidence could be used. *Id.* The Court, however, held that when a lower-level official (the Attorney General's Executive Assistant) approved the wiretap order, the evidence obtained based on that approval could be suppressed. *Id.* at 570. The difference is that Title III contemplates conferring power on certain officials, including the Attorney General and Assistant Attorney General, and not on others. *Id. See also* CARNIVORE DIAGNOSTIC TOOL, *supra* note 8 (noting that "[t]here are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties").

80. Violations of Title III may result in imprisonment of up to five years and financial penalties. 18 U.S.C.A. § 2511 (4)(a) (West 2000).

81. According to David Sobel, General Counsel of the Electronic Privacy Information Center, "If the FBI really wants to provide any type of public assurance as to what Carnivore can and can't do, there is no substitute for releasing that source code." Meehan, *supra* note 16. *See* CNN.com, *Security Firm Tests FBI Limits with E-mail Surveillance Tool*, Sept. 19, 2000, *at* http://www.cnn.com/2000/TECH/computing/09/19/email.surveillance.ap (announcing that a private company is now offering an alternative program to Carnivore that is "open source" so that the public and ISPs can see how it operates) (on file with the North Carolina Law Review) [hereinafter *Security Firm Tests FBI Limits*]. In addition to providing ISPs an alternative to Carnivore, the private company's program, named "Altivore," may have implications with regard to the FBI's ability to use Carnivore in particular investigations. The Federal Wiretap Act requires the FBI to show that "other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c) (1994). This language suggests that when less intrusive investigative procedures exist, the FBI must try these first or show why such procedures would fail or expose agents to danger. Thus, it can be argued that the FBI first would have to ask ISPs to use Altivore to capture information because Altivore is less intrusive by virtue of its open source code and the fact that a non-governmental actor (the ISP) would conduct the search. *See Security Firm Tests FBI Limits*. Providing Carnivore's source code to the public would allow anyone with the capabilities to review the technology to assess the risk to privacy, rather than relying on the FBI's pledge to respect privacy. IITRI REVIEW, *supra* note 53, § 5.9, at 5-4. A non-governmental actor would conduct a less intrusive search in the sense that the investigating entity would not be an entity with the power to reduce one's liberty, as is the case with the government. The Founders apparently felt private searches were at least less problematic because the Fourth Amendment only proscribes searches conducted by governmental actors. *See* United States v. Jacobsen, 466

code of the Carnivore software, citing concerns that public release would allow criminals to learn how to circumvent the system.[82] In its review, the IITRI supports the FBI's decision not to release the source code to the public immediately, but suggests that the agency work toward a public release by eliminating weaknesses in the program that criminals might exploit.[83] In reaching this conclusion, the IITRI's report draws an analogy between Carnivore and wiretapping technology, pointing out that privacy advocates are more comfortable with wiretapping technology because they understand how it works while they still do not understand the mechanics of Internet surveillance.[84] Although releasing the source code to the public would allay some of the concerns of privacy advocates, doing so would not directly address the Fourth Amendment issues that Carnivore raises.[85]

Because the FBI has not released the Carnivore software source code to the public and because the *IITRI Review* offers the closest inspection of the program as a whole,[86] the IITRI's analyses and conclusions[87] necessarily serve as the foundation for any discussion of the program. The IITRI approached its review of Carnivore with several issues already on its agenda,[88] but the team sought out

---

U.S. 109, 113 (1967) (holding that Fourth Amendment protections proscribe only conduct by governmental actors).

82. *See* IITRI REVIEW, *supra* note 53, § 5.9, at 5-4. The *IITRI Review* noted that revealing the source code might provide to criminals who wish to avoid Carnivore surveillance "the keys [with which] to do so." *Id.*

83. *See id.*

84. *See id.* IITRI makes two suggestions: The FBI should release the software code once the exploitable weaknesses are fixed, or the Department of Justice should continue to commission independent assessments of its various surveillance tools. *Id.* Revealing the source code would allow the general public to assess the Carnivore software on its own and would thus allay some of the public's fears. *Id.* In lieu of releasing the software code, the continued review by independent groups would at least allow non-governmental actors to assess Carnivore's uses.

85. *See infra* notes 179–96.

86. In order to conduct its investigation and install the software in its own laboratories, the FBI gave the IITRI access to the Carnivore source code. *See* IITRI REVIEW, *supra* note 53, § 2.3, at 2-2 to 2-3. By installing the software, IITRI was able to run experiments with hypothetical situations to test the capabilities of the system. *See id.* § 2.4, at 2-3; *see also infra* notes 91–96 and accompanying text (describing a few of the tests IITRI performed on Carnivore).

87. *See* IITRI REVIEW, *supra* note 53, § 4.2, at 4-2 to 4-9.

88. *See Id.* §ES.1, at vii. The group's contract with the Department of Justice requested that the review focus on four primary areas. *Id.* The FBI asked whether Carnivore: (1) provides investigators with only the information it was configured to provide; (2) affects the operations or security of ISPs; (3) allows for the unauthorized data collection; and (4) provides operational protections equal to the risk the system presents to privacy. *Id.*

additional areas to address by meeting with groups that have opposed Carnivore vehemently.[89] After meeting with these groups, IITRI's investigation attempted to review: (1) whether Carnivore over-collects or under-collects the information it is authorized to collect pursuant to court order; (2) whether Carnivore imposes any risks to the operation or security of the ISP into whose data stream the system tapped; (3) whether Carnivore risks unauthorized interception by the intentional or unintentional acts of either FBI personnel or anyone else, such as an employee of the ISP; (4) whether Carnivore includes adequate protections that match the accompanying risk of the system; (5) the capabilities of the system as a whole, regardless of the intended and authorized use; (6) the entire process used by the FBI, the Department of Justice, and the courts, with particular attention being paid to the controls on and the auditability of the process; (7) the actual and potential roles of third parties such as the ISP; and (8) the function of the Carnivore software when combined with other software.[90]

As a part of its review, the IITRI conducted thirteen tests, using hypothetical court orders, scenarios, and purposes for collection.[91] The review team constructed one scenario in which Carnivore was configured to collect information contained in the header,[92] including the "To" and "From," but not including information in the "Subject" header.[93] Another test sought to capture the source and destination information for all of "John Doe's" activities on the World Wide Web, in particular including the links "John Doe" accessed at a Web page but excluding information after the Web page was opened.[94] The review team designed a third test to intercept only the packets coming from and going to a "Mary Doe" at a regular e-mail address.[95]

89. These groups include the American Civil Liberties Union, the Electronic Privacy Information Center, and the Center for Democracy and Technology. *See* IITRI REVIEW, *supra* note 53, § ES.1, at vii. *See, e.g.*, Pierce Statement, *supra* note 16 (explaining the Electronic Privacy Information Center's opposition to Carnivore).

90. IITRI REVIEW, *supra* note 53, § ES.1, at vii. The *IITRI Review* expressly set aside addressing or answering questions regarding the constitutionality of the system or the trustworthiness of the agents who will be using the system to conduct investigations. *Id.*

91. *See id.* §§ C.1–C.13, at C-1 to C-32.

92. The header of an e-mail message typically includes the "To," "From," and "Subject" fields at the top of the communication.

93. *See* IITRI REVIEW, *supra* note 53, § C.1.1, at C-1. Incidentally, the review team indicated that Carnivore failed this test. *Id.* The FBI attempted to fix the problem, but the agency only provided a partial solution. *Id.* § C.1.4, at C-3. Carnivore's failure resulted in the FBI's loss because the shortcoming in the software resulted in collection of e-mail that "is not of much use" rather than over-collection. *Id.*

94. *See id.* § C.2.1, at C-4. Carnivore passed this test. *See id.* § C.2.4, at C-5.

95. *See id.* § C.4.1, at C-9. Carnivore passed this test as well. *Id.* § C.4.4, at C-9.

