A CONSTITUTIONAL CRISIS IN THE DIGITAL AGE: WHY THE FBI'S "CARNIVORE" DOES NOT DEFY THE FOURTH AMENDMENT

A suspected drug smuggler types anxiously into his computer. He hurriedly writes an e-mail[1] to an overseas accomplice, confirming plans for the importation of two tons of cocaine into the United States. The smuggler's highly incriminating message, if seized by law enforcement agents, could effectively place him in prison for life. His hand trembling slightly, the smuggler dispatches the message. As the revealing e-mail rushes across swiftly moving streams of digital data, racing furiously to its destination, it is suddenly stopped and sniffed by a powerful Orwellian[2] watchdog that lives and breathes in "cyberspace."[3] That imposing watchdog, controlled by the Federal Bureau of Investigation (FBI) and installed at various Internet[4] Service Providers ("ISPs")[5] around the

---

[1] E-mail is short for "electronic mail" and it is the most common, basic function that allows individuals to correspond using computers. *See* Robert S. Steere, Note, *Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 231 (1998).

[2] *See* GEORGE ORWELL, 1984 (New Amer. Lib. Classics 1990) (1948).

[3] Cyberspace is the nonphysical environment in which the Internet operates, it is as ubiquitous as the air we breathe and as amorphous as tiny gaseous particles we do not see. The term was coined in William Gibson's 1984 book, "Neuromancer". *See* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591 n.4 (1997); *see also Guide to the Ways and Words of Cyberspace*, TIME, Special Issue, Spring 1995, at 42-43 (containing some basic cyberspace terminology); Michael Johns, Comment, *The First Amendment and Cyberspace: Trying to Teach Old Doctrines New Tricks*, 64 U. CIN. L. REV 1383, 1383 (1996) (detailing cyberspace as the "conceptual space where words, human relationships, data, wealth and power are manifested by people using computer technology"). The term cyberspace connotes more than just the Internet itself. It encompasses Bulletin Board systems, public and private computer networks, and all e-mail and electronic data interchange systems. *See* Jay Krasovec, Comment, *Cyberspace: The Final Frontier, for Regulation?* 31 AKRON L. REV. 101, 101 n.1 (1997).

[4] The Internet, or "Net," is a loose connection between millions of computers at different places around the world that share information and data files. *See* Krasovec, *supra* note 3, at 103. These computers, working in unison, create a connection and in turn, numerous systems form networks. *See id.* These networks can be likened to a "spider's web" where communication software manages the different computer connections. *See id.* The individual computer user perceives the entire system to be a special network, the Internet. *See id.* at 103 n.11 (citing Giorgio Bovenzi, *Liabilities of System Operators on the Internet*, 11 BERKELEY TECH. L.J. 93, 97 (1996)). The Internet was developed for reasons relating to the Cold War in the 1960s, when the Department of Defense ("DOD") created the Advanced Research Project Agency Network ("ARPANET") to connect the DOD's computers. *See id.* at 104. The Internet thus had its origins as a research and investigative tool for the government. The courts have recognized the inconspicuous origins of the Internet as well. *See* Shea *ex. rel.* Am. Reporter v. Reno, 930 F. Supp. 916, 925-27 (S.D.N.Y. 1996) (detailing the experimental origins of the Internet and offering a broad overview of Internet communications).

[5] *See* Ariana Eunjung Cha, *Carnivore Debate Centers on FBI Trustworthiness*, WASH. POST, Sept. 13, 2000, at E3 (explaining that ISPs are computer networks that send and deliver e-mail, acting as portals to the Internet. A popular example of an ISP is "America Online"(AOL)).

country is notoriously named "Carnivore,"[6] and it is the subject of a raging debate over Fourth Amendment[7] privacy issues in the digital age. Privacy advocates, in response to Carnivore's arrival, demanded a full, independent review of Carnivore's capabilities and have expressed outrage that the source code that permits Carnivore to function has not been made publicly available.[8] The FBI subsequently assigned an independent[9] review commission to study

