NEW YORK LAW SCHOOL

NYLS Journal of Human Rights

Volume 18 | Issue 2 Article 7

Spring 2002

Will Carnivore Devour the Fourth? An Exploration of the Constitutionality of the FBI Created Software

Gina Tufaro

Will Carnivore Devour the Fourth? An Exploration of the Constitutionality of the FBI Created Software

I have chosen the velociraptor as the symbol of the FBI's program Carnivore because Carnivore like the velociraptor is small, merciless, ruthless and with virtual razor claws, slices through our right to privacy, devouring the meat of our email messages.

—Dr. John Baker[1]

Imagine sitting at your desk at 12:30 a.m. It has been a long day and you cannot wait to tell your friend who lives in Arizona about the latest work place gossip. You compose the salacious e-mail, thinking it impossible for anyone but you and your friend to see it. Would you include the same juicy details if someone, other than the intended recipient, might be able read the message? Would you even e-mail the letter in the first place? What if such surveillance was not limited to e-mail but that invisible eyes might monitor every move you make on the web? The Federal Bureau of Investigation (FBI) has made such surveillance possible with its creation of Carnivore, an e-mail and Internet activity monitoring program.[2] This program has received much criticism as an unjustified intrusion into protected areas of privacy.[3]

Carnivore essentially allows the FBI to read one's personal e-mail. A law enforcement agent can sit on an internet service provider (ISP) and intercept e-mail sent to and from a criminal suspect without notice. This search is passive and either the internet user, the receiver or the sender of the email, never suspects that his e-mail has been intercepted.[4]

---

[1] *See* Dr. John Baker, *The FBI Becomes You Big Brother,* http://www.stop carnivore.org/news.htm (last visited October 6, 2000) (arguing the unconstitutionality of Carnivore and how such FBI devices are creating an Orwellian world).

[2] *See* John Schwartz, *FBI Makes Case For Net Wiretaps; Carnivore System Faces Fire On the Hill*, WASH. POST, July 25, 2000 at E01.

[3] *See id.*

[4] *See* Margaret Johnston, *FBI Demos, Defends Carnivore Surveillance System,* COMPUTERWORLD MAG., July 24, 2000, at 10 (describing the Carnivore installation process. "Carnivore doesn't adversely affect the flow of traffic on the

While the existence of Carnivore has been a proverbial thorn in the side of civil libertarians, the passage of the USA Patriot Act, which provides for an easier implementation of the program, has exacerbated the privacy intrusions.[5] The Act, signed into law on October 26, in the wake of terrorists attacks, has met much opposition.[6]

This note focuses on the *unconstitutionality* of Carnivore as a passive search in the context of the Fourth Amendment and under federal wiretapping laws, both before and after the passage of the Patriot Act. Even in its least intrusive form, Carnivore intrudes upon one's reasonable expectation of privacy. Part I explores the fundamentals of Carnivore as a crime-fighting tool. Although the FBI advocates implementation of the software, groups such as the American Civil Liberties Union (ACLU) and Electronic Information Privacy Center (EPIC) seriously question Carnivore's constitutionality.[7] Part II explores the evolution of current wiretapping laws. The Supreme Court originally focused on whether or not wiretaps seized any tangible evidence. Seeing that they did not, the Court held that the Fourth Amendment was not implicated.[8] However, with the introduction of the notion that the Fourth Amendment protects "people, not places," both the courts, as well as the legislature, have held "content" wiretaps to stricter standard.[9] The culmination of these principles can be found in the Electronic Communications Privacy Act, (ECPA), amended as recently as October 26, 2001.

Part III argues that, prior to the terrorist attacks of September 11, federal wiretapping laws, namely ECPA, did not cover uses of

---

network, and it can be installed for only as long as the court order allows."). *See also* Carnivore FAQ, http://www.robertgraham.com/pubs/carnivore-faq.html (last visited October 6) (dispelling rumors about Carnivore's presence on the internet. "It is important to note that Carnivore is a passive wiretap. It does not interfere with communication. Some news reports falsely claim that Carnivore interposes itself into the stream, first grabbing data, then passing it along.").

5 ACLU PRESS RELEASE, USA PATRIOT ACT BOOSTS GOVERNMENT POWERS WHILE CUTTING BACK ON TRADITIONAL CHECKS AND BALANCES, *available at* http://www.aclu.org/congress/1110101a.html (last visited January 8, 2001) (enumerating the problems with the Act, including the extension of Internet surveillance programs under federal wiretapping laws).

6 *Id.*

7 *See* Ann Harrison, *Critic Bash U.S. Plan for Surveillance Standards*, COMPUTERWORLD MAG., July 19, 2000, at 6.

8 *See* Olmstead v. United States, 277 U.S. 438 (1928).

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

Carnivore. Because of Carnivore's unique nature, the statute, which only provided for the use of telephone taps, was not applicable to this software situation. Congress tried to rectify this inapplicability through the passage of the USA Patriot Act. These amendments proved to only be partially effectual, as they did not address the distinction between "content" and "non-content" information.

Part IV suggests that whether analysis be under the pre-Patriot Act wiretapping laws or post, the use of Carnivore, even in its least intrusive form violates Fourth Amendment principles. The Fourth Amendment is the guardian against unreasonable searches and is implicated whenever one's privacy has been unconstitutionally invaded.[10] As a consequence of this violation, the use of Carnivore, under existing law, constitutes an unreasonable search.

Finally, Part V concludes that since Internet users have a reasonable expectation of privacy and because Carnivore, regardless of the legitimization via the Patriot Act, invades this reasonable expectation, Carnivore is unconstitutional. In finding Carnivore unconstitutional, Part V suggests some legal remedies.

I. (A) THE FUNDAMENTALS OF CARNIVORE AND THE DEBATE OVER ITS CONSTITUTIONALITY

While the concept of "sniffing" is not a novel one, the FBI has managed to join the technology superhighway with its development of Carnivore, the e-mail surveillance system.[11] True to its codename, the FBI admittedly explained that the appellation is derived from the systems actions - "Carnivore *chews* all the data on the network."[12] The Carnivore system consists of an ordinary personal computer running Microsoft Windows 2000 and some propri-

---

[10] *See* ROBERT M. BLOOM AND MARK BRODIN, CRIMINAL PROCEDURE: EXAMPLES AND EXPLANATIONS 14 (1996) (explaining "in addition to the provision concerning warrants, the Fourth Amendment (in its first clause) prohibits 'unreasonable searches and seizures.'").

[11] *See* http://www.techweb.com/encyclopedia (last visited October 6, 2000) (defining a "sniffer" as a piece of hardware or software that analyzes date on a network).

[12] *See* Carnivore FAQ, http://www.robertgraham.com/pubs/carnivore-faq.html (last visited October 6, 2000) (answering frequently asked questions about Carnivore).

etary (closed-source) software.[13] The computer, encased in a "black box," is then installed, with the cooperation of the ISP, on the ISP, itself.[14] Carnivore is commonly referred to as a "packet sniffer," meaning that it takes in packets of data, or traffic on the Internet.[15] Carnivore then copies and records the data within the box.[16]

More specifically, however, Carnivore functions in two ways. First, it acts as a "content wiretap" and second as a "trap and trace/ pen register."[17] As a "content wiretap," Carnivore copies all of the e-mail to and from a specific users account.[18] This function is self-explanatory. "X's" messages to "Y" may be retrieved as well as "Y's" messages to "X." In addition, Carnivore is capable of collecting all of the traffic of user, "X", while he is on an ISP.[19] In other words, if X decides to go to www.abc.com and enter in certain data, the FBI may have access to this data.

As a "trap and trace/ pen register," Carnivore functions at a slightly less invasive level. Instead of copying the entire content of any given e-mail, it will copy only the header (the "To," "From" and "Re:" lines) of e-mail going to and from a specific account.[20] In this capacity, Carnivore can also "list all the servers (web servers, FTP servers) that the suspect accesses, but (cannot) copy the content of this communication."[21] In copying all of this information,

---

13 *See* About.com, http://www.about.com/computer/technology (last visited October 6, 2000) (describing the fundamentals of Carnivore).

14 *See* Harrison, *infra* note 25 ("At present, Carnivore is installed by the FBI as a 'black box' system that's attached to the networks of ISPs, which can't examine or access the system.").

15 *See* Carnivore FAQ, *supra* note 12 (explaining how "Carnivore acts like a 'packet sniffer.' All Internet traffic is broken down into bundles called 'packets.' Carnivore eavesdrops on these packets, watching them go by, then saves a copy of the packet it is interested in.").