Carnivore failed four of the thirteen tests by not collecting data that matched the review team's configuration criteria; however, only one failure appeared to lead to over-collection of data.[96] The IITRI's review suggests two important conclusions. First, because Carnivore is far from a perfect system, the FBI needs to improve its filtering technology. Second, when the system is configured properly and when it operates according to the configuration, Carnivore may serve as a highly effective and efficient law enforcement tool.

As a general matter, the *IITRI Review* argues that the safeguards in place outweigh the potential risks of the system and therefore tends to support the use of Carnivore in law enforcement.[97] Among Carnivore's operational strengths is the precision with which it can collect data, if it is configured properly.[98] Such precise surveillance, which allows Carnivore to gather large or small pieces of information or any point in between, does not exist in other current technology.[99] The *IITRI Review* also debunks several popular fears underlying much of the concern about Carnivore:[100] that Carnivore could read, record, and store all incoming and outgoing e-mail; that Carnivore could monitor the Web activity of all ISP customers; and that Carnivore could monitor all the other activity of an ISP.[101] The *Review* notes that in order to read, record, and store those messages authorized by court order, Carnivore operates effectively only if it rejects a majority of the packets with which it comes into contact.[102] Thus, the vast number of packets that stream through an ISP, when combined with Carnivore's limited storage capacity, serve as an important practical check against general surveillance.[103]

But Carnivore clearly did not pass the *IITRI Review* easily. The *IITRI Review* identifies at least four problem areas with respect to

96. *See id.* § C.12.4, at C-28. Over-collection occurred in test twelve, which used a hypothetical court order authorizing the collection of certain e-mail messages sent to and from a target that contained the word "planning." *Id.* § C.12.1, at C-27. The test's purpose was to determine whether Carnivore was able to collect e-mail directed to a target containing a particular piece of text. *Id.* During the test, Carnivore collected all of the target's e-mail messages, regardless of whether the messages contained the word "planning." *Id.*

97. *See id.* § ES.5, at xii.

98. *See id.* § 4.2.1, at 4-2.

99. *See id.*

100. *See* Pierce Statement, *supra* note 16.

101. *See* IITRI REVIEW, *supra* note 53, § 4.2.7, at 4-7. Other activities include instant messaging, person-to-person file transfers, Web publishing, news groups, and online purchases. *Id.*

102. *Id.* § 4.2.3, at 4-4.

103. *See id.*

Carnivore's operation. First, in certain situations, Carnivore may over-collect information.[104] This over-collection may result from faulty software[105] and poor design.[106] Second, although auditing is highly important to security and accountability in a software system, Carnivore offers no auditing.[107] Auditing refers to the ability of the FBI to retrace the steps of its agents after the collection has occurred.[108] At the collection computer, the system always operates in "administrator" mode. This means that the FBI cannot conduct audits of individual uses of the system, because everybody who accesses the collection computer does so as "administrator."[109] Similarly, the remote access also does not provide an audit.[110] Third,

104. *See id.* § 4.2.3, at 4-3.

105. *See id.* In one situation, the FBI configured Carnivore to operate only in the "pen mode"—the mode that is supposed to be the effective equivalent of a "pen register"—and only collect information in the "To" and "From" fields. *Id.* However, because the software replaced each character found in the other fields (such as "Subject") with an X, it allowed the testers (and the FBI agents in a real-life situation) to determine the length of the information contained in each of these fields. *Id.* IITRI concludes that such information operates as the equivalent of allowing FBI agents to determine the length of a telephone call, whereas court orders authorizing pen registers only allow the collection of information about who placed the call. *Id.*

106. *See id.* § 4.2.3, at 4-4. Carnivore places the minimal pen register and trap-and-trace equivalents and the full-collection mode in the same device. *Id.* This construction is equivalent to one device allowing for a wiretap, a pen register, or a trap-and-trace, depending on how that device is configured. Faulty configuration thus may result in over-collection, a problem easily fixed by separating the devices. *See id.* § 5.3, at 5-2.

107. *Id.*

108. *See id.* § 4.2.4, at 4-5.

109. *Id.* By requiring a non-investigating technical agent to configure the electronic surveillance, the FBI has arguably created an informal oversight mechanism. This oversight mechanism is extremely limited, however, because the technical agent has no continuing responsibility to monitor the investigating agents' use of the electronic surveillance. Additionally, Carnivore's lack of an auditing function prevents the technical agent from conducting a post-investigation review of the investigating agents' use of the electronic surveillance.

110. *Id.* The remote access software currently in use does not have an audit mode. *Id.* But, even if the software did include an audit mode, an individual could delete any audit because the collection computer is logged in under "administrator," providing no trail to the individual who deleted the audit. *Id.* The lack of an audit function raises the accountability question of whether the FBI can track the actions of individual agents conducting a Carnivore surveillance for later review. Because no audit function exists, a rogue agent conceivably could alter the permissible filter, gather vast amounts of data, then erase any signs that such information had been collected. While the information would be subject to the exclusionary rule because it was collected in violation of the Fourth Amendment, *see* Mapp v. Ohio, 367 U.S. 643, 657 (1961) (ruling that evidence obtained in violation of the Fourth Amendment is excludable in state courts), the information would have some value to an agent conducting an investigation. For example, the evidence might provide the agent with leads not otherwise available. The exclusionary rule is subject to a "good-faith exception," which was enunciated in *U.S. v. Leon*, 468 U.S. 897, 913 (1984) (holding that evidence obtained when officers reasonably relied on a

the *IITRI Review* raised questions about the integrity of the data collected, a concern that has implications for chain-of-custody determinations when the collected information reaches a courtroom.[111] Finally, the *IITRI Review* criticized the "Carnivore development environment," which accounted for the auditing concern in addition to other issues.[112] Because the FBI developers created Carnivore hastily to deal with the emerging problem of crime on the Internet,[113] no formal development process existed.[114] Thus, FBI developers never addressed, or did not fully address, key technical questions.[115]

Although the IITRI concludes that the FBI should continue to use Carnivore despite the problems identified in the review,[116] much larger questions persist, such as why the FBI chose to use a surveillance program with important and troubling deficiencies, and why it chose to do so in the absence of federal statutory controls to regulate such searches.[117] These difficult questions tend to fuel skepticism about Carnivore, despite its operational strengths. The concerns about Carnivore, however, are not limited to skepticism of the system's software. Indeed, the Carnivore system implicates values fundamental to American society embodied by the Fourth Amendment.

II. THE CONSTITUTION AND CARNIVORE

A. *Fourth Amendment Foundation*

Because the federal statutes governing Carnivore are outdated,[118] the FBI and Department of Justice require their agents to comply

---

facially valid search warrant was not excludable, even though it was later shown that the warrant was not supported by probable cause).

111. *See* IITRI REVIEW, *supra* note 53, § 4.2.4, at 4-5.

112. *Id.* § 4.2.6, at 4-6.

113. *See id.* § 1.1, at 1-1.

114. *Id.* § 4.2.6, at 4-7. The IITRI report stated that "[b]ecause of this lack of formal development process, technical issues such as software correctness, system robustness, user interfaces, audit, and accountability and security were not well addressed." The IITRI report further concluded that while the lack of a formal development process was acceptable in the very early stages of development, the continued lack of a formal development process for an operational system is "not appropriate." *Id.*

115. *Id.*

116. *Id.* § 5.1, at 5-1.

117. *See id.* ("Controls on use of Carnivore stem from FBI and [Department of Justice] standards and practices as opposed to statute.").

118. The FBI performs Carnivore searches based on court orders approved pursuant to the Federal Wiretap Act and the Electronic Communications Privacy Act. *See infra* notes 202–47 and accompanying text.

with statutes that regulate more traditional methods of electronic surveillance.[119] The statutory scheme regulating electronic surveillance stems from Fourth Amendment jurisprudence of search and seizure questions.[120] The Fourth Amendment prohibits the government from conducting unreasonable searches and seizures and generally requires the government to conduct searches and seizures pursuant to warrants based on probable cause.[121] The threshold constitutional question, therefore, is whether the government is conducting a search and/or seizure when it uses the Carnivore system. If the answer is "yes," then the Fourth Amendment is implicated and constitutional proscriptions will regulate the search and/or seizure.[122] If the answer is "no," then the governmental actors—here, the FBI—may conduct their investigations without constitutional concerns.[123] Applied to Carnivore, the threshold question must be asked of three sets of individuals: the person who sent the message; the person who

119. *See* Kerr Statement, *supra* note 6.

