Washington University Journal of Law & Policy

Volume 11 *Promoting Justice Through Interdisciplinary Teaching, Practice, and Scholarship*

January 2003

# Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?

Stephen W. Tountas
*Washington University School of Law*

# Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?

Stephen W. Tountas*

## INTRODUCTION

On July 11, 2000, the Wall Street Journal[1] lifted the two-year shroud of secrecy on the Federal Bureau of Investigation's (FBI) "Carnivore"[2] program. The FBI designed Carnivore to sift through the contents of a suspect's e-mail and, when appropriate, to record the suspect's e-mail address for further review. In response to privacy concerns, the FBI pointed to the rise in cybercrime as a national security threat justifying the use of programs such as Carnivore.[3] In July of 2001, despite much criticism,[4] the FBI announced its goal to

---

* J.D. Candidate, 2003, Washington University School of Law.

1. *See* Neil King, Jr. & Ted Bridis, *FBI's System to Covertly Search E-Mail Raises Legal Issues, Privacy Concerns*, WALL ST. J., July 11, 2000, at A3 (revealing that an unidentified internet service provider refused to comply with the FBI's order to install Carnivore on its system).

2. The program is currently known as DCS1000, but for the purposes of this Note, will be referred to as Carnivore. The FBI changed the program's name to curtail future controversy, particularly over the running joke that its operation "eats away" at constitutional liberties. *See* Matt McLaughlin, *FBI's Upgrade of Carnivore Includes a New Name*, GOV'T COMPUTER NEWS (Feb. 12, 2001), *available at* http://www.gcn.com/vol1_no1/daily-updates/3661-1.html.

3. *See Fourth Amendment Issues Raised By The FBI's "Carnivore" Program: Hearing Before the House Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 11 (2000) [hereinafter *Fourth Amendment Issues*] (statement by Dr. Donald Kerr, Director of the FBI's Lab Division, finding that a wide variety of cybercrime threatens the safety, security, and privacy of others).

4. *See* Press Release, American Civil Liberties Union, ACLU Urges Congress to Put a Leash on "Carnivore" and Other Government Snoopware Programs (July 12, 2000), *at* http://www.aclu.org/news/2000/ n071200b.html; Electronic Privacy Information Center's Carnivore FOIA Litigation, *at* http://www.epic.org/privacy/carnivore; Michael Kirkland, *Analysis: Bringing the FBI to Heel*, United Press Int'l (Aug. 22, 2001) (describing the legislative movement to remove Carnivore from the FBI's control).

further curtail crime by expanding Carnivore's capabilities[5] to include the monitoring of both incoming and outgoing wireless messages.[6]

Although the FBI initially faced significant opposition to the usage and expansion of Carnivore, opinions drastically changed[7] after the September 11, 2001, terrorist attacks.[8] Within months of the attacks, an increasing amount of evidence surfaced to support the FBI's contention that Osama bin Laden coordinated the assault by using both the Internet and wireless technology.[9] This evidence reawakened the public to the merits of federally regulating electronic communication[10] and prompted Congress to implement new legislation to combat cybercrime.[11]

Rather than ending the debate, the new legislation begs the question of whether Carnivore is a legally viable means to combat cybercrime. Moreover, regardless of Carnivore's constitutionality, a policy question emerges as to whether national security requires

---

5. *See*, *e.g.*, Robert O'Harrow, Jr., *FBI's 'Carnivore' Might Target Wireless Text*, WASH. POST, Aug. 24, 2001, at E1 (discussing the possibility of Carnivore's expansion to wireless technology); Erich Luening & Ben Charny, *Carnivore to Add Wireless to its Menu?*, ZDNET NEWS (Aug. 24, 2001) (explaining how Carnivore could become the de facto means to monitor wireless communications), *at* http://zdnet.com.com/2100-1105-272144.html.

6. Wireless messaging involves sending short phrases through the numbered keypad of a cellular phone, "blackberry," or paging device. Approximately 20 billion text messages were sent during 2000, 750 million of which were sent in North America. *See* Simon Romero, *A Nation Challenged: The Surveillance; Bigger Brother in the Wireless World,* N.Y. TIMES, Sept. 24, 2001, at C10.

7. *See*, *e.g.*, Caron Carlson & Dennis Callaghan, *I Need to Read Your E-Mail*, EWEEK, *at* http://www.eweek.com/article2/0,3959,113740,00.asp (Sept. 24, 2001) (discussing how even the most principled civil liberty groups will concede the need for increased regulation, but only when it will lead to a drastic improvement in national security).

8. *See*, *e.g.*, Tim Golden, *A Day of Terror: The Operation; Terrorism Carefully Synchronized and Devastatingly Effective*, N.Y. TIMES, Sept. 12, 2001, at A13 (providing a detailed account of the September 11, 2001 terrorist attacks).

9. *See infra* notes 64-68, 103 and accompanying text.

10. *See*, *e.g.*, Romero, *supra* note 6 (explaining that, because "terrorists may have used wireless technology to coordinate the attacks, [it] has breathed new life into efforts to monitor even the most arcane and complex features of wireless networks"); Judith Lockwood Purcell, *Wiretaps: Not To Worry, Yet*, WIRELESS WEEK, Sept. 24, 2001, at 4 (stating that "[i]n the two weeks since attacks on the World Trade Center and the Pentagon, wireless carriers have seen a significant upsurge in requests for cell phone records and wiretaps").

11. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act].

Congress to disregard the inherent drawbacks of electronic surveillance by law enforcement agencies.

Part I of this Note focuses on the judicial and legislative histories of the federal wiretap provisions and establishes the legal foundation for surveillance tools such as Carnivore. Part II discusses the FBI's development and expansion of Carnivore and introduces the various facets of cybercrime that the FBI aims to prevent. Part III applies the modern wiretap provisions to Carnivore's current incarnation, assessing whether wireless regulation is a legal exercise of the FBI's authority. Part IV posits whether any legally viable alternatives to Carnivore exist and, if not, whether Carnivore is a necessary evil for winning the war against cybercrime. Lastly, Part V summarizes the findings and concludes the Note.

## I. JUDICIAL AND LEGISLATIVE EFFORTS TO OVERSEE THE MONITORING OF ELECTRONIC COMMUNICATION

The Fourth Amendment to the Constitution of the United States[12] formally creates and protects a right to privacy for all U.S. citizens.[13]

---

12. U.S. CONST. amend. IV. 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.

*Id.*

13. For a discussion on the origins of the Fourth Amendment, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999), explaining:

> To make sense of the [Fourth A]mendment, we must go back to its framing. At that time, the legal protection against the invasion of privacy was trespass law. If someone entered your property and rifled through your stuff, that person violated your common law rights against trespass . . . . The law gave an officer an incentive to obtain a warrant before he searched; if he was uncertain, or wanted to avoid all risk of liability, he could first check his judgment by asking a judge . . . . The weak link in this system was the judge. If judges were too lax, then warrants would be too easy to get . . . . Having seen much abuse of the power to issue warrants, the framers were not keen to give judges control in determining whether the government's searches were reasonable . . . . [Thus, t]he framers required that judges, when issuing warrants, name particularly "the place to be searched, and the persons or things to be seized," so that judges would not be able to issue warrants of general power. The immunity of the warrant would be limited to particular people and places, and only when probable cause existed to issue the warrant.

In *Olmstead v. United States*,[14] the U.S. Supreme Court first considered whether telephone conversations could receive Fourth Amendment protection and held that they could not.[15] The Court explained that, despite its trend to liberally construe the Fourth Amendment,[16] it could not equate an "interception" with a wiretap that did not physically intrude on Olmstead's house, paper, or effects.[17] Therefore, the Court's approach under *Olmstead* established that, unless the FBI obtains its evidence from an area that could be physically trespassed upon, its collection would neither require a warrant nor infringe upon Fourth Amendment protections.