16 *See id.*

17 *See id.* (A pen register is a device, normally attached to a telephone line which collects numbers dialed to and from a specific location.).

18 *See id.*

19 *See id.*

20 *See* About.com, *supra* note 13 (describing the way Carnivore functions as a trap and trace/ pen register. "By scanning the subject lines and headers of incoming or outgoing messages, the system identifies relevant communications among selected individuals as part of a criminal investigation. Data deemed useful can be off-loaded onto removable drives and retrieved through secure dial-up sessions.").

21 *See* Carnivore FAQ, *supra* note 12.

Carnivore plays the role of a passive sniffer, collecting data virtually undetected.[22]

The most controversial aspect of Carnivore, however, is its resemblance to a "'trunk side" wiretap—"that is, a monitoring system that takes in all communications running through a telephone office to find the calls related to a suspect."[23] In its most "ferocious" capacity, Carnivore enables an FBI agent to access every e-mail, including its contents and header information, sent and received by every single customer of a given ISP.[24]

While an FBI agent may be able to retrieve all of this information in the privacy of his own cubicle, participation of a third party is required. Without cooperation from an ISP, agents cannot install Carnivore's hardware, also known as a "black box."[25] Over 25 cases have been reported in which different ISP's have allowed the implementation of Carnivore.[26] The details of these investigations have not been released publicly.[27] Although the FBI has received the assistance of these ISP's, some, including EarthLink, are staunch opponents of its incorporation because of possible uniden-

---

22 *See* Carnivore FAQ, *supra* note 12.

23 *See* John Swartz, *Republicans Oppose FBI Scrutiny of E-mail*, WASH. POST, July 21, 2000, at A1 (balancing the views of privacy advocates and those that support Carnivore. Swartz points out that while the FBI et al have defended Carnivore, Clinton's overall plans for "policing the internet are running into sharp opposition from Republican leaders.").

24 *See id.* (describing the ongoing controversy over Carnivore. "Critics object to the fact that the system sorts through the communications of innocent people in order to monitor suspects." The majority House Leader, Richard Armey complained, 'Nobody can dispute the fact that this is not legal . . . within the context of any current wiretap law.').

25 *See* Ann Harrison, *DOJ Signs Up Team to Review Carnivore,* COMPUTERWORLD MAG., October 2, 2000, at 20 (describing the way in which FBI agents install Carnivore. "Currently, Carnivore is installed by the FBI as a "black box" system that's attached to the networks of Internet service providers, which can't examine or access the system." This installation process has raised much concern because while the cooperation of the ISP is necessary, no one but the ISP may monitor Carnivore's use. When a law enforcement agent installs a traditional wiretap, however, the telephone company may monitor the use. Privacy groups feel that this distinction, amongst others, make current wiretapping laws inapplicable to Carnivore.).

26 *See* Margaret Johnston, *FBI Demos, Defends Carnivore Surveillance System,* COMPUTERWORLD MAG., July 24, 2000, at 10 (explaining that while the FBI has demonstrated the system, its refusal to release the source code has caused much criticism especially by the ACLU).

27 *See* About.com, *supra* note 13.

tified constitutional violations.[28] Cooperation of the ISP is mandated by law, under the Communications Assistance for Law Enforcement Act (CALEA) passed in 1994.[29]

Even after unveiling the purpose behind the system and a subsequent demonstration of its capabilities, the FBI has received much criticism of Carnivore from groups other than ISP's.[30] The ACLU and EPIC have repeatedly pointed out that "the potential for abuse is high."[31] The ACLU first learned about the existence of Carnivore in April, 2000 when attorney, Robert Corn-Revere[32] testified before the Constitutional Subcommittee.[33] In a letter dated July 11, 2000, the ACLU's Director, Laura Murphy, and its Associate Director, Barry Steinhardt, explicated the group's concern over the device.[34]

"Carnivore . . . cries out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age," wrote Murphy.[35] In voicing its concern about a need to act, the ACLU differentiated Carnivore from its constitutional predecessor, the wiretap.[36] When an officer receives a warrant for a wiretap, he has

---

28 *See* Harrison, *infra* note 45 (explicating Earthlink's opposition to Carnivore. "The company resisted the installation of the secretive system because it caused performance problems on its network. It also couldn't examine the technology to determine if its capturing of e-mail, IP addresses and other traffic violated the privacy of other customers.").

29 *See* 47 U.S.C. §§ 1001–1008 (Under § 1002(a)(3) "a telecommunications carrier shall ensure that its equipment . . . are capable of . . . delivering intercepted communications and call-identifying information to the government, pursuant to a court order"). *See also* U.S. Telecom v. FCC, 227 F. 3d 450 (D.C. Cir.2000) (detailing the purpose behind CALEA. "Congress enacted (CALEA) 'to preserve the government's ability, pursuant to a court order or other lawful authorization, to intercept communications involving advanced technologies . . . while protecting the privacy of communications without impeding the introduction of new technologies, features and services.'").

30 *See* Johnston, *supra* note 26.

31 *See* Ann Harrison, *ACLU Calls For Limits on FBI's Carnivore System,* COMPUTERWORLD MAG., July 14, 2000.

32 Corn-Revere represented EarthLink, an ISP who refused to allow FBI agents to attach the system to its network.

33 *See* Letter from Barry Steinhardt, Associate Director of the ACLU, to Charles Candy and Melvin Watt, House Representatives, (July 11, 2000) (on file with author).

34 *See id.*

35 *See id.*

36 *See id.* ("But unlike the operation of a traditional . . . wiretap on a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP 's network, not just the communications to or from a particular target.").

access to the suspects phone call conversations, and only that suspect's. The ACLU points out that Carnivore, in contrast, is capable of reading millions of messages per second, not just those involving the criminal suspect.[37] Although the FBI may hone in on a specified suspect, everyone on the ISP, theoretically, is an equal target. The only safeguard that internet users have is the "assurance that the FBI will record only conversations of the specified target."[38] Such an attitude is the main reason for procedures required under wiretapping law.[39]

In response to this super FBI tap, the ACLU calls for strict legislation that reflects the notion that ISP has the burden of protecting its customers from clear invasions of privacy.[40] In closing, the ACLU extended its desire to work with Congress on the drafting of any such legislation.[41]

The ACLU is not the only civil liberties group that is up in arms about Carnivore, EPIC has also expressed grave reservations.[42] Marc Rotenberg, head of EPIC, questioned whether or not Carnivore is a reasonable search and seizure.[43] Precipitated by such concerns and the lack of governmental response, EPIC and ACLU separately filed a request on July 12, 2000, pursuant to the Freedom of Information Act (FOIA), for the production of all documents relevant to the Carnivore system.[44] Despite this attempt, the FBI,

---

37 *See id.*

38 *See id.*

39 See Letter for Barry Steinhardt, *supra* note 33.

40 *See id.*

41 *See id.*

42 *See* Harrison, *supra* note 7 (describing EPIC's concern over Carnivore's continued use. David Sobel, EPIC's general Counsel asked, "Why wasn't some moratorium on Carnivore announced?" "How can the administration on one hand say they are trying to improve online privacy and also, at the same time, approve the use of technology that appears to be inherently invasive?" Sobel complained about the Clinton administration's supposed goal to protect online privacy and its reluctance to address Carnivore.).

43 *See* John Schwarz, *FBI's Wiretap Raises Privacy Concerns,* WASH. POST, July 12, 2000 at A1.

44 *See* Press Release, EPIC (August 2, 2000) (explaining the need for public disclosure of pertinent information, including Carnivore's source code. "The only way that the privacy questions can be resolved is for the FBI to release all relevant information, both legal and technical," said David Sobel, General Counsel for EPIC.).

was slow and inadequate in its response.[45] The first installment of information, required as per a judicially-set release schedule, withheld 200 pages of data and another 400 were "sanitized," containing nothing but page numbers.[46] The document text revealed only fundamental information such as the date of creation (February 1997) and reviews of previous test.[47]

Dissatisfied with the dearth of data and the absence of a source code (programming language in which Carnivore was written), Rottenberg announced that EPIC intended to pursue litigation until all relevant documents were disclosed.[48] Taking these concerns once again into the courtroom, EPIC demanded that something be done. Rottenberg claimed that he was amazed by the Department of Justice's inability to "recognize the high level of public concern that Carnivore has generated."[49]

With hopes of putting the civil liberty group at ease, the U.S. Justice Department appointed a team of government employees to lead an investigation into Carnivore.[50] This appointment, however, exacerbated the situation.[51] The team, from the IIT Research Institute (IITRI), a not-for-profit research and development organization associated with the Illinois Institute of Technology, was to review Carnivore and to determine whether the tool contained a sufficient amount of privacy invasive safeguards.[52] The ACLU,

---

45 *See* Ann Harrison, *Privacy Group Critical of First Release of Carnivore Data,* COMPUTERWORLD MAG., October 3, 2000, at 24 (detailing the minimal information revealed by the FBI –released Carnivore documents).