120. *See infra* notes 197–208 and accompanying text.

121. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring); Wong Sun v. United States, 371 U.S. 471, 481 (1963) (holding that officers were required to obtain an arrest warrant before seizing a suspect based on vague evidence); United States v. Jeffers, 342 U.S. 48, 50–51 (1951) ("Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes."); Agrello v. United States, 264 U.S. 20, 30–33 (1925) (finding a Fourth Amendment violation when officers searched the home of a suspect without a warrant). Under the Fourth Amendment, a governmental actor conducting a search or seizure of a constitutionally protected area generally must obtain a warrant based on probable cause. *Katz*, 389 U.S. at 362; WILLIAM E. RINGEL, SEARCHES & SEIZURES, ARRESTS AND CONFESSIONS § 5.1 (1990) ("[I]t is generally accepted that, absent special circumstances, search warrants are required for all searches in the criminal investigative area."). Although the Fourth Amendment does not expressly require warrants for searches and seizures, it does require that all searches and seizures by governmental actors be reasonable. U.S. CONST. amend. IV. The Supreme Court has interpreted the Fourth Amendment to require warrants based on probable cause to make a search and seizure reasonable. Illinois v. McArthur, 531 U.S. 326, 330 (2001) (upholding a warrantless search); *Katz*, 362 U.S. at 362 (Harlan, J., concurring); RINGEL, *supra*. Several exceptions exist to the general warrant requirement, including searches of automobiles, drunk-driving checkpoints, temporary seizure of luggage, and a temporary stop and limited search for weapons. *McArthur*, 531 U.S. at 330–31.

122. U.S. CONST. amend. IV.

123. A search arguably occurs when any e-mail message gathered by the Carnivore system is subject to an FBI agent's review. A seizure argument is more difficult and requires a close review of the technology. It may be possible to argue that the FBI seizes a message at the point at which the FBI reroutes the message into the Carnivore system, whether or not it passes through the Carnivore filter. *See supra* notes 69–74 and accompanying text. Consider this point in the context of ordinary mail. A seizure would likely occur if an FBI agent intercepted a letter in the U.S. mail, copied it, and then sent the letter on to the intended recipient. Whether this can be analogized to Carnivore requires a close review of the Carnivore technology. The FBI says that it copies messages, which probably means that the original message continues unimpeded. *See supra* notes 75–80 and accompanying text.

received it, and the non-targeted Internet user whose e-mail the FBI rerouted and "compared with" the preordained filter.[124]

Over the past century, the Supreme Court has advanced two tests for determining the scope of the Fourth Amendment.[125] Well into the middle of the twentieth century, the Supreme Court held that the Fourth Amendment applied only to "constitutionally protected areas," basing protection on a bright-line, property-based standard.[126]

---

124. *See supra* notes 69–74 and accompanying text. As to the Internet user whose e-mail is copied and the copy is then rerouted, the threshold Fourth Amendment question is impossible to answer without knowing more about how Carnivore actually operates. *See supra* notes 47–80 and accompanying text. If Carnivore intercepts or inspects the targeted message, it can be argued that a search has occurred. If, however, Carnivore rejects a message before it passes through the system, one can argue that no search has occurred and the Fourth Amendment is not implicated as to this particular person.

125. Despite the Fourth Amendment's more prominent role in today's constitutional jurisprudence, the Supreme Court took nearly 100 years before stepping into the Fourth Amendment arena. *See* Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1100 (1996). Ironically, Mr. Adler's 1996 Note explores the hypothetical situation in which the government possesses a tool that allows its agents to conduct an Internet-wide search, pouring through millions of files but only passing on to authorities those containing illegal activity. *Id.* at 1093. Because Carnivore searches at an ISP access point and does not scan the entire Internet, Adler's hypothetical does not precisely predict Carnivore, but it is eerily prescient. Adler concludes that early twentieth century Fourth Amendment doctrine would protect individuals from such searches, while the "reasonable expectation" doctrine under *Katz v. United States*, 389 U.S. 347 (1967), would not. *Id.* at 1101.

Boyd v. United States, 116 U.S. 616 (1886), represents the Supreme Court's first significant foray into Fourth Amendment law. *See id.* at 1101. In *Boyd*, the Court found protection of property to be at the core of the Fourth Amendment. *Id.* at 630 (finding that a constitutional violation occurs not in "the breaking of [a citizen's] doors, and the rummaging of his drawers . . . but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . ."). The *Boyd* case stemmed from the conviction of members of the E.A. Boyd and Sons firm for violating customs duty. *Id.* at 618-19. The government seized thirty-five cases of plate glass, alleging the firm failed to pay the required duties and citing a federal statute as authority for seizing the property. *Id.* at 617–18. In addition to seizing the plate glass, the government also seized the firm's records and used the documents to convict the members of the firm. *Id.* at 618. In overturning the convictions of the defendants, the Court held that an individual's interest in his own property outweighed the government's interest in prosecuting crime. *Id.* at 631. In reaching this conclusion, the Court examined American and English history. *Id.* at 624–26. According to the Court, the English authorized revenue officers with "writs of assistance" to search suspected places in the colonies for smuggled goods at their discretion. *Id.* at 625. The English practice "was perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country." *Id.* This English practice and resistance to it were in the minds of those who wrote the Fourth Amendment. *Id.*

126. *See* Adler, *supra* note 125, at 1100.

Under the Court's property-based view, only physical trespass onto land violated the protections of the Fourth Amendment.[127]

In its landmark decision in *Katz v. United States*,[128] the Court discarded the property-based doctrine in favor of a balancing approach.[129] Under the *Katz* doctrine, two threshold questions govern an inquiry with respect to whether a Fourth Amendment violation has occurred: whether the defendant has a subjective expectation of privacy, and if so, whether society is prepared to recognize that expectation as reasonable.[130]

In *Katz*, the government placed a bug on the outside of a telephone booth frequently used by a man suspected of illegal gambling.[131] Because the property-based standard governed Fourth Amendment cases when *Katz* reached the Supreme Court, both sides spent considerable time arguing whether the telephone booth was a "constitutionally protected area."[132] However, the Court expressly discarded the property-based standard.[133] "[T]his effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem

127. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that because the government agents made no "actual physical invasion" of the defendants' homes, no Fourth Amendment violation had occurred). Interestingly, *Olmstead*, decided under the active but archaic property-based standard, represents the Supreme Court's first foray into the wiretap issue. *Id.* at 439. The case dealt with a situation in which government agents wiretapped the home and office phones of four suspects, who were charged with and convicted of violating the National Prohibition Act. *Id.* at 455–57. Agents tapped the suspects' telephone lines and recorded their conversations in order to gain the convictions. *Id.* The Court held that "[t]he reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment." *Id.* at 466. Later, in *Silverman v. United States*, the court held that government agents violated a suspect's Fourth Amendment rights when they placed a microphone in the heating duct of the suspect's home. 365 U.S. 505, 511–12 (1961). By crossing into the suspect's physical space and thus the suspect's property, the government violated the suspect's Fourth Amendment rights. *Id.* at 509–10.

128. 389 U.S. 347 (1967).

129. *Id.* at 361 (Harlan, J., concurring). Harlan's concurrence, rather than the majority opinion, created the standard courts today use to evaluate Fourth Amendment claims. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740–41 (1979) (applying Harlan's two-pronged analysis to a Fourth Amendment case).

130. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

131. *Id.* at 348. In rejecting the defendant's argument to exclude the evidence, the Court of Appeals ruled that no Fourth Amendment violation occurred because the government did not physically enter the telephone booth, which was the space the defendant occupied. *See id.* at 348–49.