Justice Brandeis dissented sharply, finding that the government's collection of phone conversations clearly violated the Fourth Amendment.[18] Brandeis reasoned that wiretapping allows the FBI to potentially overhear both confidential and intimate information.[19] He further cautioned that the Constitution must be viewed in light of the changing conditions, such as technology,[20] in modern society.[21]

---

*Id.* at 112-13.

14. 277 U.S. 438 (1928). In *Olmstead*, the government placed a wiretap on the office telephone line of its suspect and collected a significant amount of incriminating evidence. *Id.* at 456. The wiretap's installation never constituted a trespass on Olmstead's property, as the government inserted small wires into the telephone lines of other resident houses. *Id.* at 457.

15. *Id.* at 466. The government collected evidence over a series of months, indicating Olmstead's involvement in a conspiracy to illegally import, possess, and sell liquor. *Id.* at 455-57.

16. *See*, *e.g.*, Boyd v. United States, 116 U.S. 616, 635 (1886) (finding that "constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right"); Gouled v. United States, 255 U.S. 298, 304 (1921) (finding that the "[Fourth Amendment] should receive a liberal construction, so as to prevent stealthy encroachment upon or 'gradual depreciation' of the rights secured by them, by imperceptible practice of courts or by well-intentioned but mistakenly over-zealous executive officers").

17. 277 U.S. at 465. The Court further reasoned that people who install a telephone must intend to project their voice outside of their house, which would inevitably run through an exterior phone line, and, thus, would not be protected by the Fourth Amendment. *Id.* at 466. *See also* LESSIG, *supra* note 13, at 115 (explaining that "[t]his conclusion was received with some surprise, and also with shock. Already much of life had moved to the wires. People were beginning to understand what it meant to have intimate contact 'online'; they counted on the telephone system to protect their intimate secrets.").

18. 277 U.S. at 479.

19. *Id.* at 475-76.

20. Justice Brandeis's views were well ahead of his time, particularly with respect to advanced surveillance technology. Brandeis cryptically predicted that:

Accordingly, Brandeis contended that the government commits espionage and violates the Fourth Amendment when it engages in warrantless wiretaps.

Almost forty years later in *Katz v. United States*,[22] the Court formally adopted the views expressed in Justice Brandeis's dissent and overruled the traditional *Olmstead* approach.[23] In *Katz*, the Court held that the Fourth Amendment does not permit the FBI to obtain or introduce any phone conversation recorded without a warrant.[24] The Court found that the Fourth Amendment extends to the recording of oral conversations that are overheard without committing trespass under local property law.[25] Thus, a seizure of evidence need not

---

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

*Id.* at 474.

Professor Lawrence Lessig views Justice Brandeis's dissent as a cornerstone for cyberlaw, proclaiming:

> If there is a justice who deserves c-world's praise, if there is a Supreme Court opinion that should be the model for cyberactivists in the future . . . it is this Justice, this opinion, and this case. Brandeis gave us a model for reading the Constitution to preserve its meaning, and its values, across time and context. It is a method that recognizes what has changed and accommodates that change to preserve something of what the framers originally gave us.

LESSIG, *supra* note 13, at 116.

21. 277 U.S. at 472-73 (Brandeis, J., dissenting). This contention is based on Brandeis's characterization of the Constitution as a living document whose interpretation is subject to change. He stresses that a vital principle "must be capable of wider application than the mischief which gave it birth. This is peculiarly true of constitutions . . . . They are . . . 'designed to approach immortality as nearly as human institutions can approach it.'" *Id.* at 473 (quoting Cohens v. Virginia, 19 U.S. (6 Wheat.) 264, 387 (1821)). *See also* LESSIG, *supra* note 13, at 115 (explaining that "Brandeis acknowledged that the Fourth Amendment, as originally written, applied only to trespass. But it did so . . . because when it was written trespass was the [only] technology for invading privacy.").

22. 389 U.S. 347 (1967).

23. *See supra* notes 14–17 and accompanying text.

24. 389 U.S. at 348. Here, the FBI collected its evidence by attaching a recording device to a public pay-phone, from which the suspect frequently placed his calls. *Id.*

25. *Id.* at 353. The Court further extrapolated that "the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, [thus,] it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id.* Moreover, the Court stressed that these concerns do not vanish based on the location of the FBI's search and will protect an individual against an

physically intrude on the suspect's property to receive Fourth Amendment protection and, therefore, must be accompanied by a warrant when obtained via wiretap.[26]

In the wake of *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[27] This statute established a strict set of procedural guidelines with which the FBI must comply to intercept[28] electronic information.[29] First, Title III altered the procedure for enforcement agencies seeking a wiretap, requiring a written application[30] to a judge of proper jurisdiction along with a showing of probable cause.[31] Second, the judge who receives the application must affirm that probable cause actually exists before approving the issuance of a wiretap.[32] Congress justified this radical departure based on two key concerns: first, to prevent arbitrary violations of personal privacy and, second, to protect

---

unreasonable seizure, wherever he or she may be. *Id.* at 359.

26. *Id.*

27. Title III, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified in 18 U.S.C. §§ 2510-22 (1994)).

28. Title III defines 'intercept' as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1994).

29. Title III defines 'electronic communication' as:

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

18 U.S.C. § 2510(12) (Supp. IV 1998).

30. The application must include: the identity of the officer seeking the wiretap; a full and complete statement of the facts and circumstances relied on by that officer; a statement whether other investigative procedures have been tried, or why they would fail; a statement of the anticipated time frame to intercept communications; and a statement whether previous applications were made to intercept the communications of the same person. 18 U.S.C. § 2518 (1)(a)-(f) (1994).

31. *Id.* § 2518(3).

32. *Id.*

communication itself.[33] As a result, Title III eliminated any ambiguity remaining after *Katz*[34] and heightened the procedural requirements that all enforcement agencies must follow when applying for a wiretap.

The Court first addressed Title III's strict guidelines in *Smith v. Maryland*,[35] holding that a legal distinction exists between evidence recorded by a pen register[36] and evidence collected by wiretap.[37] In *Smith*, the Court refused to extend Fourth Amendment protection to information collected by a pen register, finding that such collection neither searches nor seizes evidence.[38] Furthermore, the Court explained that a person does not have a reasonable expectation of privacy for a phone number, which phone companies routinely record for billing purposes.[39] Thus, unlike a wiretap, the collection of readily accessible information, such as a phone number, will not receive Fourth Amendment protection and can be freely collected without a warrant.

---

33. *See* S. REP. NO. 1097, 90th Cong., 2d Sess. 66, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153; *see also* Gelbard v. United States, 408 U.S. 41, 50-51 (1972) (stating that Title III was enacted as a "protection for 'the victim of an unlawful invasion of privacy' . . . . [,] to protect the privacy of communications, [and] . . . the integrity of court and administrative proceedings."). Several years later, Congress furthered Title III's progress by enacting the Privacy Act of 1974, which minimized the types of information that could be collected. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552(a) (1988)).

34. Although *Katz* universally protected against unreasonable seizures of evidence, it failed to establish the procedural guidelines for an enforcement agency to follow when seeking a wiretap. 389 U.S. 347 (1967). In effect, Title III's changes instilled a strict set of guidelines to theoretically protect against any potential for governmental abuse.

35. 442 U.S. 735 (1979).

36. *See generally* New York Tel. Co. v. U.S., 434 U.S. 159, 161 n.1 (1977) (defining a pen register as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.").

37. 442 U.S. at 744-45.

38. *Id.*

39. *Id.* at 741-42. Unlike oral communication, the collection of phone numbers is distinct in that a person generally knows that the numbers dialed from a phone can potentially be accessed by a phone company for billing purposes and fraud. *See generally* New York Tel. Co., 434 U.S. at 174-75 (finding that pen registers are often used by phone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of the law").

The *Smith* Court further explained that the suspect assumed the risk of divulging this evidence, as he voluntarily conveyed information that the phone company was capable of recording. 442 U.S. at 745. It is important to note, however, that these findings have no bearing on the privacy of actual phone conversations and is limited in scope to the privacy of outgoing phone numbers. *Id.* at 744-45.