46 *See id.*

47 *See id.*

48 *See id.*

49 *See* Press Release, EPIC, *supra* note 44.

50 *See* Robert Lemos, *Carnivore Review: A 'Stacked Deck'?*, http://www.zdtv.com/news.html (last visited October 4, 2000) ("The panel of experts were appointed to review the security and reliability of Carnivore and whether the software violated search and seizure provisions of the Constitution.").

51 *See* Ann Harrison, *Government Error Exposes Carnivore Investigators; ACLU Blasts Team for Close Ties to the Administration,* COMPUTERWORLD MAG., October 5, 2000, at 20 (commenting on how the review committee is compromised by their close government connections. ACLU director said, "by selecting people with extensive government ties for what is supposed to be an independent review, the executive branch has shown once again that it cannot be trusted with carte blanche authority to conduct searches.").

52 *See* Lemos, *supra* note 50. *See also* Press Release, *IITRI Delivers Draft Report on Carnivore E-Mail Surveillance System Review,* (November 22, 2000) (explaining how the "IITRI's more than 1,500 scientists and engineers focus on solving difficult problems in a variety of technologies. The Carnivore review team

however, definitively announced its outrage.[53] A governmentally connected team, whose members included employees of the Department of Defense, did not, in the ACLU's opinion, represent an unbiased group of reviewers. Instead, the ACLU claims that the DOJ "stacked the deck."[54]

The ACLU further condemned an additional provision ordered by the DOJ which required that the Department "have the final edit on the report and that the source code not be published."[55] Other universities, who were in the running for committee selection, withdrew from the application process once this condition was made known.[56]

Aside from the ACLU and EPIC, there is a third group vocalizing objections to Carnivore, ISP's. This group, although less political than the champions of civil liberty, is just as significant, if not more so, if Carnivore is to remain a viable crime fighting weapon. Several ISP's have bashed Carnivore and the FBI for its implementation in over 25 cases.[57]

Notable criticism has come from the ISP, Earthlink Inc.[58] Although FBI agents presented Earthlink with a trap and trace order, Earthlink refused to attach the system to its network.[59] Robert Corn-Revere, Earthlink's attorney, testified before the House Judiciary Committee relaying his client's concern over the scope of Carnivore.[60] Corn-Revere noted that the system could be used to track

---

consisted of staff and senior faculty members from IIT's Chicago-Kent College of Law.").

53 *See* Harrison, *supra* note 51.

54 *See* Harrison ,*supra* note 51.

55 *See* Harrison, *supra* note 51.

56 *See* Ann Harrison, *DOJ Signs Up Team to Review Carnivore,* COMPUTERWORLD MAG., October 2, 2000, at 20.

57 *See* About.com , *supra* note 13. *See also* Steven Labaton and Matt Richtel, *Proposal Offers Surveillance Rules for Internet,* N.Y. TIMES, July 17, 2000 at A1 (discussing how a legislative proposal concerning surveillance in cyber space failed to address Carnivore. Such exclusion alarmed privacy advocates and civil liberty groups).

58 *See* Bob Barr, *Carnivore is Why New Laws are Needed for New Technologies*, Computerworld Mag., August 16, 2000 (arguing that if not for a "decision by Internet service provider EarthLink Inc. to litigate over the placement of the device on its network, which ultimately led to Carnivore's existence being publicly revealed in a congressional hearing earlier this year," the FBI would have continued to use Carnivore in secret).

59 *See* Harrison, *supra* note 45.

60 *See supra* note 32. *See also infra* note 130 (Corn-Revere noted that he would have cited the case for the committee, "but the pen register authorization

dissidents online, but more generally, involved issues of basic human rights.[61]

Other ISP's have also objected to Carnivore.[62] William Schrader, chairmen of PSINet, a major ISP, said that he would never let the government attach the little black box because of the wide access to all of his users' activities. Schrader said, "I object to American citizens and any citizen of the world always being subject to someone monitoring their e-mail . . . I believe it is unconstitutional and I'll wait for the Supreme Court to force me to do it."[63]

Certain Republicans and Democrats comprise the last group to voice a myriad of concerns over Carnivore.[64] The House Committee on the Judiciary called a hearing, at the end of July, to discuss privacy concerns over Carnivore.[65] Both parties equally expressed outrage over the invasiveness of the device.[66] For example, Spencer Bachus, (R – Ala.) sarcastically asked, "You can't go to AT&T today and say, 'We are going to analyze all of the phone calls that go through your system,' but you can do that with Carnivore?"[67] Another Republican, J.C. Watts, (R – Okla.), was so concerned over the unconstitutionality of Carnivore that he called for a moratorium on its use until further investigations.[68]

The most devastating comments came from Robert Barr (R – Ga.). Barr emphasized that the FBI contends that it has the authority to "harvest" large amounts of data and then to filter out the

---

was an ex parte order and the subsequent proceedings . . . were conducted before a Magistrate under seal.").

61 *See* Schwarz, *supra* note 43.

62 *See* Steven Labaton and Matt Richtel, *Proposal Offers Surveillance Rules for Internet,* N.Y. TIMES, July 17th 2000 at A1.

63 *See id.*

64 *See* Margaret Johnston, *House Panel Grills FBI Over Carnivore*, COMPUTERWORLD MAG., July 25, 2000, at 10 (demonstrating how democrats and republicans have joined forces in the ongoing debate over Internet privacy. During testimony before the House Committee, Republican, J.C. Watts (Okla.) and Democrat, Jerrold Nadler (NY), "launched a barrage" of questions upon the Department of Justice concerning Carnivore's high potential for abuse.).

65 Testimony before the committee took place on July, 24, 2000.

66 *See* Johnston, *supra* note 64 and accompanying text.

67 *See* Johnston, *supra* note 64 (quoting Bachus who said that the "FBI's explanation raised concerns that some people in the FBI could have free reign to check up on what their ex-spouses or political enemies were doing [on the Internet].").

68 *See* Johnston, *supra* note 64 (expressing the Republicans' "grave concern about the potential for privacy violations and skepticism that Carnivore's operations are as confined as the FBI says that they are.").

unwanted information. "Those are two very, very large steps that we are taking here . . . I don't think that this has been well thought out."[69]

Democrats, too, expressed incense. Jerrold Nadler (D – NY) emphasized that those who communicate with criminal suspect are susceptible to privacy violations. Such violations, he said, might go unnoticed.[70]

I. (B) THE FBI'S RESPONSE

The FBI has tried to respond to these growing concerns in several ways. Aside from answering a multitude of questions advanced by 25 media outlets, the FBI performed an actual demonstration of the system at its headquarters.[71] In addition to such demonstration, the FBI placed a specially designed, Carnivore devoted, website on the Internet.[72] The site is part of an ongoing effort to discuss the topic of electronic surveillance openly and to share information pertaining to Carnivore's capabilities.[73] The site features testimony

---

[69] *See* Johnston, *supra* note 64 (quoting Barr who "complained that law enforcement officials are mistreating Internet service providers" with Carnivore. On the one hand, Barr points out, the FBI is trying to break new legal ground with the application of Carnivore to new technologies. On the other hand, the FBI is trying to use authority that it does not have.).

[70] *See* Johnston, *supra* note 64 (Nadler said that those who communicate with criminal suspects would never know that their e-mail has been intercepted unless a court case comes up and such information is revealed.).

[71] *See* Letter from John Collingwood, Assistant Director of the FBI, to Brian Gallagher, USA Today Editor, (July 24, 2000) ("correcting" several assertions made in an editorial criticizing the FBI's use of Carnivore. Collingwood emphasized that "court orders authorizing the interception of criminals' e-mail come only after rigorous review and the conclusion that there is probable cause that a crime is being or has been committed." In addition, Collingwood defended the FBI by pointing to the numerous questions that the FBI has answered and its willingness to perform a demonstration of the system.). *See* Margaret Johnston, *FBI Demos, Defends Carnivore Surveillance System*, COMPUTERWORLD MAG., July 24, 2000, at 10 (explaining that the FBI, in an effort to dispel criticism, gave a demonstration of the system on July 21. During the demonstration, FBI official said that "they were confident that the system is entirely legal.").

[72] *See* http//:www.fbi.gov (last visited October 6, 2000).