132. *Id.* at 351.

133. *Id.* at 351–53.

presented in this case. For the Fourth Amendment protects *people, not places.*"[134] After rejecting the longstanding property-based standard, the Court ruled that what an individual attempts to preserve as private may receive constitutional protection, even if the area in which the activity occurs is in public.[135]

The Court then established the new test and the two prongs on which the test turns: whether the individual has a subjective expectation of privacy, and whether that expectation is objectively reasonable.[136] Turning to the facts of the case, the Court held that the defendant entered the telephone booth, closed the door behind him, and thus had a reasonable expectation of privacy.[137] This expectation was also reasonable; to rule otherwise would have been "to ignore the vital role that the public telephone has come to play in private communication."[138]

Rather than solely protecting property rights, the Fourth Amendment after *Katz* protects a wide variety of interests from unreasonable searches and seizures, including one's interest in privacy,[139] security,[140] and liberty.[141]

134. *Id.* at 351 (emphasis added).

135. *Id. at* 351–52 (citing Rios v. United States, 364 U.S. 253 (1960) and *Ex Parte* Jackson, 96 U.S. 727, 733 (1877)).

136. *Id.* at 352.

137. *Id.*

138. *Id.*

139. Winston v. Lee, 470 U.S. 753, 766 (1985) (holding that forcing a suspect to undergo surgery to remove a bullet from his leg sustained during a robbery would violate the suspect's Fourth Amendment rights); *see also* Jones v. United States, 357 U.S. 493, 498 (1958) ("[I]t is difficult to imagine a more severe invasion of privacy than the nighttime intrusion into a private home than occurred in this instance.").

140. Delaware v. Prouse, 440 U.S. 648, 662–63 (1978) (holding discretionary traffic stops unsupported by an articulable and reasonable suspicion unconstitutional because they violate the individual's security interest protected by the Fourth Amendment); *see also* United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976) ("The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and security of individuals.").

141. *See* United States v. Ortiz, 422 U.S. 891, 895 (1974) (citing Camara v. Municipal Court, 387 U.S. 523, 528 (1967) and Schmerber v. California, 384 U.S. 757, 767 (1966)). In holding unconstitutional a search conducted by Border Patrol over sixty miles from the U.S. border, the Court wrote, "the central concern of the Fourth Amendment is to protect liberty and privacy from arbitrary and oppressive interference by government officials." *Id.*

B. *The Fourth Amendment and Cyberspace*

Despite the expanding breadth of the Fourth Amendment following *Katz*, the Supreme Court has yet to rule on whether individuals have a reasonable expectation of privacy in their e-mail.[142] However, applying the two-prong *Katz* balancing test and comparing e-mail to other forms of communication,[143] the Court will almost certainly extend Fourth Amendment protection to e-mail.

Based on the *Katz* analysis, the threshold question when evaluating a governmental action in this context is whether individuals have a reasonable expectation of privacy in their e-mail.[144] If so, the government conducts a "search" for purposes of the Fourth Amendment. Unfortunately, only a few lower court decisions have applied the Fourth Amendment to the Internet, none of which appears to address the circumstances of e-mail.[145] Instead, courts that have addressed the Internet and the Fourth Amendment have dealt with whether a reasonable expectation of privacy exists in two other circumstances: first, when Internet users voluntarily exchange information online; and second, when Internet users share information offline with their ISPs.[146] In both cases, the courts have found no reasonable expectation of privacy.[147] Each of these circumstances is easily distinguishable from e-mail, which arguably entails a greater expectation of privacy.[148]

In a recent formal opinion,[149] the American Bar Association (ABA) addressed whether e-mail communication between clients and

142. *See* Skok, *supra* note 47, at 72. Skok examined whether clickstream data should enjoy Fourth Amendment protection, arguing that it should because Web users have a legitimate expectation of privacy in the data. A clickstream is the footprint Web users create when they visit Web sites. *Id.* at 64. Each time a Web user clicks his mouse, he sends an electronic signal across the Web, and that electronic signal can be tracked. *Id.* "This data can be shockingly revealing, providing a record of the entirety of one's online experience." *Id.* at 64–65. Although Skok concludes that Web users have a legitimate expectation of privacy in clickstream data, he acknowledges that post-*Katz* Fourth Amendment law does not support his conclusion. *Id.* at 64. Rather, he supports his argument by referring to the history of the Fourth Amendment and the intent of its drafters. *Id.* at 62.

143. For example, this Comment will briefly review the protections afforded faxes and cordless telephone communications. *See infra* notes 166–78 and accompanying text.

144. *See* Katz v. United States, 389 U.S. 347, 352 (1967).

145. *See* Skok, *supra* note 47, at 72.

146. *Id.*

147. *Id.*

148. *See infra* notes 179–96 and accompanying text (applying the two pronged *Katz* analysis to e-mail).

149. ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) [hereinafter ABA Opinion].

attorneys violates the ABA's Model Rules of Professional Conduct.[150] The ABA concluded that a lawyer may communicate via e-mail with a client without violating the ABA's Model Rules of Professional Conduct because the medium affords a reasonable expectation of privacy.[151] In reaching its conclusion, the ABA discussed other forms of communication and determined whether each of these forms enjoyed a reasonable expectation of privacy.[152] The ABA reviewed the rules regarding ordinary U.S. mail and commercial mail, land-line telephones, cordless and cellular phones, and faxes.[153] The ABA's report provides useful insight because the Supreme Court likely would employ a similar analysis when it addresses whether e-mail should receive Fourth Amendment protections in the future.

1. U.S. and Commercial Mail

Caselaw supports the ABA's conclusion[154] that a reasonable expectation of privacy extends to U.S. and commercial mail.[155] The ABA noted in its opinion that the reasonable expectation of privacy exists even though mail can be lost, stolen, or misplaced once it leaves the sender.[156] In *Ex Parte Jackson*,[157] the Supreme Court held that letters and sealed packages are protected against unreasonable searches and seizures. Moreover, the Court stated that governmental authorities must obtain a warrant based on probable cause before opening them.[158]

---

150. The ABA issued the Formal Opinion to address whether lawyers could communicate via e-mail with their clients or others about client-related matters without violating the client's expectation of confidentiality. *See* MODEL RULES OF PROF. RESPONSIBILITY R. 1.6(a) (1998). The ABA concluded that a lawyer may communicate via e-mail with a client without violating confidentiality expectations, but should follow the client's instructions with respect to highly sensitive information regarding a client matter. ABA Opinion, *supra* note 149, at 181. The ABA Opinion only addresses Carnivore interceptions of unencrypted e-mail. E-mail is sometimes encrypted, usually using special software programs, to discourage someone who intercepts the message from being able to decipher the content. While some of the e-mail Carnivore targets might be encrypted, certainly most of it is not because encryption technology is not widely used.

151. *See* ABA Opinion, *supra* note 149, at 188.

152. *See id.* at 182–85.

153. *Id.*

154. *Id.* at 183.

155. *See Ex Parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by parties forwarding them in their own domiciles.").

156. *See* ABA Opinion, *supra* note 149, at 183.

157. 96 U.S. at 733.

158. *Id.*

2. Land-Line Telephones

Because the Supreme Court held that a reasonable expectation of privacy exists in the use of a public telephone,[159] the use of a private telephone also will receive Fourth Amendment protection because the expectation of privacy would be even greater. According to the ABA, a reasonable expectation of privacy is "undisputed" in the use of a telephone.[160] The reasonable expectation exists despite the fact that, as with U.S. and commercial mail communications, the telephone is not an absolutely secure medium.[161] Telephone conversations can be intercepted with wiretaps, overheard when multiple extensions exist, and eavesdropped upon when the telephone company commits a technical error.[162] Additionally, under limited circumstances, telephone companies are permitted to monitor conversations.[163]

Similarly, e-mail communications should receive at least the same level of protection as telephone communications. While e-mail communications are not absolutely secure—ISPs can monitor e-mail,[164] e-mail wiretap technology like Carnivore exists, and the potential for transmission error exists[165]—they are no less secure than telephone conversations, and thus deserve at least the same protection.