---

[6] Although originally titled "Carnivore," the system has recently been renamed "DSC100." *See* Duncan Levin, SUN-SENTINEL, Mar. 12, 2001, at 23A (detailing that because the name conjured up "so many unflattering images of flesh-eating animals" the FBI decided to switch the name). However, since the system was made immediately popular by its original, controversial title, and because the public still commonly knows it as such, this Note will continue to reference the program by its original name. As one critic declared: "If it prowls like a wolf, howls like a wolf and has the voracious appetite of a wolf, it's still a carnivore." *See* Jim Wolf, SAN DIEGO UNION-TRIB., Feb. 20, 2001, at 8. The Carnivore system was first widely reported on July 11, 2000. *See* Electronic Privacy Information Center, *The Carnivore FOIA Litigation, at* http://www.epic.org/privacy/carnivore/default.html (Nov. 1, 2000) [hereinafter EPIC].

[7] The Fourth Amendment provides:

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

U.S. CONST. amend. IV. The case law applying the Fourth Amendment in cyberspace is relatively sparse, as cyberlaw is still an emerging area of jurisprudence. A number of Fourth Amendment questions in general have been posed in reference to computer law. *See* 2 MICHAEL D. SCOTT, SCOTT ON COMPUTER LAW § 17.07 (2d ed. 1992). Such questions have been set forth as follows:

> (1) Whether [the Fourth Amendment] protects records in a computer from unreasonable search and seizure; (2) Whether it is permissible to issue warrants on the strength of computer-based information with no personal knowledge of the accuracy or timeliness of that information on the part of the affiant; (3) The amount of detail necessary in a warrant for the search of a computer or a facility containing computerized records; and (4) The permissibility, because of the complex nature of computerized evidence, of bringing in a civilian expert to assist law enforcement officers in the search.

Id. The computer law treatise also suggested that courts in general will use a "common sense approach" when applying the Fourth amendment to computer technology. *Id.*

[8] *See* William Glanz, *"Review" Urged for FBI Plan for E-Mail*, WASH. TIMES, Sept. 7, 2000, at B9 (detailing how libertarian agencies such as the "Center for Democracy and Technology" are alarmed because the FBI has not allowed them to fully examine Carnivore, which, they insist, is a grave opportunity for abuse). After initial disclosures made by the FBI, the EPIC filed a Freedom of Information Act (FOIA), *see* 5 U.S.C. § 552 (1994 & Supp. 1999), request seeking the release of all Carnivore's technical details, including its source code and other unique specifications. *See* EPIC, *supra* note 6. The FBI ultimately released some documents but many technical details, including Carnivore's source code, had been redacted, leaving Carnivore a partial mystery. *See id.*

[9] The American Civil Liberties Union (ACLU), however, does not consider the review team independent at all, but rather believes they are biased in favor of the government. *See* Telephone Interview with Christopher Chiu, Global Internet Policy Analyst, American Civil Liberties Union (Feb. 20, 2001) [hereinafter Chiu Interview]; *see also* Michael J. Sniffen, *U.S. to Pick Team to Evaluate FBI E-Mail Tap; Foes Doubt Independence*, CHI. TRIB., Aug. 11, 2000, at 16. As Barry Steinhardt, associate director of the ACLU, declared: "This is not a truly independent review . . . . [T]he fox doesn't get to choose who guards the hen house." *Id.* at 16.

and evaluate Carnivore.[10] According to some civil libertarians, this country places itself in an extremely dangerous position when only the FBI knows the true power of Carnivore, and it is foolish to trust the FBI not to abuse its new tool against cyber-crime.[11] The FBI argues that to expose the secret source code of Carnivore would make it susceptible to the whims of hackers.[12] Additionally, the FBI claims, in an age where terrorists and criminals have increasingly turned to the Internet to engage in illegal activity,[13] Carnivore is a useful and necessary instrument that perfectly tailors its search to properly balance the privacy of individuals against the advancement of law enforcement. The FBI even argues that Carni-

---

[10] The study was conducted by the IIT Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law. *See Independent Review of the Carnivore System, Draft Report, at* http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (Nov. 17, 2001) [hereinafter *Independent Review*]. The purpose of the study, as stated in the Independent Review, was to report on whether Carnivore:

> (a) Provide[s] investigators with all, but only, the information it is designed and set to provide in accordance with a given court order; (b) Introduces any new, material risks of operational or security impairment of an Internet Service Provider's (ISP's) network; (c) Risks unauthorized acquisition, whether intentional or unintentional, of electronic communication information by: (1) FBI personnel or (2) persons other than FBI personnel; and (d) Provides protections, including audit functions and operational procedures or practices, commensurate with the level of the risks . . . . [Q]uestions of constitutionality of Carnivore-type intercepts and trustworthiness of law enforcement agents were outside the scope of evaluation.