[73] *See id.* (recounting Donald Kerr's, Assistant Director of FBI's Laboratory Division, testimony before the Committee on the Judiciary. Kerr discussed, amongst other Carnivore related topics, the purpose behind the system and its constitutionality.).

given by Donald Kerr, Assistant Director of the Laboratory Division of the FBI before the Committee on the Judiciary.[74]

Kerr's testimony constituted the main defense put forth by the FBI. Faced with a "barrage" of cynical questions, Kerr vehemently defended Carnivore's constitutionality.[75] Kerr began his testimony by advancing the need for a system like Carnivore.[76] Specifically, Kerr mentioned the perpetration of crimes such as terrorism, espionage, information warfare, child pornography, and "serious" fraud.[77] After explaining each of these crimes in detail, Kerr discussed why the public should "have confidence in the FBI's lawful use of Carnivore."[78] The first rationale involved the statutory protections made applicable to wire and electronic communications under the Electronic Communications Privacy Act (ECPA) of 1986.[79] Under the ECPA, all electronic surveillance requires some form of a court order.[80] In sum, the FBI must show probable cause,

---

[74] On July 24, 2000, the Committee on the Judiciary held hearings on the functionality of Carnivore. Members of the ACLU and EPIC testified, citing the privacy concerns mentioned above. Members of the FBI also testified offering step-by-step information on the installation of the device and the procedure of capturing data.

[75] *See* Johnston, *supra* note 64 (commenting that the FBI, as well as the Department of Justice, in general, "remained firm in their defense of Carnivore.").

[76] *See* Kerr's testimony (explaining that "it has become common knowledge that terrorists, spies, hackers, and dangerous criminals are increasingly using computers and computer networks, including the Internet, to carry out their heinous acts. In response to their serious threats to the Nation . . . the FBI responded by concentrating their efforts and resources, to fight the broad array of Cybercrimes.").

[77] *See id.* (listing the specific types of crimes that occur in the context of computers).

[78] *See id.*

[79] *See* 18 U.S.C. § 2510 (Electronic Communications Privacy Act) (1986) hereinafter referred to as ECPA, (amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968). According to 18 U.S.C. § 2510(12) defines "electronic communication" as "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photo-electronic, or photo-optical 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 device, (c) any communication from a tracking device, or (d) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer or funds.

[80] *See* Kerr's testimony, *supra* note 76 (explaining that a search of one's electronic communication, as defined by the ECPA, requires a showing of probable cause or "an ECPA created court order based upon relevancy for communications' addressing and transactional record information." "Transactional record informa-

and only after judicial review of the cause and authorization, may an FBI agent install Carnivore.[81]

Kerr next pointed out that while Carnivore is "configurable" to gain access to unauthorized information (information not covered by the warrant), a "filter" may be placed in the device to prohibit it from doing so.[82] A filter allows Carnivore to discriminate against certain types of information. A Carnivore "black box" with a specially designed filter will only retrieve the information requested under the warrant. Theoretically, a filter will only allow Carnivore to see suspect X's e-mail and other computer related activities while ignoring the activities of the other thousands of ISP customers.

Kerr then addressed the argument that 18 U.S.C. §§ 3123 and 2703 preclude the gathering of transactional information.[83] This concern, according to Kerr, is not supported by any caselaw and must therefore be invalid.[84] In connection with this contention, Kerr mentioned that the Supreme Court has found no Constitutional requirement of probable cause for the acquisition of a criminal suspects transactional information.[85] Since probable cause is not required and 18 U.S.C. §§ 2703(c) and 3123 do not serve as a bar, the FBI may gain access to transactional information without violating the Constitution.[86]

Kerr concluded his testimony with a discussion of "why computer network services (and the public) should not be fearful about

---

tion" includes "To" and "From" lines, routing, billing, or other information obtained or generated by the Internet service provider.").

81 *See id.* (describing the FBI's burden to obtain authorization for Carnivore).

82 *See id.* (explicating the benefit of a filter).

83 *See id.* (arguing that 18 U.S.C. § 3123 (2000) and 18 U.S.C. § 2703(2000) does not prohibit access to the transactional information. 18 U.S.C. § 3123 provides that an order for a trap and trace device must include inter alia, the suspect's name, the location of his telephone line, and his telephone number). *See also* 18 U.S.C. § 2703(c) (2000) governs governmental access to records concerning electronic communication service or remote computing service. Subsection (c) provides that an ISP may disclose "a record or any other information pertaining to a subscriber." Opponents of Carnivore, according to Kerr, argue that "transactional information" is not included in this language.). For an explanation of "transactional information" *see supra,* note 12.

84 *See id.*

85 *See supra* note 76 (citing *Smith v. Maryland,* 425 U.S. 435 (1976) holding that there was no reasonable expectation of privacy in information given by a banking customer to a third party financial institution).

86 *See supra* notes 79-85 and accompanying text.

Carnivore's use."[87] He relies heavily on the notion of trustworthiness.[88] For Kerr, the vast amount of trust placed in the FBI is the safeguard against abusive use of Carnivore. "The FBI certainly does not recruit honest and law abiding people only to employ them in corrupt and dishonest ways."[89] In other words, since the FBI are so trustworthy, customers of the ISP as well as the ISP's themselves, should not worry about any unauthorized use of the system.

II. LAWS GOVERNING CARNIVORE

As evidenced by these objections and responses to such, almost every aspect of Carnivore is contentious and hotly debated. Another such aspect is the law governing the existence of electronic surveillance. While proponents of Carnivore argue that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, controls, opponents question its applicability.[90] While Congress did

---

[87] *See* Kerr's testimony, *supra* note 76 (addressing whether the FBI would ever take full advantage of Carnivore's ability to function without a filter. Kerr focused on the caliber of FBI agents and how trustworthy they have been over the years. "To become an FBI employee requires a substantial showing of trustworthiness, lawfulness, and personal and professional integrity. The structure of the FBI would quickly collapse if the agency and all of its employees could not trust without reservation its new employees.).

[88] *See* Kerr's testimony, *supra* note 76.

[89] *See* Kerr's testimony, *supra* note 76 (contrasting the high level of trustworthiness required by the FBI with the lower level required by others who work in the telecommunications field. "Indeed, in contrast with the requirements placed upon many of the personnel employed by telecommunication and computer network service providers (who may have some role in implementing electronic surveillance orders), all FBI employees are specifically sworn to uphold the Constitution, obey the law, and to faithfully execute the laws of the land.").

[90] *See* Margaret Johnston, *FBI Demos, Defends Carnivore Surveillance Systems,* COMPUTERWORLD MAG., July 24, 2000 (explaining how the FBI believes that Carnivore operates in conformity with the Electronic Communications Privacy Act, ECPA. Johnston describes how "the FBI began developing Carnivore three years ago when law enforcement officers began seeking and obtaining court orders to intercept e-mail as part of their investigation. . .the result was (a system) designed to operate in strict conformance with federal wire tap laws and the Electronic Communications Privacy Act). *See also* Letter from Barry Steinhardt, *supra* note 33 (questioning whether applicable federal law, ECPA, even allows the FBI to serve an order on an ISP to obtain the addresses of incoming and outgoing messages. Steinhardt, writing on behalf of the ACLU, concluded that while the ECPA may cover collection of a suspect's e-mail it "is (not) clear that law enforce-

not enact these federal statutes until the latter part of the 20th century, electronic surveillance dates back to a time long before society contemplated surfing the "net."[91] This issue first came before the Supreme Court in *Olmstead v. United States* where the Court held that the interception of telephone conversations by federal law enforcement officials did not constitute a search or seizure under the Fourth Amendment.[92] The Court reasoned that because law enforcement agents did not seize anything tangible, the Fourth Amendment was not implicated.[93]

Although the Court concluded that wiretapping was not subject to the Fourth Amendment, Congress soon removed the wiretap "from the repertoire of evidence-gathering tool" by enacting the Communications Act of 1934.[94] Interception of wire or radio signals without the consent of the sender was rendered illegal by the federal statute.[95] The Communications Act, however had limits. It did not allow for the technological advancements made by the telecommunications industry, namely its inapplicability to electronic bugs.[96] *Goldman v. United States* reinforced the legality of electronic bugs.[97]

---

ment can install a *super* trap and trace device that (allows for) access to such information for all of an ISP's subscribers.").

[91] *See An Overview of Electronic Surveillance: History and Status* (visited November 2, 2000) http://www.nap.edu/readingroom.books/crisis/D.txt. (chronicling the birth of electronic surveillance beginning in 1927 with *Olmstead v. United States* which was overturned 40 years later in *Katz v. United States*); *see* Olmstead *infra* note 92 and accompanying text.