3. Cordless and Cellular Phones

Prior to 1994, cordless and cellular communications were not afforded the same Fourth Amendment protection as traditional

159. *See* Katz v. United States, 389 U.S. 347, 352 (1967).

160. *See* ABA Opinion, *supra* note 149, at 183.

161. *Id.*

162. *Id.*

163. *Id.*

164. *See* Tyson, *supra* note 47. The Fourth Amendment would not prevent ISPs from monitoring e-mail communications because they are not governmental actors, and the Fourth Amendment only applies to governmental actors. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1967) (holding that Fourth Amendment protections proscribe only conduct by governmental actors). In *Jacobsen*, employees of a private freight carrier examined a white powdery substance coming from a damaged package. *Id.* at 111. They called federal agents, who determined that the substance was cocaine. *Id.* The owner of the package was convicted on drug charges, and, on appeal, asserted that the search violated his constitutional rights. *Id.* The Court held that the private company employees were not regulated by the Fourth Amendment, *id.* at 113, and that the government agents did not violate the defendant's rights because the seizure of the package was not unreasonable. *Id.* at 121–22.

165. For example, a user who misspells an e-mail address will transmit the message to someone other than the intended recipient.

telephone conversations.[166] At least two circuits declined to extend protection to cordless and cellular communications, in part because the absence of protective federal laws undermined a reasonable expectation of privacy.[167] However, the Federal Wiretap Act[168] now prohibits the intentional and unauthorized interception of cordless and cellular communications;[169] thus privacy advocates can make a stronger case that a reasonable expectation of privacy exists.

Nevertheless, cordless and cellular communication expose users to disclosure risks that do not exist with e-mail.[170] Cordless phones use FM and AM radio waves to send signals to base units, which then forward the signal to the land-based lines.[171] The disclosure and interception risks thus include not only the risks associated with traditional telephones, but also the risk that the communication may be intercepted by radios, baby monitors, and other cordless phones.[172] Further, cordless conversations are comprehensible upon interception or disclosure, as opposed to e-mail communications, which are not immediately understandable in digital format.

As with cordless phones, cellular phones present disclosure risks that are not present with e-mail communications. In fact, the risks are greater with cellular phones than with cordless phones because cellular phones transmit radio signals to towers, which then feed the signal to a land line. The distance from the cellular phone to the tower is larger than the distance from a cordless phone to its base unit.[173] The larger area over which the cellular transmission travels increases the possibility of disclosure or interception.[174] Because cordless and cellular telephone communications expose users to a heightened risk of disclosure and interception, the expectation of privacy is correspondingly lower than e-mail communications. E-mail

166. *See* ABA Opinion, *supra* note 149, at 183–85.

167. *See* McKarney v. Roach, 55 F.3d 1236, 1238–40 (6th Cir. 1995); *In re* Askin, 47 F.3d 100, 104–05 (4th Cir. 1995). The cases reflect the dual operation of *Katz's* two prongs: although an individual might have had a first-prong reasonable expectation of privacy in a cordless or cellular conversation, the silence of federal law on the matter undercut the second prong requiring society to accept that expectation as reasonable.

168. Omnibus Crime Control and Safe Streets Act, ch. 119, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (1994)); *see also infra* notes 197–214 and accompanying text (discussing the origins of the Act).

169. 18 U.S.C. § 2511(1)(a) (1994) (prohibiting the interception of wire, oral, or electronic communication).

170. *See* ABA Opinion, *supra* note 149, at 184.

171. *Id.*

172. *See id.*

173. *Id.*

174. *See id.*

communications thus deserve protection greater than cordless and cellular phones and at least equal to that of land-line telephones.

4. Faxes

Communication via fax machine presents risks clearly not present with e-mail messages. The ABA opinion, however, authorizes the use of faxes and concludes that such communication is consistent with the attorney's duty of confidentiality.[175] Risks associated with the use of fax machines include the misdialing of a number and the tendency of faxes to pass through the hands of an intermediary, such as a secretary, before they reach the intended recipient.[176] Despite the risks of interception and disclosure, individuals enjoy a reasonable expectation of privacy in their faxes as illustrated by the fact that the ABA[177] and at least one court have concluded that the use of faxes conforms with the attorney's duty of confidentiality.[178]

Unlike faxes, e-mail messages are sent directly to the e-mail in-box of the intended recipient. Although someone with access to the e-mail message box might open an e-mail intended for another recipient, this risk exists with regular mail as well and thus should not defeat the reasonable expectation of privacy. Thus, because communication sent via fax machines presents a greater risk of interception than communication sent via e-mail and yet still carries a reasonable expectation of privacy, e-mail communication warrants at least as much protection as fax communication.

5. E-mail communications

In most instances, e-mail messages afford greater security than traditional forms of communication, both because of the packet-switching technology at their foundation and the possibility of encryption.[179] As noted earlier, packet-switching technology breaks an e-mail message into several packets, each of which travels over a

175. *Id.* at 185.
176. *Id.*
177. *Id.*
178. *See* State *ex rel.* United States Fid. & Guar. Co. v. Canady, 460 S.E.2d 677, 689 (W. Va. 1995) (ruling that communications sent over fax machines were protected by the attorney-client privilege); *see also* Peter R. Jarvis & Bradley F. Tellam, *High-Tech Ethics and Malpractice Issues*, 1996 SYMPOSIUM ISSUE OF THE PROF. LAW., 51, 55 (1996) (concluding that "courts seem to have taken it for granted that fax machines may be used" when confidential information is communicated).
179. *See supra* notes 37–46 and accompanying text; *see also supra* note 150 (discussing encryption technology).

decentralized network, following a different route to the intended recipient.[180] When the recipient's computer reassembles the packets and the recipient opens the e-mail, the message appears as it did when it left the sender's machine.[181] Thus, intercepting an entire e-mail message as it travels over the decentralized network would require interception at many, indeterminable points.[182] In this respect, e-mail sent using the packet-switching technology is more secure than regular mail and land-line telephone communications.

But not all e-mail users employ packet-switching technology.[183] Some e-mail users configure their modems to dial the intended recipient's modem, and send the e-mail over landlines directly to the recipient's machine.[184] Interception of e-mail using direct dialing requires a sophisticated wiretap. The wiretap must be more advanced than the type used for telephone taps because it not only intercepts the message, but it also deciphers the message in its digital format.[185]

Complicating the analysis is the fact that most people communicate via ISPs.[186] An ISP makes e-mail message boxes available in an online public forum to which other ISP members have access, although passwords protect the message boxes.[187] Additionally, ISPs can and have monitored e-mail communication for various reasons.[188] However, both federal law[189] and internal ISP policies[190] provide limits on such ISP monitoring.

Considering the strengths and weaknesses of e-mail security, the analysis then turns to the two-pronged *Katz* test:[191] Do e-mail users

180. *See supra* notes 37–46 and accompanying text.

181. *See supra* notes 37–46 and accompanying text.

182. *See supra* notes 37–46 and accompanying text.

183. *See* David Hricik, *Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 485 (1998).

184. *See id.*

185. *See* ABA Opinion, *supra* note 149, at 185.

186. *See* Jeffrey Pollock, *A Tangled Web—Thoughts for a Law Firm Using the Web*, 198 N.J. LAW. 18, 19 (1999) (noting that "virtually all" users access the Internet through the ISPs).

187. *See* ABA Opinion, *supra* note 149, at 187–88.

188. *See supra* notes 48–50 and accompanying text.