In 1986, Congress amended Title III with the Electronic Communications Privacy Act (ECPA)[40] to institute a set of procedural guidelines for obtaining a pen register.[41] In effect, the ECPA creates a hierarchy of governmental standards, most notably a strict standard for wiretapping and a more flexible standard for obtaining pen registers.[42] Moreover, under the ECPA's hierarchy, a pen register that is installed without judicial authority yields less restitution than an unauthorized wiretap.[43] Thus, even though the ECPA functions to establish procedural guidelines for pen registers, it still reinforces *Smith's* notion that a pen register should receive less protection than a wiretap.[44]

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA)[45] to further advance the

---

40. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-22, 2701-09, 3121-27 (1994)). For a detailed discussion of the statutory changes enacted by the ECPA, see S. REP. NO. 99-541 (1986), *available at* WL S. Rep. 99-541.

41. 18 U.S.C. §§ 3121-27 (1994). An officer applying for a pen register need only show "the identity of . . . the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation[, along with] a certification . . . that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." *Id.* § 3122(b)(1)-(2).

42. *Compare* 18 U.S.C. §§ 2510-22 (1994) (establishing the standard for obtaining a wiretap) *with* 18 U.S.C. §§ 3121-27 (establishing the standard for obtaining a pen register). In particular, whereas a wiretap must be accompanied by a showing of "probable cause," a pen register need only be "relevant" to an ongoing criminal investigation. *See* 18 U.S.C. § 2518(3)(a) (requiring a showing of probable cause to receive a wiretap); § 3122(b)(2) (requiring that the information be "relevant to an ongoing criminal investigation" to receive a pen register).

Additionally, a wiretap is limited to the investigation of specific felonies, such as counterfeiting, aircraft piracy, or the sale or distribution of narcotics. *See* 18 U.S.C. § 2516(1)(a)-(o). In contrast, pen registers are subject to no such limitation, as the guidelines for specific crimes are left entirely open-ended. *See generally* 18 U.S.C. §§ 3122-3127 (failing to limit a pen register's scope to an enumerated set of felonies).

Finally, whereas the FBI may operate a pen register for sixty days, the duration for operating a wiretap is only thirty days. *See* 18 U.S.C. § 2518(5) (stating that a wiretap may be in effect no longer than thirty days); 18 U.S.C. § 3123 (c)(1) (stating that a pen register may not be used for a period longer than sixty days).

43. *Compare* 18 U.S.C. §§ 2518(10)(a), 2520 (allowing a person whose rights are violated by an illegal wiretap to move for a suppression of evidence and to receive civil damages) *with* § 3121(d) (stating that "[w]hoever knowingly violates [the pen register requirements] shall be fined under this title or imprisoned not more than one year, or both").

44. *See supra* notes 38–39 and accompanying text.

45. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 18 U.S.C. §§ 2510-2522 (1994)).

government's role in modern surveillance.[46] Generally, CALEA mandates that a provider of electronic service[47] must assist in the installation of pen registers and wiretaps on its system when law enforcement requests as such.[48] Further, the Act requires the internet service provider (ISP) to limit the device's access to the specific information that the government is cleared to monitor.[49] Lastly, CALEA mandated that all networks have the ability to accommodate authorized electronic surveillance by October 25, 1998.[50] These changes permit the monitoring of a wireless packet-switched network that remains connected at all times,[51] thus, bridging the gap between the ECPA and modern law to facilitate the implementation of

---

46. *See* H.R. REP. No. 103-827, pt. 1 (1994) (discussing the need to implement advanced forms of technology to maintain the government's role in electronic surveillance).

47. The United States Code defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (Supp. IV 1998).

48. *See* 18 U.S.C. § 2518(4) (1994) (stating that "[a]n order authorizing the interception of a wire, oral, or electronic communication . . . shall, upon request of the applicant . . . furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively").

49. *See* 47 U.S.C. § 1002(a)(2) (1994) (requiring a carrier to "expeditiously isolat[e] and enabl[e] the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier").

50. *See generally* Press Release, Federal Communications Commission, In the Matter of: Communications Assistance for Law Enforcement Act CC Docket No. 97-213 (Apr. 20, 1998) (soliciting public suggestions on the appropriate standard for the wireless industry) (on file with author); Heather Forsgren Weaver, *Anti-Terrorism Legislation Hits Civil Liberties Wall*, RCR WIRELESS NEWS, Oct. 1, 2001, at 3 (explaining how CALEA gives the authority to allow wiretaps on packet-mode data).

Due to the objections of several wireless providers, such as AT&T and Lucent, the FCC extended its deadline until June 30, 2000, to allow the industry to develop the appropriate technology. *See* Press Release, Federal Communications Commission, FCC Adopts Extension of CALEA Compliance Date (Sept. 11, 2000) (providing an extension of two years to develop the technology required by CALEA standards), *available at* http://www.fcc.gov/Bureaus/Wireless/News_Releases/1998/nrwl8039.html.

In 2001, the FCC denied the wireless industry's appeal for a blanket extension, but gave providers until November 19, 2001, to either bring themselves within compliance with packet-mode communications or seek individual relief. *See* Press Release, Federal Communications Commission, FCC Denies Blanket Extension For Packet-Mode Communications, Temporarily Suspends CALEA "Punch List" Deadline (Sept. 19, 2001), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/News_Releases/2001/nrcc0137.html.

51. *See*, *e.g.*, J. William Gurley, *Making Sense of the Wireless Internet*, CNET NEWS, Aug. 14, 2000 (explaining how a packet-switched network differs from a circuit-switched network), *at* http://news.com.com/2010-1072-281347.html?legacy=cnet. In general, a packet-switched network remains online at all times, whereas a circuit-switched network is only accessed at limited times through the use of a modem over an ordinary phone line. *Id.*

governmental surveillance.

On September 11, 2001, seventeen terrorists collectively hijacked four airplanes flying within the United States and crashed them into both the World Trade Center in New York and the Pentagon in Washington, D.C.[52] In response to this catastrophe, Congress enacted the USA Patriot Act (Patriot Act),[53] radically altering federal wiretap and pen register provisions.[54] First, the Act specifically states that pen registers may be used to collect information transmitted both over the Internet and among computer networks.[55] Second, the Act extends the jurisdiction of all pen registers across the United States, abandoning the traditional limitations placed upon the issuing court.[56] Third, the Act requires an enforcement official to file for a special court order to attain the pen register.[57] Lastly, the Act requires an ISP that is hosting a surveillance device to supply the court with the name of the officer who installed the program, the date of installation, and the configuration under which it is programmed to search.[58] By making judicial approval more easily obtainable for electronic communications monitoring, these changes are evidence of congressional endorsement of the Carnivore technology.

In sum, while the law still preserves a hierarchy for obtaining wiretaps and pen registers,[59] it has come a long way since the original

---

52. *See*, *e.g.*, Tim Golden, *A Day of Terror: The Operation; Terrorism Carefully Synchronized and Devastatingly Effective*, N.Y. TIMES, Sept. 12, 2001, at A13 (providing a detailed account of the September 11th terrorist attacks on the United States).

53. *See* Patriot Act, *supra* note 11. The Patriot Act overwhelmingly passed in the Senate by a vote of 98-1 and in the House of Representatives by a vote of 357-66. *See, e.g.,* David Lerman, *Critics Say Patriot Act Could Impose on Civil Liberties*, DAILY PRESS (Oct. 28, 2001), *at* http://www.dailypress.com/news/columnists/dp-1795cm0oct28.column (on file with author).

54. The Patriot Act has far-reaching implications in many facets of surveillance and terrorism that are not relevant to this Note. Such changes include long-arm jurisdiction over money launderers, forfeiture of funds in U.S. interbank accounts, and a prohibition against harboring terrorists. For a complete discussion of the Patriot Act's changes, see U.S. DEP'T OF JUSTICE, FIELD GUIDANCE ON NEW AUTHORITIES (Redacted) (2001) [hereinafter Field Guide], *available at* http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf.