Id.

[11] *See* Kevin Butler, *Is Big Brother Surfing the Internet? FBI's Carnivore Raises Privacy Issue*, INVESTOR'S BUS. DAILY, Aug. 9, 2000, at A22. Barry Steinhardt of the ACLU stated: "The FBI asks us to trust them, because they're the government, that they will only look at those communications to which they have a right under a proper court order . . . . [B]ut they have a long history of abusing trust." *Id.* at 22. For example, the FBI has been accused of spying on Dr. Martin Luther King Jr., Eleanor Roosevelt and Supreme Court Justice William Douglas. *See id.*

[12] The FBI fears that exposing Carnivore's code will result in hacking efforts that might exploit Carnivore and ultimately wreak havoc on the Internet, causing great damage. *See* Steve Mathieson, *U.S. Users Bite Back Over Their Right to Privacy*, NETWORK NEWS, Sept. 13, 2000, at 10.

[13] *See Digital Privacy and the FBI's Carnivore Internet Surveillance: Hearing Before the Senate Judiciary Committee*, 106th Cong. (2000), *available at* LEXIS, News Library, Federal News Service File [hereinafter *Senate Hearing*]. In the hearing testimony, Dr. Donald M. Kerr, Assistant Director of the FBI, explained that Carnivore was developed in context of a significant increase in cyber-crime. *See id.* For example, the convicted terrorist who masterminded the World Trade Center bombing in 1993 had encrypted files on his laptop containing plans to blow up U.S. airplanes around the world. *See id.* Also, Kerr pointed to a case where nineteen people were charged with insider trading when they entered Internet chat-rooms to recruit people to provide information on two major brokerage firms' customers. *See id.* Furthermore, since 1995, the FBI has investigated nearly 800 cases involving adults traveling interstate to meet children they met over the Internet for purposes of sexual relationships. *See id.* The FBI has also investigated more than 1,800 cases of people trading child pornography over the Internet. *See id.* In one particularly morally repulsive incident stemming from deceptive online communication, a teenage boy, after communicating with a man over the Internet, and eventually meeting him in person, was brutally forced to have sex, bound, blindfolded and forced to have an enema. *See also* Barbara Kantowiz et al., *Child Abuse in Cyberspace*, NEWSWEEK, Apr. 18, 1994, at 40.

vore actually enhances privacy on the Internet by increasing online consumer confidence.[14]

The right to privacy is deeply and inextricably woven into the fabric of the Fourth Amendment.[15] An individual who enjoys a reasonable expectation of privacy can be said to merit Fourth Amendment protection.[16] If law enforcement does not take proper measures to respond to cyber-crime, however, we may turn cyberspace into a haven for criminals and terrorists to communicate without fear of criminal or civil liability. As Dr. Donald M. Kerr, Assistant Director of the FBI, noted, "America's Internet users are legitimately concerned that surfing the Internet is like walking in a big city at night. The enjoyment is tempered by a fear of what's lurking unnoticed in the dark alleys."[17]

This Note argues that Carnivore does not violate the Fourth Amendment's protection against "unreasonable searches and seizures" since one does not enjoy a "reasonable expectation of privacy" as to their e-mail headers. The refined characteristics of the Carnivore search, the important overriding policy concerns of effective law enforcement and extant Fourth Amendment jurisprudence, compel a verdict of constitutionality for Carnivore. Part I of this Note presents an introduction of the Carnivore system, explaining its environment, its technical nature, and the controversy it has engendered. Further, Part I sets forth a hypothetical to help explain why the Carnivore system is necessary and why other alternative methods of searching e-mail are insufficient and legally inappropriate. Moreover, Part I contends that those who commit crime should not be shielded from accountability simply because they break the law in the anonymous confines of cyberspace. Part II of this Note offers a brief history of the Fourth Amendment, detailing its deepest origins and modern development. Part III explores the Electronic Communications Privacy Act ("ECPA"),[18] discussing its legislative history and its governance over the Carnivore system. Part IV claims that the Carnivore search should have no different Constitutional ramifications than that of a regular mail search. In addition, it argues that the precise, restricted elements