189. 18 U.S.C.A. § 2511(2)(a)(i) (West 2000) (allowing employees of electronic communication service providers to intercept, disclose, or communicate messages in the normal course of business). This subsection prohibits observing or random monitoring, but an exception exists for mechanical or service quality control checks. *Id.*

190. *See* Hricik, *supra* note 183, at 489. For example, America Online prohibits monitoring of customer e-mail except in three instances: (1) to comply with the law; (2) to protect the rights of America Online; and (3) to monitor e-mail when the company believes someone's safety is at risk. *Id.*

191. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

have a subjective expectation of privacy when they communicate via e-mail? If so, is this privacy interest one that society considers to be reasonable? Because e-mail offers security equal to or greater than U.S. and commercial mail, faxes, and land-line telephone conversations, an e-mail user's expectation of privacy should be equal to or greater than those forms of communication. Courts generally grant these forms of communication a reasonable expectation of privacy, and thus e-mail should receive the same treatment from courts, thereby satisfying the first *Katz* prong.

Applying the second prong to e-mail messages produces a more ambiguous result. While society chooses to protect e-mail messages in certain instances,[192] it has not yet done so in other instances. One glaring example regards interception laws,[193] which do not directly address programs such as Carnivore but cover telephone wiretapping, pen registers, and trap-and-trace surveillance.[194] But, because e-mail clears the first *Katz* hurdle and because society has taken some steps to protect e-mail,[195] courts likely will conclude that e-mail communications warrant protection under *Katz*. Thus, because e-mail communications satisfy the *Katz* analysis, a government agent who monitors or reviews e-mail messages is conducting a search. This search, unless subject to an exception, must be authorized by a warrant supported by probable cause or it is unreasonable and therefore unconstitutional.[196]

III. THE STATUTORY SCHEME

As Fourth Amendment jurisprudence shifted from a property-based standard to a doctrine that balances interests,[197] the laws regulating searches and seizures necessarily evolved in step.[198] The present-day statutory scheme stems directly from the Supreme Court's rulings in *Katz v. United States*[199] and *Berger v. New York*.[200]

192. *See* 18 U.S.C.A. § 2511(1)(a) (West 2000) (prohibiting the interception of electronic communications).

193. *See supra* notes 215–41 (discussing pen trap and trace wiretaps).

194. *See* 18 U.S.C.A. § 2511; *see also* 18 U.S.C. § 3121(a) (1994) (prohibiting the use of pen registers or trap-and-trace devices without court authorization).

195. *See supra* note 189 (noting that federal law prohibits random observation of e-mail by ISPs).

196. *See* U.S. CONST. amend IV.; *supra* note 121 (discussing the warrant requirement and exceptions under the Fourth Amendment).

197. *See supra* notes 118–41 and accompanying text.

198. *See supra* notes 118–41 and accompanying text.

199. 389 U.S. 347 (1967).

200. 388 U.S. 41, 59–60 (1967) (holding that electronic surveillance must satisfy certain requirements, including a warrant describing with particularity the conversations to be

Concerned that the Supreme Court severely hampered law enforcement,[201] Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[202] One provision of the Act authorizes courts to grant warrants permitting interception of wire or oral communications upon a finding of probable cause.[203] The 1968 Act has become popularly known as the Federal Wiretap Act.[204] The Act prohibits the interception of any wire[205] or oral[206] communication by parties other than those listed in the Act[207] and sets forth criteria for obtaining a warrant to conduct surveillance.[208] When the government satisfies the Act, therefore, it fulfills the constitutional obligations with respect to probable cause and the issuance of warrants.

While technology changed over the ensuing years, the Act remained static for eighteen years until Congress amended it in 1986.[209] The amendments, called the Electronic Communication Privacy Act,[210] added electronic communications to the Act's regulations,[211] including communications over computers, digital-display pagers, and fax machines.[212] In addition to extending the same landline communications protections to wireless

collected, probable cause that a crime has been or is being committed, limited surveillance time, names of the suspects, judicial review of the surveillance, and termination when the government collects the information it has been seeking); *see also* James X. Dempsey, *The Fourth Amendment and the Internet*, 607 PRACTICING L. INST. 1015, 1019 (2000) (listing the requirements needed to permit electronic surveillance); Robert S. Steere, Note, *Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 249 (1998) (listing the *Berger* requirements).

201. *Berger*, 388 U.S. at 59–60; *see also* Dempsey, *supra* note 200; Steere, *supra* note 200.

202. Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510–2520 (1994)).

203. *See* 18 U.S.C.A. § 2518(3) (West 2000).

204. *See* Steere, *supra* note 200, at 249.

205. 18 U.S.C.A. § 2510(1) (West 2000) (defining wire communication as "any aural transfer" made through transmission facilities).

206. *Id.* § 2510(2) (defining oral communication as anything "uttered by a person exhibiting an expectation that such communication is not subject to interception").

207. *Id.* § 2511(1)(a).

208. *Id.* § 2516(1).

209. Electronic Communications Privacy Act, Pub. L No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C); *see* 18 U.S.C. §§ 2510–2513, 2516–2521, 2701–2711, 3117, 3121–3127 (1994).

210. 18 U.S.C.A. § 2510(12) (West 2000).

211. *Id.* (defining electronic communication as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system").

212. *See* U.S. DEP'T. OF JUST., ATTORNEYS' MANUAL, § 9-7.100 (1998) [hereinafter ATTORNEYS' MANUAL].

communication, the Act addressed other emerging technology.[213] The Act also established criteria for gaining access to electronic communications and adopted pen register and trap-and-trace regulations.[214]

At the outset, the Act prohibits the interception of the enumerated communications,[215] but it provides an exception for enumerated persons for particular offenses.[216] The Act requires a high-level official in the Department of Justice[217] to authorize an application for a court order to conduct electronic surveillance via wiretap, thus vesting accountability in one person.[218] Applications to judges must be in writing and include an oath or affirmation,[219] another constitutional requirement.[220] Additionally, each wiretap application must include the following: (1) The identity of the person making the application;[221] (2) A full and complete statement of the facts and circumstances on which the applying individual relied to justify the application, including particularity with respect to the offense, description of the facilities being used, type of communication to be intercepted, and identity of the person;[222] (3) A full and complete statement as to whether other procedures to obtain

213. *See* Dempsey, *supra* note 200, at 1021. The Act regulates access to stored wire or electronic communications. 18 U.S.C.A. § 2701 (West 2000).

214. *See id.* For an explanation of pen register and trap-and-trace technology, see *supra* note 25.

215. The Act prohibits the interception of "wire communication" and "oral communication." 18 U.S.C.A. § 2510(1)–(2) (West 2000). "Wire communication" is defined as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection." *Id.* § 2510(1). "Oral communication" is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *Id.* § 2510(2).

216. 18 U.S.C.A. § 2516(1)(a)–(p) (West 2000). The enumerated offenses include murder, kidnapping, robbery, extortion, bribery, counterfeiting, drug-related fraud, firearms violations, and any conspiracy to commit any of these offenses, among several others. *Id.*

217. *Id.* § 2516(1). The high-level officials are the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, any Acting Assistant Attorney General, any Deputy Assistant Attorney General, or any Acting Deputy Assistant Attorney General in the Criminal Division designated by the Attorney General.

218. *See* IITRI REVIEW, *supra* note 53, § 3.1.1, at 3-1.

219. *See* 18 U.S.C.A. § 2518(1) (West 2000).

220. In addition to ensuring that governmental actors obtain a warrant based on probable cause, the Act further satisfies the Fourth Amendment by requiring an oath or affirmation. *See* U.S. CONST. amend. IV.

221. 18 U.S.C.A. § 2518(1)(a) (West 2000).