55. *See* Patriot Act, *supra* note 11, § 216. The DOJ explains that the Act revised "[r]eferences to the target [phone] 'line' . . . to encompass a 'line or other facility.' Such a facility might include, for example, a cellular telephone number . . . [or] an Internet user account or e-mail address." *See* Field Guide, *supra* note 54, at 7.

56. *See* Patriot Act, *supra* note 11, § 216.

57. *Id.*

58. *Id.*

59. *See supra* notes 30-32 and accompanying text.

approach in *Olmstead*. Thus, although electronic information is still somewhat protected, the potential remains for governmental abuse.

## II. CARNIVORE AND ITS TARGETS

### *A. A Free Reign of Terror: The Growth of Cybercrime*[60]

The past decade featured an expansive growth of various types of cybercrime.[61] In response to this dilemma, the FBI developed Carnivore to ensure the safety and security of others by monitoring crimes such as terrorism, information warfare, child pornography, and securities fraud.[62] An understanding of the prevalence and severity of these crimes is an essential component to understanding whether efficient regulation requires technology, such as Carnivore, to further curtail its growth.

Although most communications sent through the Internet are benign, nefarious e-mails containing the plots of high-profile terrorist organizations have continued to increase at an alarming rate.[63]

---

60. Cybercrime covers an expansive area of the law, but for the purposes of this Note, will be limited in its scope to a brief overview of the key problem areas.

61. For a detailed analysis on the growth and impact of cybercrime, see Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (Apr. 2001). Professor Katyal states that:

> [C]ybercrime is becoming an increasingly common form of criminal activity. The numbers are staggering. The number of recorded computer security incidents grew from 6 in 1988 to more than 8000 in 1999. Theft on the internet caused $ 2 billion in losses in the year 1995, a number that is much higher today. One company has found 100,000 instances of illegal activity on web sites in one and a half years . . . . Last year, there were more than 22,000 confirmed attacks against Department of Defense computers. It is no surprise that the FBI's caseload has skyrocketed as a result of these trends.

*Id.* at 1014-15 (citations omitted).

62. *See Fourth Amendment Issues*, *supra* note 3, at 11 (statement by Dr. Donald Kerr, Director of the FBI's Lab Division).

63. *See Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987 and H.R. 4908 Before the House Subcomm. on the Const. of the Comm. on the Judiciary*, 106th Cong. 33 (2000) [hereinafter *ECPA 2000*] (statement by Donald Kerr explaining the growth of online terrorist activity). In particular, Kerr explains that "[t]errorist groups are increasingly using new information technology . . . to formulate plans, raise funds, spread propaganda, and communicate securely. . . . [T]errorist groups, 'including Hezbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida [sic] organization are using computerized files, E-mail, and encryption to support their operations.'" *Id.*

Terrorist organizations typically send e-mail through ISPs that offer anonymous registration and Internet access at no cost to the user.[64] If an act of terrorism occurs, the FBI will attempt to recover the suspect's e-mail history from an ISP's records but may discover that the requisite data has already been purged.[65]

Aside from the difficulties in tracing a suspect's digital trail, techniques such as encryption and steganography[66] serve to further complicate the FBI's monitoring of a terrorist's Internet usage. Recent attacks illustrate a growing propensity to utilize steganography, as suspects attempt to conceal their directives within their laptops or computers; such files, presumably, were electronically transferred from one computer to another.[67]

---

64. *See*, *e.g.*, Lisa M. Krieger, *Terrorists Use Low and High-Tech Communication Yet Evade Detection*, SAN JOSE MERC. NEWS, Oct. 10, 2001 (reporting that suspects sent hundreds of e-mails through Hotmail and Yahoo, in Arabic and English, prior to the September 11, 2001, terrorist attacks); Farhad Manjoo, *Terrorists Leave Paperless Trail*, WIRED NEWS, Sept. 20, 2001 (indicating that the "digital trail identified after the [World Trade Center] attacks—such as the use of e-mail addresses that can be created anonymously at a Kinko's store—were of the type that couldn't have been detected unless authorities were physically following the suspects").

65. James Whittaker, a Professor at the Florida Institute of Technology and expert on computer security, states that "[a]lthough some e-mail programs store messages automatically, publicly accessible computers usually are purged on a daily or monthly schedule . . . . While a record of the e-mail would remain on a computer hard drive, it would stay there only until it was overwritten by something else." Scott Wyman & Sally Kestin, *FBI Tracks Internet Role in Terrorist Plot*, SUN-SENT. (Ft. Lauderdale, Fla.), Sept. 18, 2001, at 7A; *but see* Jim Puzzanghera, *Terrorists' Internet Use May Betray Them; FBI Is Following Up on Tracks They Left Behind*, MIL. J. SENT., Sept. 21, 2001, at 14A (stating that even though bin Laden's network uses free e-mail, it "employ[s] advanced computer software [to cover its tracks] . . . [, b]ut even a sophisticated computer user would not know how to delete every trace or record of the messages from a computer's hard drive").

66. For a discussion on steganography, see J. William Gurley, *From Wired to Wiretapped: Forget Privacy Rights. The Real Problem With Government Snooping is That it Won't Work,* FORTUNE, Oct. 15, 2001, at 214. Gurley explains that steganography is:

> the act of embedding or hiding a message inside a seemingly innocent digital vessel. Several programs on the Internet, many of which . . . are free to download, make it easy to embed one file in another . . . . These encoding techniques are so slick that the resulting file is indistinguishable to the human eye or ear. As a result, a covert communication may appear as innocent as two parties sharing a . . . song over the Internet. USA Today has reported that Osama bin Laden and his followers are heavy users of steganography.

*Id.*

Additionally, steganography is extremely difficult to detect, as it requires a comparison of the data content between the suspected imagery with its original; if steganography occurred, the

Accordingly, terrorists are not only evading authorities through anonymous e-mail, but are utilizing modern technology to further complicate the FBI's surveillance.

Similar to terrorism, the possible use of "information warfare"[68] raises concerns over the susceptibility of a country's critical infrastructure.[69] Recent intelligence points to the possible future use of such tactics as a means to counter the strength of the U.S. military.[70] Likewise, in the past decade, hackers have launched a number of cyber-attacks against the electronic infrastructure of the United States, thereby exposing its vulnerability to more egregious

---

data-size of the image's current version will be substantially larger. Greg Wright, *Terrorists Leave Footprints Across Internet: Policing Poses Rights Dilemma*, DENV. POST, Oct. 8, 2001.

67. *See* Katyal, *supra* note 61, at 1048 (stating that "Ramzi Yousef, who masterminded the [1993] World Trade Center bombing, used encryption to store, on his laptop, detailed plans to destroy United States airliners. And many other terrorist networks, such as HAMAS, the Abu Nidal organization, and Osama bin Laden's al Qa'ida, are using encryption as well."); *see*, *e.g.*, Daniel McGrory, *Al-Qaeda Hid Coded Messages on Porn Sites*, N.Y. TIMES (London ed.), Oct. 6, 2001 (explaining that witnesses observed Mohammed Atta, alleged leader of the September 11, 2001, terrorist hijackings, downloading holiday photographs from a public library that likely concealed his directives with steganography).

68. The government defines "information warfare" as an aggressive act "taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer based networks while defending one's own information." Yonah Alexander, *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DEPAUL BUS. L.J. 59, 83 (1999) (quoting CJCSI, Number 3210.01 (Jan. 2, 1996)); *see also* WINN SCHWARTAU, INFORMATION WARFARE: CYBERTERRORISM—PROTECTING YOUR PERSONAL SECURITY IN THE ELECTRONIC AGE (2d ed. 1996) (providing definitions for "personal information warfare," "corporate information warfare," and "global information warfare").