[92] *See Olmstead*, 277 U.S. 438 (construing the Fourth Amendment to cover only material things).

[93] *See id.*

[94] *See An Overview of Electronic Surveillance: History and Status supra* note 91 (explaining that while the Communications Act of 1934 did not specifically state that that evidence obtained through wiretapping was inadmissible, it did make it a crime to intercept communications without the consent of the sender).

[95] *See An Overview of Electronic Surveillance: History and Status supra* note 91.

[96] *See An Overview of Electronic Surveillance: History and Status supra* note 91 ("Electronic bugs were not restricted by the Fourth Amendment, by the same principal applied in *Olmstead*—they seized nothing tangible. Nor were they subject to the Communications Act's prohibition on divulgence of intercepted communications because they intercepted sound waves, not wire or radio signals.").

[97] *See* Goldman v. United States, 316 U.S. 129 (1929) (holding that evidence obtained through the use of a bug was admissible so long as no physical trespass took place).

The Supreme Court diametrically changed its tone in 1967 with its landmark decision in *Katz v. United States.* In *Katz*, the court explicitly overturned *Goldman* and *Olmstead* by holding that a federal agents' bugging of a regularly used telephone booth was an illegal search and seizure. The Court reasoned that the Fourth Amendment did not attach itself to specific places, but rather to people.[98] Here, the court explicated the famous notion of a "reasonable expectation of privacy."[99] Since a regular user of a particular phone had a reasonable expectation of privacy when inside, evidence obtained via an electronic bug, without a warrant, was a violation of the Fourth Amendment.[100]

With the *Katz* decision, law enforcement officials could employ neither wiretaps nor bugs, without a court order, in their quest for evidence.[101] Legislation, at that time, failed to address the regulation of court ordered surveillance.[102] In response to this legal omission, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968. Title III dealt with wiretapping and procedures to obtain a court order.[103] Title III made an exception to the Communications Act's "divulgence prohibition for law enforcement officers with a court issued warrant, thus bringing wiretapping back

---

98 *See Katz,* 389 U.S. 347, 351.

99 *See id.,* 389 U.S. 347 at 353 (holding that since the "Fourth Amendment governs not only tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law' . . . and that the Fourth Amendment protects people — and not simply 'areas' against unreasonable searches and seizures, it becomes clear that the reach of the Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

100 *See Katz,* 389 U.S. 347.

101 *See An Overview of Electronic Surveillance: History and Status supra* note 91 (explaining that the Communications Act of 1934 and *Katz* made it difficult for an officer to use electronic surveillance as a means of collecting evidence against a suspect. The absence of these tools was devastating because "they were thought to have a great potential usefulness for investigating and prosecuting conspiratorial activities such as organized crime, a high–profile and social crime in the 1960's.").

102 *See An Overview of Electronic Surveillance: History and Status supra* note 91("The judicial record made it clear that electronic surveillance without a court order was not prohibited by the Constitution, but new legislation was needed to define and regulate court ordered surveillance.").

103 *See An Overview of Electronic Surveillance: History and Status supra* note 91 (noting how the Omnibus Crime Control and Safe Streets Act "was the first legal framework for electronic surveillance of oral and wire (telephone) communications.").

into legal use.[104] Congress amended Title III in 1986 with the enactment of the Electronic Communications Privacy Act (ECPA).[105] Congress wanted to keep on par with the many technological advancements developed after 1986, particularly e-mail.[106]

One feature of the 1986 ECPA was the addition of "electronic communications" to Title III's protection of oral and wire communications.[107] Since e-mail is a form of "electronic communication" and the ECPA covers interception of "electronic communication," the FBI is allowed to intercept e-mail pursuant to the ECPA.[108]

While the ECPA provides for the interception of the content of electronic communication, it does not allow for unrestricted interception.[109] An officer must make an application to a judge in order to intercept any electronic communication.[110] After examining the application, the judge may enter an order authorizing such interception, provided that there is probable cause for the belief that the individual whose communication is about to be intercepted has engaged, or is about to engage in a particular offense.[111] If an officer

---

104 *See An Overview of Electronic Surveillance: History and Status supra* note 91. *See also* 18 U.S.C. § 2516(1) (2000) (providing that "the Attorney General, Deputy General . . . may authorize the application to a Federal Judge . . . for . . . an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation). *See also* 18 U.S.C. § 2517(2) (2000) (providing that "any investigative or law enforcement officer who . . . has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.").

105 18 U.S.C. §§ 2510-3127 (2000).

106 *See An Overview of Electronic Surveillance: History and Status supra* note 94 (explaining that many of the new technological advancements "stretched the framework of Title III. Electronic mail, data interchange, medical records and fund transfers are examples of potentially confidential communications that did not fit within the original Title III definitions of oral and wire communications.").

107 18 U.S.C. § 2510(1) (2000).

108 *See* Carnivore FAQ, *supra* note 12 (enumerating the laws governing Carnivore, including the Omnibus Crime Control and Safe Streets Act of 1968 and the ECPA).

109 *See* 18 U.S.C. § 2518(1) (2000) (providing that "each application for an order authorizing or approving the interception of a wire, oral, or electronic communication . . . shall be made in writing upon oath or affirmation to a judge. Each application shall include the following information: (a)identity of the law enforcement officer, (b)a full and complete statement of the facts and circumstances relied on by the applicant, etc.).

110 *See* 18 U.S.C. § 2518(1)(a)-(f) (2000).

111 *See* 18 U.S.C. § 2518(3)(a) (2000) (providing that "upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or

violates any provision of this Act, a customer of an electronic service, or the service, itself, may seek recovery in a civil action.[112] Such relief may include an injunction, damages pursuant to §2707(c), and reasonable attorney's fees.[113] It is these remedies for violations that proponents of Carnivore argue will assure FBI compliance with the ECPA.[114]

While the standard to intercept the content of one's e-mail is that of probable cause,[115] a judge may issue an order for a pen register or trap and trace device, like Carnivore, on the basis that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[116] This lower burden of proof, along with the unique nature of pen registers and trap and trace devices on the Internet environment is a demonstration of the inadequacy of current wiretapping laws.

---

approving interception of wire, oral, or electronic communications . . . if the judge determines that there is probable cause for the belief that the individual is committing, has committed, or is about to commit a particular offense." In addition, § 2518(b) permits a judge to grant an officer's application if there is "probable cause for the belief that particular communications concerning that offense will be obtained through such interception." § 2518(c) allows interception if the judge determines that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."). *See infra* part II for a discussion of "probable cause."

112 *See* 18 U.S.C. § 2707 (2000) ("Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter . . . may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.").

113 *See* 18 U.S.C. §2707(b)-(c) (2000) ("The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person (be) entitled to recover (or) receive less than the sum of $1000.").

114 *See* Kerr's testimony, *supra* note 76 (arguing that it is unlikely for FBI agents to violate the ECPA and abuse Carnivore because of their high moral caliber. Furthermore, if violations do occur, agents will be subjected to criminal prosecution, civil liability, pursuant to 18 U.S.C. § 2707, and termination.).

115 *See* Carnivore FAQ, *supra* note 12 (explaining that "at least for now, the government considers tapping your e-mail a serious thing and curtails most of the FBI's ability to read it."). *See also* Caroll v. U.S., 267 U.S. 132 (1925) (holding that a showing of probable cause includes the facts and circumstances within one's knowledge sufficient to warrant a person of reasonable caution to believe that a crime has been committed or that property subject to seizure is at a designated location).

116 18 U.S.C. § 3123(a) (2000).

In the wake of terrorist attacks, however, Congress once again decided to amend provisions of ECPA.[117]Both the House and the Senate collectively termed these amendments the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act, or more succinctly, the USA Patriot Act, (Patriot Act).[118] The Act, which amends a host of statutes, including but not limited to ECPA, contains more that 270 sections.[119]Section 216 amended 18 U.S.C. §§3121, 3123, 3124, and 3127 "to clarify that the pen/trap statute applies to a broad variety of communications technologies."[120]In contrast with the 1986 version of §3127, the current statute explicitly includes e-mail interception programs like Carnivore.[121]

III. (A) THE INAPPLICABILITY OF THE ECPA TO CARNIVORE BEFORE THE PATRIOT ACT

As previously mentioned, the impetus in enacting the ECPA was to keep up with the ever-growing realm of super technologies.[122] ECPA, however, prior to September 11, 2001, did not cover

---

117 President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, hereinafter Patriot Act, into law on October 26, 2001. *See* Martha Mendoza, *Response to Terror: New Anti-Terror Law Brings Consternation; Security: Officials and Lawyers Try to Decipher Complex Provisions*, L.A. TIMES, Dec. 16, 2001 at 4.