---

14 *See* Elisabeth Frater, *Law Enforcement: The Carnivore Question*, 32 NAT'L J. 2722, 2722 (2000). David Green, the Justice Department's principal attorney for computer crimes, contended that in some instances, for example, when the FBI investigates the hacker who has stolen someone's identification, that individual's privacy is actually enhanced. *See id.*

15 *See generally* Katz v. United States, 389 U.S. 347 (1967) (holding that a reasonable expectation of privacy exists under the Fourth Amendment when one makes telephone calls from a public pay phone).

16 *See id.*

17 *Senate Hearing, supra* note 13.

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

of the search and compelling public policy should render Carnivore a proper balance between privacy rights and law enforcement protection.

I. ELEMENTS OF THE CARNIVORE CONTROVERSY

A. *The Realm in Which Carnivore Exists*

To understand Carnivore, one must appreciate the realm in which it operates. Today, where over forty million Americans are using the Internet regularly[19] and where the rate of increase of Internet usage is nearly 55,000 users every day,[20] cyber-crime is a very serious problem. Credit card and telephone access codes are stolen.[21] Child pornography is accessible via the Internet,[22] as are copies of pirated music[23] and copies of programs that are designed for the purpose of breaking into other computers.[24] "Digital cash," or money passed through cyberspace, can be traded without leaving a trace, making cyber-crime increasingly difficult to track.[25] Hate mail, libel and copyright infringement continue unimpeded and largely unchecked.[26] Terrorists, drug traffickers and embezzlers do not exist in a technological vacuum. On the contrary, they have been able to benefit from advancing technology just like the rest of society.

B. *The Technical Aspects of Carnivore*

To understand the technical nature of Carnivore,[27] one must

---

19 *See Senate Hearing, supra* note 13.

20 *See id.*

21 *See* Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search,* 105 YALE L.J. 1093, 1097 (1996).

22 *See id.*

23 *See id.*

24 *See id.*

25 *See* Lawrence Lessig, *Reading the Constitution in Cyberspace,* 45 EMORY L.J. 869, 874 (1996); *see also* Randy Gainer, *Allocating the Risk of Loss for Bank Card Fraud on the Internet,* 15 J. MARSHALL J. COMPUTER & INFO. L. 39 (1996) (discussing the various risks in electronic transfers of funds over the Internet and examining who should bear the loss if online consumer information is misused).

26 *See* Krasovec, *supra* note 3, at 113 n.60.

27 This technical overview is very general and in simple terms. *See Independent Review, supra* note 10 (containing an extremely technical report, accompanied by diagrams, of Carnivore's software and precise collection mechanisms). For an example of how technical a true description of Carnivore software can be, consider the following:

> Carnivore software has four components: (1) a driver derived from sample C source code provided with WinDis 32, a product of Printing Communications Associates implements preliminary filtering of IP packets; (2) an application program interface (API); (3) a down line load (DLL) program written in C++ provides additional filtering and data management; and (4) an executable (EXE) program written in Visual Basic provides a graphical user interface.

Id. For a picture of both a basic and an advanced Carnivore screen, see *id.*

first recognize that information sent over the Internet travels in "packets."[28] When an e-mail user clicks the "send" icon on their e-mail software, that e-mail message is broken down into multiple packets and then sent.[29] Within each digital packet lies a section called the "TCP payload,"[30] where the information of the e-mail header is found, including the "To" and "From" address information.[31] Carnivore is installed in an ISP's server via a high-speed connection.[32] It sniffs the "To" and "From" e-mail address information embedded within the digital packets that are streaming past.[33] If a targeted suspect's address is detected, Carnivore will record either the e-mail address information or the entire informational packet depending on the particular search authorized.[34] Carnivore is thus a combination of computer hardware and software,[35] but on its face appears to be nothing more than a simple sealed, black box.[36] The system has so far been employed only between twenty-five and thirty times.[37]

C. *The Swirling Controversy*

Critics of Carnivore argue that, since ISPs have the independent ability to monitor a targeted suspect's e-mail and can do so upon the issuance of a court order, Carnivore is an unnecessary evil.[38] But, according to the FBI, the ISP does not always have the equipment or capability to meet the terms of a court order.[39] Further, the FBI maintains, since Carnivore keeps a detailed record of all its activities, it is actually a friend of privacy.[40]

---

[28] *See* James H. Johnston, *Beware of Carnivore's Voracious Appetite,* LEGAL TIMES, Sept. 4, 2000, at 29.