69. *See ECPA 2000*, *supra* note 63, at 33 (statement by Donald Kerr, explaining that "several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional weapons, nations see Cyber attacks . . . as a way to hit . . . our growing dependence on information technology.").

70. *Id.* For example, Kerr notes that two Chinese military officers authored a publication on the utility of launching computer viruses to counter the force of the United States military. *Id.* Additionally, a Russian official publicly recognized the potential for destruction from information warfare and likened it to a "weapon of mass destruction." *Id.* Likewise, the FBI believes that Osama bin Laden directed his followers to launch cyber-attacks against the United States' infrastructure. *See*, *e.g.*, Dan Verton, *Report: Al Qaeda a Potential Cyberthreat*, CNN.COM, Jan. 8, 2002 (stating that "Bin Laden's foot soldiers . . . have stated that they were trained specifically to attack critical infrastructures, including electric power plants, Natural gas plants, airports, railroads, large corporations and military installations"), *at* http://www.cnn.com/2002/TECH/internet/01/08/cyberterror.report.dg/index.html; John Lasker, *Net Wars: Hackers are Using the Internet to Fight Battles at Home and Abroad*, COLUMBUS DISP., Feb. 11, 2002, at E1 (explaining that "transportation, government, water, information and energy systems all could be damaged by negative entry into the Net").

attacks.[71] While information warfare poses a serious risk to a country's electronic infrastructure, a clear means to combat it has yet to emerge.

Terrorists are not the only ones exploiting the Internet for criminal ends; pedophiles often use it to lure children into sexual relationships[72] and to distribute child pornography.[73] Several governmental task forces exist solely to curtail this type of activity.[74] Difficulties often arise, however, because a task force must decode encrypted evidence to ascertain the identity of anonymous suspects.[75]

---

71. *See generally* ALEXANDER, *supra* note 68, at 84-86 (providing an overview of cyber-attacks against our country). Alexander notes that as early as 1986, a group of West German hackers were compiling stolen passwords from military and scientific computers. *Id.* at 84. Additionally, in 1998 an Israeli hacker launched cyber-attacks against the Pentagon and nuclear research labs. *Id.* Likewise, another hacker launched an attack in 1998 against the computers in the U.S. Department of Defense. *Id.* at 85. Lastly, in 2000, a number of attacks flooded and disabled web sites such as eBay, E*Trade, CNN, and Yahoo. *Id.* Moreover, Alexander cautions that information warfare has the potential for mass destruction, citing violent acts including:

> [A]ltering formulas for medication at pharmaceutical plants, "crashing telephone" systems, misrouting passenger trains, changing pressure in gas pipelines to cause valve explosions and fires, scrambling the software used by emergency services, "turning off" power grids, and detonating simultaneously hundreds of computerized bombs around the world . . . . [T]his new medium of communication . . . forces us to think about the "unthinkable" with grave concern.

*Id.* at 88.

72. *See ECPA 2000*, *supra* note 63, at 34 (stating that "sexual predators find the Internet to be a well-suited medium to trap unwary children. Since 1995, the FBI has investigated nearly 800 cases involving adults traveling interstate to meet minors for the purpose of illegal sexual relationships"); *see also* President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet (2000) [hereinafter President's Working Group] (finding that pedophiles are online twenty-four hours a day, looking to abduct children using chat channels and message boards), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#FTC.

73. *See ECPA 2000*, *supra* note 63, at 34 (finding that "[s]ince 1995, the FBI has investigated . . . more than 1850 cases involving child pornography–almost all of these involve the exchange of child pornography over the Internet").

74. A sampling of these task forces include the Innocent Images Initiative of the FBI, the Office of Juvenile Justice and Delinquency Prevention within the DOJ, and the Customs' CyberSmuggling Center within the Customs Service. *See* President's Working Group, *supra* note 72, at Appendix C § 3. The styles within each group vary widely, ranging from the FBI proactively finding suspects that are willing to travel to meet minors, to the Customs Service operating off the tips and leads submitted through their website. *Id.* Additionally, each group boasts a varying level of success, ranging from the FBI convicting over 358 offenders since December 1999, to the Customs Service convicting 436 offenders between November 1998 and September 1999. *Id.*

75. *Id.* at Appendix C § 4 (finding that "[t]he ease with which sophisticated users can be

Thus, not only does unregulated technology allow pedophiles to mask their identity and imagery, but it may also compromise the health and safety of young children.

Finally, the use of electronic communication to facilitate securities fraud has thus far evaded federal regulation.[76] Corporate insiders regularly commit this crime by electronically communicating[77] with investors to convey both privileged[78] and fraudulent information.[79] With a growing number of investors opening online accounts,[80] the government's limited resources simply cannot uncover the majority of fraudulent activity.[81] The situation is exacerbated by the vast nature of the Internet, which provides countless convenient locations

---

anonymous on the Internet, [along with] the use of sophisticated encryption to conceal [the] evidence of unlawful conduct[,] . . . hinder[s] law enforcement agencies' ability to fight these types of crimes").

76. *Id.* at Appendix H §§ 1-5 (discussing the problems associated with regulating electronic communication utilities that facilitate the commission of securities fraud). The FBI purports that the government's inability to regulate this type of fraud "results in a loss to investors of approximately $10 billion per year (or nearly $1 million per hour)." *ECPA 2000*, *supra* note 63, at 34.

77. Fraudulent information is typically leaked over the Internet through Internet Relay Chats (IRC), message boards, and systems analogous to America Online's Instant Messenger. *Id.*

78. *See, e.g., id.* (describing how one insider electronically leaked privileged information over a two-and-a-half year period, making $500,000 for his partners, and $170,000 for himself).

79. The President's Working Group concluded that individuals using electronic communications to release fraudulent information helped promote market manipulation, offering frauds, and illegal touting. President's Working Group, *supra* note 72, at Appendix H § 1. *See also*, Katyal, *supra* note 61, at 1028-29 (describing a manipulation of the stock market when "someone holding XYZ stock will announce on message boards the likelihood of a hostile takeover . . . thousands will read the message and purchase XYZ, and the person who posted the messages will then quickly sell the stock at a high profit").

80. *See Securities Fraud on the Internet: Hearing Before the Permanent Subcomm. on Investigations of the Senate Comm. on Governmental Affairs*, 106th Cong. 2 (1999) [hereinafter *Securities Fraud*] (indicating that "nearly one-third of the [thirty million] American households now on-line use the Web for researching or investing in securities. In addition, studies report that some [three] million people now have on-line trading accounts, a number which is anticipated to reach [fourteen] million people by the year 2001.").

81. The President's Working Group found that current regulatory resources are inadequate, particularly as an increased number of investors are relying on the Internet for stock quotes and tips. President's Working Group, *supra* note 72, at Appendix H § 1. Moreover, the Securities and Exchange Commission's Enforcement Director openly admits that "[their] greatest problem will likely be one of resources, as the size of [their] staff has remained relatively constant while the Internet has grown by leaps and bounds." *See id.* at Appendix H § 4 (discussing the investigative challenges of regulating online securities fraud).

for the anonymous disclosure of fraudulent information.[82] Until the government obtains the proper resources to monitor these disclosures, online securities fraud will continue to hamper the national economy.

As cybercrime continues to become more common, an increasing number of criminals will rely on modern technology to evade detection. As evidenced by the aforementioned areas of crime, the FBI's resources are simply inadequate to eliminate, or arguably curtail, the continual growth of cybercrime.

### *B. A Call to Arms: The Implementation of Carnivore*

In 1999, the FBI recognized its limited resources and developed Carnivore to regulate and monitor online criminal activity.[83] Although initially implemented in secrecy,[84] a newspaper revealed Carnivore to the public by detailing the plight of an ISP that refused to comply with the FBI's request to install the system.[85] Despite an initial wave of criticism, the FBI justified Carnivore's monitoring system under the authority of the ECPA.[86]

The FBI contends that Carnivore complies with the ECPA by operating on a case-by-case basis to collect information through either a pen register or a wiretap and, thus, can comport with a judicial order for either standard.[87] In particular, the FBI maintains

---

82. *See generally Securities Fraud*, *supra* note 80, at 274-81 (explaining the utility of disclosing fraudulent information in various areas of cyberspace, including bulletin boards, chat rooms, "spam" emails, and "spoofing" websites).