118 Pub. L. No. 107-56 (HR 3162) (2001); *see also* Neil Lewis and Robert Pear, *A Nation Challenged: Legislation; Terror Law Nears Votes in House and Senate*, N.Y. TIMES, October 5, 2001 at B8.

119 Pub. L. No. 107-56 (2001).

120 Field Guidance on New Authorities, at http//: www.epic.org/privacy/terrorism/DOJ_guidance.pdf (last visited January 8, 2001) (enumerating the effects of the Patriot Act on different statutes). "Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect, and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device . . . on computers belonging to a public provider." *Id. See also* 18 U.S.C. § 3127(3) (2001) ("the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information does not include the contents of the communication.").

121 18 U.S.C. § 3127(3) (2001).

122 *See An Overview of Electronic Surveillance: History and Status supra,* note 94.

the use of Carnivore.[123] In order to come to an understanding as to why ECPA was inapplicable it is essential to understand the way in which trap and trace/pen registers function on a traditional telephone line.[124] In contrast to these more traditional taps, one must further analyze the way in which these same surveillance tools operate when the Internet becomes involved. When placed on a telephone line, trap and trace/ pen registers only collect the telephone numbers of the incoming and out going calls.[125] The 1986 ECPA defined a "pen register" as a device which "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such a device is attached."[126] Immediately one recognizes that the information gathered by Carnivore did not fall within the plain meaning of the statute.[127] Carnivore gathers, in its less invasive form, the header of an e-mail not impulses that "identify the numbers dialed."[128] This header does not contain any numbers like the information gathered by trap and trace/ pen registers. In addition, it collects the URL addresses of the sites that the suspect visits.[129] It cannot be debated. This information goes far beyond the non-identifying numbers collected by traditional traps.

What are the implications of this sweeping, intrusive search? In collecting information more than just the statutorily recognized numbers, Carnivore is not only functioned outside the ECPA, but it did not even functioning as a trap and trace device nor as a pen register. With the advancements of technology, courts have been

123 *See* Field Guidance, *supra* note 120 (explaining that "when congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and did not unambiguously encompass communications over the computer networks.").

124 *See* Carnivore FAQ, *supra* note 12.

125 *See* Carnivore FAQ, *supra* note 12.

126 *See* 18 U.S.C. § 3127(2000).

127 *See* 18 U.S.C. § 3127(3) (2000) (excluding "any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or customer of a wire communication service for cost accounting or other purposes in the ordinary course of business.").

128 18 U.S.C. § 3127(3) (2000).

129 *See* Carnivore FAQ, *supra* note 12.

reluctant to squeeze new surveillance tools under the narrow definition provided under the ECPA.[130]

Brown v. Waddell is an example of such reluctance.[131] In *Brown*, the Fourth Circuit questioned whether the implementation of a display pager by law enforcement officials constituted a use of a pen registered as defined by the ECPA.[132] The Circuit Court, reversing the determination that the pager fell within the ambit of the ECPA, held that the device was not a "pen register."[133] The court scrutinized the statue, extrapolating very important requirements.[134] The court noted that the statute requires the pen register to be attached to the telephone line.[135] The pager, a stand alone piece of equipment, was not affixed to the telephone line. Similarly, Carnivore is not attached to a telephone line, it is attached to an ISP's network, a data center.[136] Given this distinction, under the holding of *Brown,* an in-depth analysis leads to the conclusion that

---

130 *See* Testimony of Robert Corn-Revere before the Subcommittee on the Constitution of the Committee on the Judiciary, April 6, 2000 (explaining that courts have interpreted the ECPA very narrowly and applied it only when a device fits within the plain meaning of the statute. "Consistent with the statutory language . . . reviewing courts have interpreted these provisions literally.").

131 *See* Brown v. Wadell, 50 F.3d 285 (4th Cir. 1995) (holding that use of a clone pager, one that mimics the signals coming into another pager, did not fall within the ECPA's definition of a "pen register" because of its ability to function without being affixed to a telephone line. The courts rational was based heavily on statutory interpretation and the legislative history of the ECPA. For example, the court stated that "the type of communication that it receives fits perfectly into the general definition of the 'electronic communications' that are subject to" the more stringent requirement of probable cause.).

132 *See id.*

133 *See id.*

134 *See id.* 50 F.3d 285 at 289 (noting that both the attachment, or in this case, the non-attachment, of the device's as well as the signals received are dispositive to the devices classification as a pen register).

135 *See id.* 50 F.3d 285 at 290 (quoting from 18 U.S.C. § 3127(3)(2000) "a 'pen register' is defined by statute as a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached).

136 *See* About.com, *supra* note 13 (describing the manner in which an FBI agent attaches Carnivore. "For Carnivore to gain access to this much data, its hardware must be plugged directly into the network at a central location. Because most Internet-based communications in the USA flow through large Internet Service Providers (ISPs), the FBI would typically install a Carnivore box inside an ISP *data center*. Controlled physical and network access improves the system's overall security.").

Carnivore would not have been a trap and trace device nor a pen register as defined under the ECPA.

Given the reluctance in *Brown* to find a device not specifically attached to a telephone line within the statute, a court would have been unlikely to have extended the ECPA to Carnivore because it does not collect "numbers to which calls have been placed." Carnivore captures e-mail addresses. Such a function differs greatly from that of a pen register or trap and trace device defined in the statute. The *Brown* court specifically recognized that the signals received by the pager were not telephonic, but rather radio waves.[137] This difference placed the pager out of the realm of "pen registers" and into the realm of "electronic communication."[138] If a court would have found the non-attachment as a deviation from ECPA, the fact that Carnivore collects not numbers, but addresses, would have been as great a deviation.

The fact that Carnivore collects e-mail addresses raises another problem separate from the exclusion of the system under the statue's definition of a trap and trace device or pen register. It can be argued that this information is not purely transactional, but is rather "content." ECPA defines "content" as "*any* information concerning the substance, purport, or meaning of that communication."[139] It only contemplates the retrieval of telephone numbers.[140] But as pointed out, e-mail addresses are not numbers; they are combinations of letters and numbers. The Congressional intent in enacting the ECPA was to exclude information bearing any resemblance to "content" from the section defining trap and trace devices and pen registers.[141]

In *Brown*, the 4th Circuit engaged in an analysis of the legislative history behind the 1986 federal wiretapping laws.[142] It noted that Congress sought to distinguish technologies that are capable of

137 *See Brown*, 50 F.3d 285 at 289.
138 *See id.*
139 *See* 18 U.S.C. § 2510(8) (2000).
140 *See* 18 U.S.C. § 3127(3) (2000).
141 *See Brown*, 50 F.3d 285.
142 *See Brown*, 50 F.3d 285 at 289 (paraphrasing the intent of Congress in enacting the ECPA. "The principal purpose of the ECPA amendments to Title III was to extend to 'electronic communications' the same protections against unauthorized interceptions that Title III had been providing for 'oral' and 'wire' communications via common carrier transmissions. This extension was found necessary by Congress because of the 'dramatic changes in new computer and telecommunications technologies that had created new risks to privacy.').

intercepting substantive content from those that cannot.[143] "Content" information is the type of information in which people have a reasonable expectation of privacy.[144] In quoting from Congress, the court concluded that those forms of technology that intercept content without a warrant based on probable cause are illegal.[145] Such a distinction can be seen, pointed out the court, by Congress' recognition of pagers capable of collecting alphanumeric (letters and digits) characters.[146] These pagers collect substantive content. If Congress and the court believed that the alphanumeric pagers collect "substantive content," then the same protection should be afforded to alphanumeric e-mail addresses.

Steinheardt, Associate Director of the ACLU, pointed out in his testimony before the House Judiciary Committee that e-mail addresses differ from phone numbers in two significant ways.[147] First of all, argues Steinhardt, many people, over the course of time, may be assigned the same phone number.[148] Phone numbers are not personalized like an e-mail address. As a matter of fact, E-mail servers are designed so as not to assign the same e-mail address twice.[149] Every address is unique. Secondly, the classification of e-mail addresses as "content" is strengthened by the fact that an e-mail address may contain some "information concerning the substance, purport, or meaning of that communication."[150] For example, an address like Bob@pornpics.com may contain information, namely the wording following the @ symbol and the sender's name (Bob), as to the content of the e-mail. There is no specific amount of information required to fall under the classification of "con-

---

143 *See Brown*, 50 F.3d 285 at 291 (explicating the different requirements for pen registers and wiretaps. The former requires a showing of probable cause because of its ability to intercept "content.").