222. *Id.* § 2518(1)(b).

the information have tried and failed, or may be dangerous,[223] (4) A statement of the time period during which the surveillance will take place;[224] (5) A full and complete statement as to previous surveillance applications regarding the same matter.[225]

The judge may issue a wiretap interception order if the application satisfies the requirements of the Act,[226] the judge finds probable cause, and the court order lists much of the same material as the application, including the name of the target and the time period during which the interception is to occur.[227] If granted, the wiretap interception order allows the government to conduct surveillance "unobtrusively and with a minimum of interference"[228] for no longer than thirty days, although the judge may grant an extension.[229] Once a court has authorized a wiretap interception, the court may request periodic reports.[230] The Department of Justice views the requirements under the Federal Wiretap Act as more restrictive than the requirements of the Fourth Amendment.[231]

Because pen register and trap-and-trace searches are less intrusive than a wiretap,[232] the Act requires less from the government

223. *Id.* § 2518(1)(c).
224. *Id.* § 2518(1)(d).
225. *Id.* § 2518(1)(e).
226. *Id.* § 2518(3).
227. *Id.* § 2518(4).
228. *Id.* § 2518(4)–(5). The minimization requirement is reiterated later: "Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, [and] shall be conducted in such a way as to minimize the interception." *Id.* § 2518(5). The minimization requirement stems from *Berger*, which required the government to limit the surveillance time period and to terminate the surveillance when the information sought had been collected. *See* Berger v. New York, 388 U.S. 41, 59–60 (1967).
229. 18 U.S.C.A. § 2518(5) (West 2000).
230. *See id.* § 2518(6).
231. *See* ATTORNEYS' MANUAL, *supra* note 212, at 9-7.100. The *Attorneys' Manual* states, "[S]everal of Title III's provisions are more restrictive than what is required by the Fourth Amendment." According to the *Attorneys' Manual*, one such provision requires federal investigative agencies to submit interception-order requests to the Department of Justice for review and approval before they are submitted to a court. *Id.*
232. While a wiretap allows the interception of conversations, pen registers and trap-and-trace devices collect only numeric information, including numbers dialed from a certain location and numbers dialed to a certain location from another telephone. *See, e.g.*, United States v. Brown, 351 F. Supp. 38, 39–40 (W.D. N.C. 1972) (excluding evidence obtained by a wiretap that was not authorized pursuant to the Federal Wiretap Act). The court concluded that the "[l]egislative history of the statute... demonstrates... that Congress intended that wiretapping—that extraordinary invasion of the Fourth Amendment right against unreasonable searches and seizures—should be treated by the Justice Department as a serious business." *Id.*

to conduct such surveillance.[233] For example, rather than requiring high-level Department of Justice approval, a pen register or trap-and-trace application requires only an application by "an attorney for the Government."[234] If the application satisfies the requirements of the Act, the court *must* issue an order authorizing installation of a pen register or trap-and-trace device.[235] Conversely, under the Act's wiretap provisions, the court has discretion as to whether to issue a warrant authorizing surveillance.[236]

Thus, the statutory scheme seeks to codify the Fourth Amendment requirements set forth in *Katz* and *Berger* that governmental actors conduct searches with a warrant that is based on probable cause.[237] The scheme raises the procedural bar by requiring high-level Department of Justice approval for the most intrusive surveillances,[238] mandating minimization of intrusions,[239] and limiting the duration of the search.[240] The requirements for gaining approval for electronic surveillance, therefore, exceed the requirements for typical search warrants, which may be granted by a magistrate and are unlimited as to what offenses are covered.[241]

IV. REGULATING CARNIVORE

While Congress may have considered e-mail communication when it amended the Federal Wiretap Act in 1986, it could not have predicted the ubiquitous presence of e-mail in today's culture and probably did not anticipate a mechanism like Carnivore.[242] As a

233. *See* 18 U.S.C. § 3122(a) (1994).

234. *See* 18 U.S.C.A. § 2518(3) (West 2000) ("[T]he judge *may* enter an ex parte order....") (emphasis added).

235. *See* 18 U.S.C. § 3123(a) (1994) ("[T]he court *shall* enter an ex parte order....") (emphasis added).

236. *See* 18 U.S.C.A. § 2518(3) (West 2000) ("[T]he judge *may* enter an ex parte order....") (emphasis added).

237. *See* Steere, *supra* note 200, at 249.

238. 18 U.S.C.A. § 2516(1) (West 2000).

239. 18 U.S.C.A. § 2518(3) (West 2000).

240. *Id.* § 2518(5).

241. *See* Dempsey, *supra* note 200, at 1019.

242. Congress passed the Electronic Communication Privacy Act in 1986, predating the massive growth of the Internet in the 1990s. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C); *see* 18 U.S.C. §§ 2510–2522, 2701–2711, 3117, 3121–3127 (1994). For a discussion of the development of the Internet during the past two decades, see ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996) (striking down as unconstitutional sections of the Communications Decency Act), *aff'd* 521 U.S. 844 (1997). Between 1989 and 1996, Internet usage grew by 100 times, from fewer than 90,000 computers in 1989 to more than 9.4 million computers connected to the Internet by 1996. *Id.*

result, the statutory scheme Congress designed to govern surveillance of cellular phones, cordless phones, and computer-to-computer technology[243] now regulates an interception device that Congress probably never contemplated. The question, therefore, is whether the present statutory scheme adequately regulates the use of Carnivore as a surveillance tool.

The statutory scheme governing surveillance grew directly out of Supreme Court decisions defining the Fourth Amendment.[244] The Fourth Amendment, as defined by the Supreme Court over the course of the twentieth century, protects citizens against unwarranted intrusions by the government.[245] "The basic purpose of the Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials. The Fourth Amendment thus gives concrete expression to a right of the people which is basic to a free society."[246] Responding to the Supreme Court's guidance, Congress passed laws to codify these decisions and ensure that law enforcement officials met the Fourth Amendment principles the rulings advanced.[247] By subjecting its agents using Carnivore to the statutory requirements of traditional electronic surveillance, the FBI hopes to ensure that its agents meet the constitutional standards that the Supreme Court enunciated.

As a general proposition, the use of Carnivore by government agents likely will meet the Fourth Amendment's requirements and the statutory scheme advancing the Amendment's principles. Absent bad faith, most agents will conduct searches no broader than allowed by law and by particular court orders. Even if the FBI configured Carnivore to operate at its most invasive settings—collecting all the information about a targeted suspect that passes through a data stream—the collection would be no more invasive than a wiretap. Carnivore is capable of conducting far less invasive searches as well, gleaning as little information from an e-mail message as the identities

243. *See* Dempsey, *supra* note 200, at 1019.

244. *See* Steere, *supra* note 200, at 249.

245. *See* Maryland v. Wilson, 519 U.S. 408, 411–12 (1997); Katz v. United States, 389 U.S. 347, 361 (1967); Berger v. New York, 388 U.S. 41, 59–60 (1967); *see also* Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 85 (1974) ("The privacy secured by the [F]ourth [A]mendment fosters large social interests. Political and moral discussion, affirmation and dissent, need places to be born and nurtured, and shelter[ed] from unwanted publicity.").

246. Camara v. Municipal Court, 387 U.S. 523, 528 (1967).

247. *See supra* notes 198–202.

of the sender and recipient.[248] If FBI agents follow the statutorily mandated procedure and gain approval to deploy Carnivore, the agents will likely meet their Fourth Amendment obligations requiring searches and seizures to be regulated by a warrant supported by probable cause.[249]

Several operational issues, however, complicate the analysis of adequate regulation, the most troubling of which involves the exposure to non-targeted communications. When FBI agents conduct a wiretap and listen to conversations, they are only exposed to conversations on the telephone for which they have a court's authorization to monitor.[250] The same is not true for Carnivore searches. When FBI agents tap into an ISP's data stream, the tap necessarily exposes every packet that flows through that data stream, even those packets not authorized for interception and search by court order.[251] The FBI, using Carnivore, avoids collecting non-authorized information by relying on Carnivore's filters, which match the court order to particular packets and allow only the targeted packets to be stored.[252] But the filters do not eliminate or even diminish the FBI's exposure to the non-authorized information in an ISP's data stream, because it is currently technologically impossible to isolate a single data stream that carries only those packets sent to a targeted person. Rather, the FBI must tap into a broader data stream, which carries both targeted and non-targeted information, and allows the Carnivore filters to weed out the non-targeted messages. Compare this technology to telephones, which allow taps to be placed on a single line and thus expose only conversations that cross that particular line. As long as the FBI is tapped into the ISP's system, it necessarily is exposed to communications it has no authorization to monitor.