83. *See ECPA 2000*, *supra* note 63, at 32-41 (explaining the FBI's justification for implementing Carnivore). Kerr states that "the ability of the law enforcement community to effectively investigate and prevent these serious crimes is, in part, dependent upon our ability to lawfully and effectively intercept and acquire vital evidence of these crimes." *Id.* at 41.

84. *See Id.* at 34 (stating that the FBI used Carnivore approximately twenty-five times during its period of secrecy);

85. *See* King & Bridis, *supra* note 1.

86. *See ECPA 2000*, *supra* note 63.

87. *See Fourth Amendment Issues*, *supra* note 3, at 11-14 (prepared statement of Donald Kerr explaining Carnivore's function). Kerr contends that:

> [Carnivore] works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc. . . . It does NOT search through the contents of every message and collect those that contain

that Carnivore confines its search by "sniffing" any e-mail that passes through the ISP, filtering the data, and searching for whatever information it is programmed to find.[88] Thereafter, Carnivore records the pertinent data and processes an event file to demonstrate its compliance with the court order.[89] Thus, according to the FBI, Carnivore performs a confined search tailored to its judicial order and is therefore in compliance with the Fourth Amendment.

By contrast, both the Electronic Privacy Information Center (EPIC)[90] and the American Civil Liberties Union (ACLU)[91] contend that the FBI collects more data than it reports and, thus, have filed for the release of Carnivore's source code under the Freedom of Information Act (FOIA).[92] The House Judiciary Committee responded by conducting a lengthy hearing to examine Carnivore's constitutionality.[93] Although the hearing produced nothing conclusive, it did prompt the Department of Justice (DOJ) to contract with the Illinois Institute of Technology Research Institute[94] (IITRI)

---

> certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order . . . .

*Id.* at 13.

88. *Id.*

89. *See ECPA 2000*, *supra* note 63, at 37-38 (prepared statement of Donald Kerr, explaining the various phases of a Carnivore search). In general, each search filters through the data, pinpoints the relevant information, records it for storage, and appends an event file. *Id.* at 37-38. The event file serves as the FBI's evidence that the search was conducted in compliance with the judge's order. *Id.* at 38. Specifically, the file indicates whether the search functioned under pen register or wiretap mode and states the specific data that the enforcement agency programmed it to searched for. *Id.*

90. *See* Electronic Privacy Information Center's Carnivore FOIA Litigation, *at* http://www.epic.org/privacy/carnivore (last modified May 28, 2002).

91. *See* Press Release, American Civil Liberties Union, ACLU Urges Congress to Put a Leash on "Carnivore" and Other Government Snoopware Programs (July 12, 2000), *at* http://www.aclu.org/news/2000/ n071200b.html.

92. *See* 5 U.S.C. § 552, *as amended by* Pub. L. No. 104-231, 110 Stat. 3048 (1996) (allowing citizens to access information, unless protected, that is contained in federal agency records).

93. *See Fourth Amendment Issues*, *supra* note 3, at 1 (stating that the hearing will be geared towards Carnivove, which raises "the question as to whether or not existing statutes protecting citizens 'from unreasonable searches and seizures' under the fourth amendment appropriately balance the concerns of law enforcement and privacy").

94. The IITRI was founded in 1936 and is "a contract organization of more than 1,500 scientists, engineers, and technical personnel focused on solving critical technology problems that often involve the use of sensitive, highly classified, or proprietary information." IITRI, Company Profile, *at* http://www.iitri.org/company_info/company_info.cfm (last modified Aug.

to examine whether Carnivore operates as intended.[95] Prior to the formal release of the IITRI's report, the FBI attempted to allay public concern by complying with the FOIA and issuing several documents to the EPIC on the technical aspects of Carnivore.

In December 2000, the IITRI released its report, which found that Carnivore was operating as claimed and was capable of adhering to a court order's specific limitations.[96] However, the study received a barrage of criticism premised on perceived governmental bias.[97] Critics also pointed out that the study implicitly contradicted several of the FBI's prior assertions regarding Carnivore[98] and failed to offer an opinion as to whether the program's operation was legally, rather

---

25, 2002).

95. *See* Press Release, U.S. Dep't of Justice, *Justice Department Selects Team to Review Carnivore System* (Sept. 26, 2000) (explaining that IITRI team members are proficient in the technical and legal aspects of Carnivore and will assess whether the "system's design, function and method of use" are as reported), *available at* http://www.usdoj.gov/opa/pr/2000/September/565jmd.htm.

96. *See* IITRI, Independent Technical Review of the Carnivore System, 65 (Sept. 20, 2000) [hereinafter IITRI] (concluding that Carnivore's source code indicates that the system cannot collect data without the knowledge of the agent using it), *available at* http://www.usdoj.gov/jmd/pss/iitritechnicalproposal.pdf. Specifically, the IITRI report responded to four questions posed by the DOJ. First, when Carnivore is used correctly, it has no hidden capabilities to collect additional information without any agent's knowledge. *Id.* at 4-7. Second, Carnivore introduces neither a security nor operational risk to the ISP that it is installed on. *Id.* at 4-8. Third, Carnivore poses some risk of unauthorized acquisition of data by FBI personnel, but little additional risk to an acquisition by outsiders. *Id.* Finally, Carnivore "does not provide protections, especially audit functions, commensurate with the level of the risks." *Id.* at 4-9.

97. *See*, *e.g.*, Press Release, American Civil Liberties Union, ACLU Says Government Stacked Deck in Selection of Team to Review "Carnivore" Cyber-tapping System (Oct. 4, 2000) (stressing that IITRI had a governmental bias, as it "include[d] a large number of White House insiders, including a former Clinton information policy advisor, and a former Justice Department official . . . . Other team members have backgrounds in the National Security Agency, the Department of Defense, and the Department of the Treasury."), *available at* http://www.aclu.org/news/2000/n100400.html.

98. *See generally* Press Release, American Civil Liberties Union, ACLU, EPIC Say Further Study of Carnivore Review Proves "Beast Must Be Tamed" (Dec. 1, 2000), *available at* http://www.aclu.org/news/2000/n120100.html. Both the ACLU and EPIC assessed the IITRI's review, finding several inconsistencies between the IITRI's findings and recommendations. First, the ACLU notes that test nine is indicative of Carnivore's ability to collect more information than it is programmed to find. *Id.* Second, the ACLU objects to Carnivore's conspicuous absence of an auditing function, contrary to the FBI's claim that one exists. *Id.* Likewise, the EPIC points to the study's contention that when the program is improperly configured it is capable of performing a "broad sweep" of information into its records. *Id.* Further, the EPIC contends that the review suggests a heightened potential for governmental abuse because the program lacks any means of accountability. *Id.*

than technically, sound.[99]

In August 2001, a number of reports surfaced of the FBI's plans to expand Carnivore's capabilities to enable the monitoring of messages sent through wireless systems.[100] In support of the expansion, the FBI pointed to the wireless industry's failure to meet CALEA's deadline[101] for developing its own means of monitoring wireless communications.[102] The September 11, 2001, terrorist attacks further strengthened the FBI's stance, as the orchestrators may have used wireless messaging while planning the attacks.[103]

Although civil liberties organizations acknowledge the importance of wireless regulation,[104] they maintain that Carnivore's expansion will diminish personal liberties without a visible increase in national security.[105] There also exists the possibility that the expansion will provide malicious hackers with added opportunities to access the information that Carnivore collects.[106] Such concerns over

---

99. *See* IITRI, *supra* note 96, at xiv (stating that the review "specifically excluded questions of constitutionality").