144 *See* Smith v. Maryland, 442 US 735 (1979) (holding that a pen register was incapable of intruding on a legitimate expectation of privacy because it recorded only phone numbers, information routinely turned over to third parties).

145 See *Brown*, 50 F.3d 285.

146 See *id.*

147 *See* Testimony of Barry Steinhardt, Associate Director of the ACLU before House Judiciary Committee Subcommittee on the Constitution, (July 24,200) (explaining the differences between traditional pen registers and Carnivore. Carnivore, unlike traditional pen registers collects e-mail addresses.).

148 *See id.*

149 If an individual tries to duplicate an e-mail address, a message will come up stating that "this user name has already been taken."

150 *See* 18 U.S.C. § 2510(8) (2000).

tent."[151] Section 2510(8) only calls for "any" information concerning the substance of a given communication.[152] Since there is a possibility that an e-mail address may contain information as to the content of the e-mail, it is itself, content.

Additionally noted Steinheardt, as a trap and trace/pen register, Carnivore is capable of collecting the URL addresses that a suspect has visited.[153] This information reveals much in the way of content. If I visit www.childporn.com, the content of the information perceived while at the site is not precise, but quite obvious, nonetheless.

The categorization of e-mail and URL addresses as content based is a significant factor, if not the most relevant to consider, when determining which provision, if any, of ECPA applies.[154] Under §3123, as a pen register or trap and trace device, only a showing that the "information likely to be obtained by the installation is relevant" is required.[155] But as previously stated, this standard only applies when the information sought is not "content." Once "content" is involved, the burden of proof increases to the more stringent "probable cause" pursuant to §2518.[156] Under these requirements, law enforcement officials utilizing Carnivore, even in its least intrusive manner, as an alleged pen register or trap and trace device, must be required to put forth probable cause. Since the ECPA does not require a showing of probable cause for the implementation of a pen register or a trap and trace device, it does not cover a beast such as Carnivore.

A problem related to Carnivore's ability to capture content information when functioning as a pen register or trap and trace de-

---

151 *See* 18 U.S.C. § 2510(8) (2000).

152 *See* 18 U.S.C. § 2510(8) (2000).

153 *See* Testimony of Barry Steinhardt, *supra* note 147 (stating that "beyond e-mail addresses, there are unanswered questions about whether pen registers and trap and trace devices can be used to obtain other sensitive information. For example, can they be used to collect URL's of sites that a target visits, the names of files that are transmitted, subject headers of e-mail, or other transaction logs of Internet activity.).

154 *See Brown*, 50 F.3d 255 at 292 (explaining that information that is not content based is not the type in which people have a reasonable expectation of privacy. For example, it has been noted that "there are no legitimate expectations of privacy in the telephone numbers that one calls, so that no warrant is required by the Fourth Amendment to install a pen register.").

155 *See* 18 U.S.C. § 3123(a) (2000).

156 *See* 18 U.S.C. § 2518(3)(a) (2000).

vice is its ability to capture content as a "content wiretap."[157] In contrast with its functionality as a pen register or a trap and trace device, as a wiretap, Carnivore is capable of reading the entire contents of a given e-mail.[158] To be used in this capacity, a law enforcement official must get an order based on a showing of probable cause.[159] When acting as a pen register or trap and trace device, the wiretapping capabilities of the system are "turned off."[160] In essence, Carnivore may be converted from a content wiretap to a pen register or trap and trace device.[161] In at least one case, New York courts have addressed the issue of a convertible wiretap.[162] In *People v. Bialostok*, the Court of Appeals held that a pen register capable of being used as a full blown wiretap on a telephone line could be utilized only upon a showing of probable cause.[163] The fact that the wiretapping capabilities of the register had been turned off did not erase the need for the heightened showing.[164] This rationale has been restated in subsequent cases, quoting the general holding of *Bialostok*.[165] Such an analysis, while based on state law, is analogous to Carnivore.

---

157 *See* Carnivore FAQ, *supra* note 12.

158 *See id.*

159 *See* 18 U.S.C. § 2518(3)(a) (2000).

160 *See* Carnivore FAQ, *supra* note 12.

161 *See* Testimony of Robert Corn-Revere, *supra* note 130 (explaining the specialized problem of devices that need to be converted from content wiretaps to pen registers. This dual nature causes much confusion as to their classifications and therefore the applicability of the ECPA.).

162 *See* People v. Bialostok, 610 N.E. 2d 374 (1993) (holding that a pen register that could be transformed into an eavesdropping device required a showing of probable cause to obtain a warrant for its use. The officer was able to transform the pen register by attaching an audio cable, a tape recorder and a wire to activate the recorder's remote start. Even though the pen register had the capabilities of performing as an eavesdropping device, no evidence of the sort was introduced at trial.).

163 *See id.*

164 *See Biolostak*, 610 N.E. 2d 374 at 377 (clarifying that the "People's case is no stronger because the audio functions were disabled and no conversations were actually overheard. The issue is not of the reasonableness of the search but statutory compliance. . . . The purpose of having a warrant is to . . . protect the people from having to rely on the good conduct of the officer in the field for the protection of their right to be free from unreasonable searches.).

165 *See* People v. Kramer, 706 N.E.2d 731 (1998) (holding that defendants had standing to seek judicial suppression of telephonically acquired evidence by a pen register that had the capabilities to intercept and record either digital or aural transmissions. Such communications could be recorded depending upon whether

If the ability of Carnivore to function as a "content" wiretap raises the standard from relevancy to probable cause, what may be said about Carnivore's ability to act as a "trunk side" wiretap? As a "trunk side" wiretap, Carnivore may access the e-mail of every user on the Internet.[166] The FBI argues that they may place a filter on Carnivore to prevent such collection.[167] But, the *Bialostok* court quoting from the Court of Appeals' opinion in *People v. Gallina* states "that no unauthorized eavesdropping may have occurred is beside the point, because it is the potential for abuse that is the focus of the analysis."[168] Such a statement directly refutes the position of the FBI. FBI agents may be "trustworthy" and may not employ Carnivore as a "content" wiretap or a "trunk side" wiretap. But, such abstention is "beside the point." What really matters is that Carnivore, as a "content" wiretap carries with it the high possibility of abuse. Even more potentially abusive is its function as a "trunk side" wiretap. Under the logic of *Bialostok*, the ability to convert requires a focus on this potential for abuse and an adjustment of the standard of proof required to install Carnivore.

III. (B) GOVERNMENT'S RESPONE TO THE 'INAPPLICABILITY PROBLEM'

Recognizing that there was an increased need to use programs like Carnivore, so as to keep track of potential terrorists, the President signed into law the Patriot Act.[169] As mentioned above, the Patriot Act changed the literal definition of "pen register" so as to include programs like Carnivore. In doing so, the fact that Carnivore does not collect impulses that "identify the numbers dialed" is no longer fatal to the application.

The fact that the statute, however, is seemingly applicable does not solve everything. For example, the Patriot Act does not delineate the difference between "content" and "non content" information as discussed above. Carnivore still collects content information

---

the officer switched on an audio switch. While in "audio off" mode, the device only intercepted telephone numbers.).

166 *See* Schwartz, *supra* note 23 and accompanying text.

167 *See* Letter from John Collingwood, *supra* note 71.

168 *See Bialostok,* 610 N.E. 2d 375 at 375.

169 Neil Lewis and Robert Pear, *A Nation Challenged: Legislation; Error Law Near Votes in House and Senate,* N.Y. TIMES, Oct. 5, 2001, at B8 (quoting Attorney General Ashcroft, "without the new legislation, law enforcement authorities lack all of the tools they need to thwart terrorists.").

and is treated under the new law as if it does not. This distinction is far more relevant to the intrusion of privacy than that of inclusion under the definition of "pen register".

IV. CARNIVORE TAKES A BITE OUT OF FOURTH AMENDMENT PROTECTIONS

As a result of allowing Carnivore to operate, even in its least ferocious form, without a showing of probable cause, every citizens' right to privacy on the internet slowly diminishes.[170] In other words, allowing these warrantless searches implicates the Fourth Amendment.[171] The Fourth Amendment, governing all governmental searches and seizures, contains two separate clauses: "a prohibition against unreasonable searches and seizures, and a requirement that probable cause support each warrant issued."[172] While the problem presented by Carnivore is an amalgam of the two clauses, the strongest argument involves unreasonable searches. Without a warrant based on probable cause a Carnivore search of header information (To: and From: statements) is unreasonable.[173] In order to explain this problem in depth, we must decide if, according to *Katz*, people have a "reasonable expectation of privacy" in their e-mail header information.[174] In doing so, *Katz* tells us to answer two questions: 1) whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy and 2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as

170 *See* Elinor Abreu, *ACLU Investigating Carnivore's Diet*, http://www.thestandard.com/article/display/0,1151,16877,00.html (last visited October 6, 2000) (quoting David Sobel, attorney for EPIC. Sobel says, "This system potentially compromises the privacy of all of the ISP's subscribers.").