The danger, of course, is that Carnivore will collect information beyond what a warrant allows and thus will violate a person's Fourth Amendment rights. Over-collection might occur as a result of innocent human error in configuring the Carnivore filter.[253] But a

248. *See supra* notes 62–68 and accompanying text.

249. *See supra* notes 237–41 and accompanying text.

250. *See* IITRI REVIEW, *supra* note 53, § 3.1.1, at 3-1 to 3-2. If the agents hear conversations that exceed the scope of the court order, then they are required to turn off the wiretap so that they do not collect information beyond that which they are authorized to collect. *See id.*

251. *See id.* § ES.4, at xi.

252. *See id.* § ES.4, at xi–xii.

253. In fact, the IITRI notes that the potential for such an error is present and compounded by the fact that the FBI constructs the filters based on interception orders.

more troubling over-collection would occur when an agent intentionally exceeds his authority. Without question, purposeful over-collection is the precise type of activity the Fourth Amendment and the statutory scheme prohibit.[254]

Just as over-collection may occur with Carnivore, it may also occur with traditional forms of surveillance. For example, an agent might overhear conversations outside the scope of a court order while conducting a wiretap, either inadvertently or purposefully. The troubling difference between Carnivore and traditional surveillance, however, is that Carnivore allows exposure to a significantly greater volume of non-authorized information. In addition to exposing agents to non-authorized information involving the target of an investigation, Carnivore exposes agents to non-authorized information involving non-targets.

Compounding the issue of over-collection is the fact that Carnivore does not provide for auditing.[255] Without even minimal auditing, the FBI is unlikely to notice and punish purposeful over-collection. Carnivore's inability to audit agents severely diminishes agent accountability and seriously erodes the deterrent purpose of the Fourth Amendment.[256]

A final factor complicating the issue of over-collection involves the FBI's decision to include in one device the ability to conduct wiretap-equivalent as well as a pen register or trap-and-trace equivalent searches.[257] Simply clicking one button can switch Carnivore from a low collection mode (the equivalent of a pen register or a trap-and-trace) to its highest collection mode (the equivalent of a wiretap).[258] Thus, both a simple mistake and an

---

Id. § 3.2.2, at 3-5. An unclear order may result in the creation of a filter that does not match the specifications of the order. *Id.* The problematic filter then may either overcollect or undercollect. *Id.* During the course of its review, the IITRI discovered a case in which an agent did not fully understand a court order. *Id.* The FBI asked the U.S. Attorney to gain approval for another court order to eliminate the ambiguities and allow for the construction of an appropriate filter. *Id.*

254. Wolf v. Colorado, 338 U.S. 25, 27 (1949) ("The Security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society.").

255. *See id.* § 4.2.4, at 4-5. "Auditing is crucial in security. It is the means by which users are held accountable for their actions. There is no auditing in Carnivore." *Id.*

256. *See* Steere, *supra* note 200, at 236 (noting that the exclusionary rule "operates as a deterrent to government agents who violate the Fourth Amendment by excluding evidence seized as a result of such conduct . . .").

257. *See* IITRI REVIEW, *supra* note 53, § 5.3, at 5-2.

258. *See id.* Among its recommendations, the IITRI suggests that the FBI separate these functions into two devices. *Id.*

unnoticed purposeful act have the same result: the vast over-collection of information.[259] In a system with no auditing and very little accountability, the simplicity with which one can alter the parameters of a search is troubling.

A statutory scheme designed to regulate systems such as Carnivore could easily handle the issues of over-collection, auditing, and accountability. But the FBI deployed Carnivore before Congress considered the system and was able to respond to concerns about the technology with legislation. As a result, the dated statutory structure predictably fails to cover all of the sharp edges of a new technology.

Although the public may be under-protected in certain circumstances when Carnivore is deployed, the public may be over-protected in other situations. Depending on the scope of an interception order, Carnivore is capable of conducting a wide variety of searches and collecting various amounts of information.[260] Every use of Carnivore must satisfy the Federal Wiretap Act, even when some deployments fall far short of collecting as much information as would be obtained with a wiretap. For example, Carnivore can be configured to capture information equivalent to a pen register or a trap-and-trace device. Carnivore would only be used in this way after satisfying wiretap laws, which require the approval of a high-level official in the Department of Justice. A traditional pen register or trap-and-trace search, however, requires a lower level of approval.[261]

While over-protection should not be a cause for alarm for privacy advocates, the circumstances to which the over-protection can be attributed should cause concern. Over-protection in this context is yet another symptom of the outdated statutory scheme regulating Carnivore. Similar to the over-collection issue, over-protection exists because the laws regulating Carnivore never contemplated such a system and thus are ill-equipped to deal with the new technology.

259. It is equally true to say that a simple mistake or purposeful act could lead to the vast undercollection of information, but an undercollection does not raise constitutional violations with respect to agents exceeding their authority.

260. Carnivore is capable of acting as a wiretap, collecting entire e-mail messages, or as a pen-register or a trap-and-trace device, collecting information indicating who sent a message and to whom it was intended to reach. *See supra* notes 50–55 (discussing the scope of information collected via a wiretap, pen-register, and trap-and-trace device).

261. *See* 18 U.S.C. § 3122(a) (1994) (allowing "[a]n attorney for the Government" to apply for a court order authorizing a pen register or trap-and-trace search).

V. CONCLUSION

In an age of ever-expanding technological promise, Carnivore represents the nation's first journey into the use of the Internet as a law enforcement tool. Even Carnivore's harshest critics do not dispute that the system has the capability of serving as a highly effective law enforcement tool.[262] Carnivore can conduct broad searches that gather large chunks of information and smaller searches that collect specific pieces of information, or it can collect any amount of information between these extremes. Carnivore accomplishes these collection tasks without interfering with ongoing communications or with the systems over which these communications are conducted.

But Carnivore has several glaring and troubling deficiencies, several of which implicate the values our nation protects with the Fourth Amendment. Without the ability to audit agents who conduct investigations, Carnivore fails to provide a means by which the public can be assured that the system is used properly. Without an auditing function, Carnivore further fails to offer assurances to the public that the system will not be abused due to the lack of accountability. Therefore, the important deterrent function of the Fourth Amendment suffers greatly.

In addition to the operational shortcomings of Carnivore, another serious problem exists with respect to the system: The present statutory structure governing electronic surveillance is inadequate to regulate the use of Carnivore. Congress enacted the two statutes regulating electronic surveillance, the Federal Wiretap Act and the Electronic Communications Privacy Act, without comprehending the possibility of a system as powerful as Carnivore. Neither statute speaks adequately to the issues of over-collection of information; exposure to non-authorized and non-target communications; or the lack of auditing, accountability, and thus deterrence. Congress drafted the two statutes in response to Supreme Court decisions dealing with electronic surveillance, and they have served as the baseline that government actors must cross in order to satisfy the Fourth Amendment. Because statutes do not satisfactorily address the over-collection, exposure, and auditing and accountability issues, and because each of these problems could arise during every Carnivore search, the Carnivore system requires a new statutory model.

262. *See* Pierce Statement, *supra* note 16.

While Carnivore offers law enforcement a number of attractive strengths in conducting investigations in the Internet age, it presents troubling problems that require Congress's attention. Congress must investigate the Carnivore system, considering the system in light of past Fourth Amendment electronic surveillance jurisprudence, and tailor a statute that answers the legitimate privacy concerns that critics have raised. The statute should require Carnivore to include an auditing function that will satisfy the current accountability shortcomings. In addition, because Carnivore exposes governmental actors to so much non-authorized and non-targeted information, the statute should require stricter judicial oversight than is required with traditional electronic surveillance. Finally, the statute should provide harsh penalties for Fourth Amendment violations that occur due to intentional over-collection of information. The penalties should exceed those allowed by the statutes presently in place because the potential and opportunity for over-collection with Carnivore vastly exceeds abuse of traditional methods of electronic surveillance. While Carnivore has a role to play in American law enforcement, its present operational deficiencies and the antiquated statutory scheme regulating the system threaten to undermine the values protected by the Fourth Amendment.

FRANK J. EICHENLAUB