100. *See*, *e.g.*, Robert O'Harrow Jr., *FBI's 'Carnivore' Might Target Wireless Text*, WASH. POST, Aug. 24, 2001, at E1 (discussing the possibility of Carnivore's expansion to wireless technology); Luening & Charny, *supra* note 5 (explaining how Carnivore could become the de facto means of monitoring wireless communications).

101. *See supra* note 50 and accompanying text.

102. *See*, *e.g.*, Caron Carlson, *Wiretap Provisions On Verge Of Change*, WIRELESS WEEK, Sept. 24, 2001, at 1 (stating that the wireless industry is not close to meeting the FCC's deadline); Heather Forsgren Weaver, *Anti-Terrorism Legislation Hits Civil Liberties Wall*, RCR WIRELESS NEWS, Oct. 1, 2001, at 3 (stating that the wireless industry could not comply with CALEA due to "the tricky issue of allowing wiretaps on packet-mode data").

103. *See*, *e.g.*, Romero, *supra* note 6 (explaining that because "terrorists may have used wireless technology to coordinate the attacks, [it] has breathed new life into efforts to monitor even the most arcane and complex features of wireless networks"); Purcell, *supra* note 10 (stating that "[i]n the two weeks since attacks on the World Trade Center and Pentagon, wireless carriers have seen a significant upsurge in requests for cell phone records and wiretaps").

104. Civil liberty groups are willing to concede their stance against heightened regulation, but want proof that for a decrease in personal rights there will be a "commensurate improval" in public security. *See* Carlson & Callaghan, *supra* note 7.

105. *See id.* (explaining that civil liberty groups are concerned that "when individual rights are curtailed for the sake of public security at a time of heightened threat, those freedoms are lost forever").

106. *See*, *e.g.*, Luening & Charny, *supra* note 5 (stating that "it doesn't take a rocket scientist to intercept [wireless] transmissions"); Michelle Delio, *Wireless Networks in Big Trouble*, WIRED NEWS, Aug. 20 2001, *at* http://www.wired.com/news/wireless/0,1382, 46187,00.html. Delio describes a program called AirSnort, which allows hackers to intercept

Carnivore's traditional function to monitor e-mail, and its potential expansion to wireless technology, bring forth the question of whether the program is in violation of the Fourth Amendment.

## III. ANALYSIS

### *A. Was the FBI's Use of Carnivore, Prior to its Expansion, a Legal Exertion of its Governmental Authority?*

Although Justice Brandeis's concerns may once have appeared far fetched, the rapid development of technology has turned his cryptic prophecy into a modern reality.[107] Under Brandeis's dissent in *Olmstead*,[108] and the subsequent standard in *Katz*,[109] evidence collected by Carnivore is arguably entitled to Fourth Amendment protection. At a glance, such evidence appears to fall well within the Fourth Amendment boundaries of *Katz* because the data is intangible and would, thus, receive the same protection as other tangible evidence.[110] Furthermore, as stated in *Katz*, the Fourth Amendment applies to people and not places, and, thus, its protections are not limited to the government's physical intrusion into a suspect's home.[111]

The FBI sidesteps this apparent protection, however, by likening Carnivore to a pen register.[112] Under *Smith*, a pen register is not entitled to Fourth Amendment protection because a person has no reasonable expectation of privacy for the phone number of an

---

wireless signals. *Id.* Recognizing that AirSnort might breach the security of a wireless network's database, Delio states:

> Wireless networks are a little less secure . . . with the public release of . . . a tool that can surreptitiously grab and analyze data moving across just about every major wireless network. When enough information has been captured, AirSnort can then piece together the system's master password. In other words, hackers and/or eavesdroppers using AirSnort can just grab what they want from a company's database wirelessly, out of thin air.

*Id.*

107. *See supra* notes 18–21 and accompanying text.
108. *Id.*
109. *See supra* notes 22-26 and accompanying text.
110. *See supra* note 25 and accompanying text.
111. *Id.*
112. *See supra* notes 42-44 and accompanying text.

outgoing call.[113] Congress echoed the Court's view by promulgating the ECPA, which makes it much easier for law enforcement agencies to implement pen registers than wiretaps.[114] Information gathered by pen registers accordingly receives little or no constitutional protection.

Although characterizing Carnivore as a pen register enables the FBI to circumvent Fourth Amendment protections,[115] it begs the question of whether Carnivore technically operates as a pen register. As discussed in *Smith*,[116] a pen register simply collects a listing of phone numbers dialed by the suspect.[117] In contrast to a true pen register, Carnivore collects a wide range of information, including the e-mail addresses of both the sender and recipient.[118] Even this limited information would exceed the *Smith* test, as Internet users are far less likely to expect an outsider to freely access their e-mail as compared to their phone records. Specifically, whereas nearly all ISP's guarantee security for their users,[119] the same cannot be said for telephone numbers. A person dialing a phone number is readily aware that any phone number can be instantly identified either by caller identification or the phone company.[120] Accordingly, this lack of personal privacy prevents Carnivore from sidestepping Fourth Amendment protections by complying with the flexible guidelines applicable to pen registers.

If Carnivore does not operate as a pen register, it is seemingly most analogous to a wiretap. Similar to a wiretap's ability to collect all information passing through a phone line, Carnivore can be

---

113. *See supra* notes 38–39 and accompanying text. In hindsight, it appears suspect that the Court would freely dispense of all Fourth Amendment protection for evidence collected by pen registers, particularly after the significant progress made in *Katz*. *See supra* note 25 and accompanying text.

114. *See supra* notes 40-44 and accompanying text.

115. *See supra* text accompanying notes 112-13.

116. *See supra* notes 35–39 and accompanying text.

117. *See supra* note 36 and accompanying text.

118. *See* IITRI, *supra* note 96, at C-1.

119. For example, America Online's corporate policy states that "[it does] not use or disclose information about [a user's] individual visits to AOL.COM or information that [the user] may [provide], such as [their] name, address, *email address* or telephone number." *See* America Online, America Online Privacy Policy, *at* http://www.corp.aol.com/privacy_policy.html (last visited Aug. 25, 2002) (emphasis added).

120. *See supra* note 39 and accompanying text.

programmed to collect all information passing through an ISP.[121] Although the FBI concedes that Carnivore has the potential to operate as either a pen register or wiretap, even in "pen register" mode the program mimics the function of a wiretap by sifting through and collecting massive amounts of data.[122] Further, whereas wiretaps are constantly monitored and may be shut off upon encountering intimate information, Carnivore cannot; instead, the program continuously collects and records its evidence.

In sum, Carnivore exceeds the limited collection that exemplifies a pen register, instead mimicking the broad search capabilities of a wiretap. As such, any evidence collected by Carnivore must receive Fourth Amendment protection.

### *B. Will Carnivore's Expansion Violate the Federal Wiretap Provisions?*

Since the enactment of CALEA, the FBI has continuously pressed the wireless industry to develop a means by which it can freely monitor wireless messages.[123] Despite the industry's continual requests for extensions, the FBI's most recent ultimatum echoes as loudly as ever.[124] With the enactment of the Patriot Act and the subsequent increase in Carnivore's capabilities,[125] it appears imminent that one of two situations will arise—either the wireless industry will develop the necessary technology or the FBI will formally implement Carnivore's capability to intercept wireless messaging. Considering that it will take the wireless industry two years to develop its own technology and will cost the industry over one billion dollars,[126] an expanded version of Carnivore is seemingly

---

121. *See supra* note 87 and accompanying text.

122. *Id.* Specifically, while operating under pen register mode, Carnivore can at a minimum collect the e-mail addresses of both the sender and recipient. If the EPIC's claims are accurate, however, then Carnivore might in fact be collecting the entirety of the e-mail's text. Regardless, under either approach the sender's personal information is improperly breached, as he would have a reasonable expectation of privacy over the contents of his e-mail and, thus, must receive Fourth Amendment protection.

123. *See supra* note 50 and accompanying text.

124. *See id.*

125. *See supra* notes 53-58 and accompanying text.