171 *See* 68 Am. Jur. 2d § 327 (2000) (explaining how the use of electronic surveillance constitutes a search under the Fourth Amendment. "With the exception of situations involving the national security, electronic surveillance . . . constitutes a search and seizure within the meaning of the Fourth Amendment.").

172 Kevin Allen, *Overview of the Fourth Amendment*, 88 GEO. L. J. 883 (2000) (explaining the requirements of the Fourth Amendment. "The Supreme Court imposes a presumptive warrant requirement for searches and seizures, and generally requires probable cause for a warrantless search or seizure to be "reasonable.").

173 *See id.*

174 *See Katz*, 389 U.S. 347 (holding that a defendant had a "reasonable expectation of privacy" in conversations taking place in a telephone booth).

'reasonable.'"[175] The first prong of the test is purely subjective while the second prong is objective.[176]

In explicating this second objective standard, courts often look at the nature of the intrusion and whether or not a third party has access to the information revealed in the search.[177] For example, the Court in *Smith* concluded that there was no objective expectation of privacy in phone numbers retrieved by a pen register.[178] Since the search did not reveal any "content" and the telephone company had access to these numbers, the second prong of the *Katz* test was not satisfied.[179]

Along the same lines, the Supreme Court held in *United States v. Miller* that a defendant had no legitimate expectation of privacy in his bank records since the bank was a third party to which he disclosed his affairs when he opened the account.[180] While the Court did not focus as much on the nature of the intrusion, i.e. whether the information contained "content," it heavily emphasized that the Fourth Amendment was not a bar to information revealed to a third party.[181]

---

175 *See id.* at 361 (explaining how the twofold requirements work. For example "a man's home is, for most purposes, a place where he expects privacy . . . On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable). *See also* 68 Am. Jur. 2d §327 (outlining the framework for determining whether a reasonable expectation of privacy exists. "Whether a warrantless eavesdropping by the police violates the Fourth Amendment depends on whether the defendant had a justified expectation of privacy at the place and the time of the communication.").

176 *See id.*

177 *See Smith*, 442 U.S. 735, 741 (applying the *Katz* analysis, the Court says that "it is important to begin by specifying precisely the nature of the state activity that is challenged." The Court noted that the pen register installed on defendant's telephone line did not retrieve any contents. In addition, the Court focused on the fact that third parties, namely the telephone company, had access to phone numbers dialed by their customers. These two factors led the court to conclude that there was no objective expectation of privacy in such phone numbers.).

178 *See id.*

179 *See Smith*, 442 U.S. 735, 745.

180 *See* U.S. v. Miller, 425 U.S. 435 (1976) (reversing an order of the appellate court which found that defendant's bank records should have been suppressed. The Court held that by giving the records to the bank, defendant surrendered his privacy expectations in them.).

181 *See Smith*, 442 U.S. 735, 443. (explaining that "this Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to the Government authorities,

More recently, the United States Court of Appeals reinforced the notion that one who conveys information to a third party thereby relinquishes his reasonable expectation of privacy in such.[182] In *U.S. v. Hambrick*, the fourth circuit Court of Appeals refused to suppress billing records which contained non-content information.[183] The *Hambrick* court followed an identical approach to the Court in *Smith v. Maryland.* It first addressed the issue of content. It found that the defendant's name and several of his phone numbers, the information seized, did not contain any content.[184] The Appellate Court next turned its attention to the fact that the defendant voluntarily handed the information over to a third party, the ISP.[185] Such an act, as in *Smith*, precluded the defendant's Fourth Amendment argument.[186]

---

even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed).

182 *See* U.S. v. Hambrick, 2000 U.S. App. LEXIS 18665 (4th Cir. 2000) (affirming the judgment of the district court holding that defendant did not have a legitimate expectation of privacy in non content information given to an internet service provider in order to establish an account. *Hambrick* is more than just a modern application of *Smith*. In dicta, the court stated that "in this case, the government never utilized the non-content information retrieved from the (ISP) to attain additional content information, such as the substance of Hambrick's e-mails." *See Hambrick* at 12. Additionally, the court recognized the 'revolutionary' "nature of the internet as well as the vast extent of communications it has initiated. We do not address here any subsequent use of the non-content information to reveal the substance of an Internet user's e-mails or other file content." This is an important distinction between the information obtained here and that obtained by Carnivore. Many times, FBI agents use the alleged "non-content" header information to obtain a warrant seeking the contents of a defendant's e-mail. Under *Hambrick*, such a use might change the holding.).

183 *See id.* 2000 U.S. App. LEXIS 18665 at 11 (explaining that the information in question included Hambrick's name, address, home, work, and fax phone numbers. The court reiterated the holding in *Miller*, namely that 'the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena issued.'").

184 *See id.* 2000 U.S. App. LEXIS 18665 at 12 (stating that "while under certain circumstances a person may have an expectation of privacy in content information, a person does not have an interest in account information given to an ISP . . . which is non-content information).

185 *See id.*

186 *See id.* (relying on *Miller*, the Court of Appeals concluded that this information is "merely third party business records, and therefore, [defendant's] Fourth Amendment claim cannot succeed").

Assuming that a suspect believes, subjectively, that he has an expectation of privacy in the information collected by Carnivore and applying these principles relating to the second prong of *Katz,* we can conclude that this information falls within the ambit of Fourth Amendment protection. First, the information collected by Carnivore, as stated previously, is content information, under the ECPA. The Supreme Court in *Smith* strengthens this conclusion.[187] The Court defined "content" information as any information that gives an indication as to the "purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[188] The information seized by Carnivore would fall under the *Smith* definition of "content" because it not only gives an indication as to the content of the communication, as discussed above, but also reveals the identities of the sender and the receiver and is an acknowledgement that the delivery of a message was "completed."

The inquiry that must be made is whether the information collected by Carnivore was ever turned over to a third party. There is absolutely no reason to assume that the e-mail addresses that Carnivore intercepts have been turned over to anyone other than the receiver and sender of any message in question. Often times people do not give out their e-mail addresses for fear of receiving unwanted "Spam." Other times, an individual may create more than one e-mail account and only give out one address, saving the other as an account for privileged senders. Absent some concrete evidence of exposure to third parties, it is not safe to assume that any given e-mail address has been made available. Since the information collected by Carnivore is "content" under both the ECPA and *Smith* and the information is not voluntarily handed over to a third party, one has a legitimate expectation of privacy in it, satisfying the second prong of the *Katz* test. Since both prongs of the test are met, collection of this information without a warrant forms a prima facie case for a violation of the Fourth Amendment.

---

[187] *See Smith*, 442 U.S. 735, 741 (quoting from the holding in *U.S. v. New York Tel. Co*, 434 U.S. 159, 167, the court defined "content" information).

[188] *See id.*

V. CONCLUSION

Such an analysis is not to suggest that technology has no place in the crime- fighting world. It is only meant to point out pitfalls into which we, the government, and law enforcement officials might step when introducing the future to the present. The fundamental rationale behind Carnivore, namely to stop Internet crime, is not something that should be scoffed at. The goal of the tool is laudable. But, the tool itself, enhances the danger involved. Carnivore is, all joking aside, a beast. It devours our Internet privacy. If people on the net are to feel secure, we must put a leash on the beast. In other words, the most intrusive aspects of Carnivore, namely its ability to collect all mail and activity on an ISP must be done away with. Carnivore's program must be reconfigured – permanently.

If law enforcement officials are not willing to mitigate Carnivore's potential for abuse, then there is only one more viable option; Congress must change the law. The ECPA must be amended to reflect the ease at which new technologies may obliterate our right to privacy. Specifically, the EPCA must introduce a hybrid category—a definition that covers a device capable of morphing from a "pen register" to a "content wiretap" to a "trunk side wiretap." Congress must consider just exactly how ferocious a device such as Carnivore may be.

If neither road is traveled, then Internet users all over the world, not just the United States, are left vulnerable. The only thing standing in the way of such abuse is the "trust us" attitude of the FBI. Such a notion is archaic and contrary to the existence of the Fourth Amendment. If Carnivore cannot be caged, then we might as well consider our right to privacy as unprotected as it was millions of years ago when dinosaurs of a different breed roamed the earth.

Gina Tufaro