126. *See*, *e.g.*, Jess Bravin & Dennis K. Berman, *FBI Pressures Telecom Firms on Wiretaps*, WALL ST. J., Nov. 21, 2001, at A3 (describing the futility of the wireless industry's

the only viable option.

Regardless of the fact that Carnivore's wireless capabilities are reportedly developed and ready for implementation, the expanded capabilities must still survive scrutiny in the courts. Prior to the passage of the Patriot Act, the implementation of this technology would have been particularly difficult, as electronic surveillance had to satisfy the ECPA's requirement that collection occur over a phone line.[127] In contrast Carnivore's initial use of a phone line to connect to the Internet, the monitoring of wireless technology departs from a circuit-switched network, instead operating under a packet-switched mode[128] that is specifically designed for continuous connection to a digital medium.[129] The continuous connection of wireless networks differs greatly from a telephone line and would therefore fall short of the ECPA's protection.

Complications with wireless technology seemingly dissipate, however, with the enactment of the Patriot Act, as it explicitly allows the government to monitor information over a phone line and through any other "facility."[130] Moreover, the DOJ clarifies the definition of "facility," specifically naming a cellular phone as a possible example.[131] The DOJ's inclusion of cellular technology not only implicitly authorizes Carnivore to monitor wireless messaging but also proceeds in the face of known security risks that allow hackers to intercept a wireless network's signals and database.[132]

Congress's reasoning is best justified, however, in light of the Patriot Act's preservation of *Katz's* hierarchy for wiretaps and pen registers.[133] Specifically, the Act permits any enforcement agency to obtain a pen register without appearing before a judge. The authorities need only make a showing of tenuous need.[134] Although

---

compliance with the FBI's demands, particularly as the FBI already has the tool it needs—i.e., Carnivore—to regulate wireless messaging).

127. *See supra* note 55 and accompanying text.
128. *See supra* note 51 and accompanying text.
129. *See id.*
130. *See supra* note 55 and accompanying text.
131. *Id.*
132. *See supra* note 106 and accompanying text.
133. *See supra* notes 22-44 and accompanying text.
134. *See supra* note 57 and accompanying text.

Congress passed the Act in response to a national crisis,[135] virtually no requirements remain intact to regulate against the potential for governmental abuse. Evidently, though, Congress will continue in its precedent to differentiate between a pen register and wiretap.

Whereas it might once have seemed improbable for Carnivore to regulate wireless technology, the Patriot Act all but implemented the necessary changes for an expeditious transition. Although questions remain as to whether wireless regulation is a sensible solution, Congress's enactment of the Patriot Act clearly demonstrates its view that the security of the United States must come before the security of personal information.

## IV. PROPOSAL

The Patriot Act severely limited any progress made for electronic civil liberties and cemented in place a proactive means for governmental surveillance.[136] While the Patriot Act made specific changes to modern surveillance laws, it sharply foreclosed any alternative that would limit governmental surveillance. The Patriot Act consequently leaves Carnivore as the only viable means to fight cybercrime.

Considering Congress's preservation of the *Katz* hierarchy, it would be best, when dealing with cyberspace, to eliminate the distinction between pen registers and wiretaps. Judging by the problems in characterizing Carnivore as a pen register,[137] a single standard for the government to abide by would be far simpler. Although this change may appear radical, in reality it is not, as Carnivore never truly functioned as a pen register.[138] Treating all electronic surveillance as a wiretap, thus allowing the government to collect information while abiding by strict procedural guidelines, is the most appropriate approach when dealing with cyberspace.

In essence, this change would merely reflect the fact that the FBI operates a powerful tool that is closely analogous to a wiretap—a tool

135. *See supra* note 52-53.
136. *See supra* Part III.B.
137. *See supra* text accompanying notes 117-18.
138. *Id.*

that should realistically be accorded with similar precautions.[139] Unfortunately, Congress's long history of distinguishing pen registers from wiretaps[140] suggests that the transition to a single standard is unlikely to occur. This is unfortunate because a single standard would preserve a regulatory role and protect against governmental abuse.

Considering that the Patriot Act overwhelmingly passed in both the House and Senate in spite of Congress's history of opposing Carnivore,[141] one wonders if legislators were fully aware of the Act's far reaching effects and thoughtfully considered other alternatives. Some speculate that certain legislators used the terrorist attacks to push through previously impassable legislation, arguing that the controversial provisions would help deter cybercrime.[142] The Act's inclusion of innocuous words such as "facility"[143] leads one to wonder whether its overwhelming passage arose out of patriotism or confusion.

Although the Patriot Act is not limited to electronic surveillance,[144] its subtle changes facilitate the future monitoring of cybercrime and realistically eclipse any other means of regulation. In particular, the Patriot Act's departure from phone lines places no limitation on a potential source for collecting evidence, making Carnivore an operational means for the government to proactively attack cybercrime. The Patriot Act not only empowers the government to combat cybercrime, but it also broadly accommodates the expansion of modern technology. As a result, future change is severely limited and would likely require drastic amendments to the Act's current version.

Lastly, public policy after September 11 is a rather thorny issue and will at least temporarily increase the authority of law enforcement. The severity of online crime unquestionably deserves

---

139. *See supra* note 42 and accompanying text.

140. *Id.*

141. *See supra* notes 93-94 and accompanying text.

142. *See generally* Editorial, *The Home Front: Security and Liberty*, N.Y. TIMES, Sept. 23, 2001, § 4, at 16 (explaining that "some [changes] amount to a wish list of things that the Justice Department and the Federal Bureau of Investigation have unsuccessfully lobbied for in the past and that do not make sense now").

143. *See supra* text accompanying notes 130-31.

144. *See supra* note 54 and accompanying text.

legislative attention,[145] but one must wonder whether this particular national security concern should trump the Fourth Amendment. Carnivore's characterization as a pen register, despite blatant differences in its operation,[146] exemplifies a means by which law enforcement agencies freely dispose of constitutional liberties. As a result, Congress's failure to address Carnivore's categorization implicitly suggests that national security takes priority over personal privacy in the area of electronic communication.

Even though Carnivore may infringe on the Fourth Amendment, there is simply no other viable means to combat cybercrime.[147] Given the devastation of September 11, along with sophisticated tactics such as steganography,[148] it is in Congress's best interest to disregard Carnivore's constitutional issues.[149] The only alternatives are to either abandon electronic surveillance or develop a new form of technology that passes constitutional muster. At this point in time, with hostilities on the horizon, both options are seemingly impractical. Likewise, one would expect that any new means of surveillance would be even more radical than Carnivore and would inevitably result in many of the same privacy concerns.[150]

## V. CONCLUSION

Carnivore's legality was tenuous before its potential expansion, and even considering the Patriot Act's changes, it still exceeds the limited collection that typifies a pen register. With the growth of cybercrime and the advent of sophisticated techniques to avoid detection, however, the only viable alternative is to turn a blind eye

145. *See supra* Part II.B.

146. *See supra* text accompanying notes 118-21.

147. *See supra* Part III.B.

148. *See supra* notes 66-67 and accompanying text.

149. *See supra* Part III.B.

150. *See, e.g., What's Next? The Issues and Ideas That Will Change and Challenge Us As We Go Forward*, NEWSWEEK INT'L, Jan. 7, 2002 (discussing Magic Lantern, "a rogue program [in development] that penetrates computers to steal the password keystrokes that can defeat encryption"); David Canton, *Virus Raises Questions*, LONDON FREE PRESS, Jan. 25, 2002, at C3 (explaining that Magic Lantern sends a virus to a suspect's e-mail that automatically grants "the FBI [with] access to the key or password to the encryption software, therefore enabling agents to read data that has been scrambled. It allows actual keystrokes to be monitored, rather than the encrypted messages that follow.").

toward the program's deficiencies. Perhaps the perfect form of regulation is ahead of us, but to get there, technology simply needs more time to develop. Until then, Carnivore remains the only effective way to combat cybercrime and should properly continue in its regulation of both electronic and wireless technology.