[29] *See id.*

[30] *See id.*

[31] *See id.*

[32] *See id.*

[33] *See id.*

[34] *See id.*

[35] *See* Yael Li-Ron, *Encrypt Your Way Past the Carnivore,* CONTRA COSTA TIMES, Sept. 3, 2000, *available at* 2000 WL 26267862 (outlining Carnivore's basic components: the hardware is a typical computer running "Windows NT," and the software is that which contains the special source code that gives Carnivore its packet-sniffing abilities).

[36] *See* Mathieson, *supra* note 12, at 10.

[37] *See Senate Hearing, supra* note 13.

[38] Before Carnivore's arrival, this is exactly what was accepted as the general practice. The FBI would obtain a search warrant and then order the ISP itself to perform the search. *See* Michael J. Himowitz, *FBI's Carnivore Program Has its Share of Skeptics,* AUGUSTA CHRON., Aug. 23, 2000, at B8.

[39] Dr. Kerr maintained that of the roughly 8,000 to 15,000 ISP servers in the country, some of them lack funds and equipment and therefore need Carnivore to search efficiently on their own. *See Senate Hearing, supra* note 13.

[40] *See id.* Dr. Kerr stated:

> We produce a record of all settings, and that becomes part of the evidentiary chain that we create. The system in fact is secured within the Internet Service

There may be a public misconception of Carnivore as a system that allows FBI agents to read portions or headers of any individual's e-mail in real time as it streams past the information superhighway. However, this fear is misguided. As Dr. Kerr stated in hearing testimony:

> There is no real-time review of text because in fact we're dealing with systems where the information is transiting at rates for instance of 40 megabytes a second. We have no one who can read zeros and ones at 40 megabytes a second and translate that into content.[41]

Critics of Carnivore present two major arguments against its constitutionality.[42] First, they argue that the system's search is too broad in that it may retrieve hundreds, if not thousands, of e-mail headers, unlike ordinary wiretaps that record only the relatively few conversations passing through a single telephone line.[43] The first argument can be labeled one of "minimization."[44] Second, unlike wiretaps that must be subjected to judicial supervision, no institution, except the FBI, audits the Carnivore system.[45] This second argument is quite simply, "limited judicial supervision."[46]

D. *The Need For Carnivore*

Carnivore is a necessary instrument because it performs a tremendous balancing act in a highly efficient manner.[47] The system simultaneously promotes the legitimate interests of law enforcement and adequately protects social privacy concerns.[48] Carnivore is needed to restrictively monitor headers of e-mail in cyberspace just as the exteriors of real envelopes are sometimes monitored by law enforcement at the post office.[49]

> Provider's spaces to provide physical chain of custody as well. And . . . we will provide the same authentication of the message information that we capture as well as the settings so that we will be able to testify later in court as to what the settings were, who set them up, and were any subsequent changes or alterations made.

Id. In addition, Carnivore does not even have a mouse, keyboard or any monitor that can view e-mail messages streaming past. In fact, the e-mails are encrypted in digital code as they flow through the Carnivore system at the ISP station. *See* Telephone Interview with Gregory Motta, Attorney, FBI (Feb. 22, 2001) [hereinafter Motta Interview].

41 *Senate Hearing, supra* note 13.

42 *See* Chiu Interview, *supra* note 9.

43 *See id.*

44 *See id.* Minimization is a short form of the argument that Carnivore's search is too broad and that it doesn't discriminate efficiently in what it gathers.

45 *See id.*

46 *Id.*

47 *See Independent Review, supra* note 10.

48 *See Senate Hearing, supra* note 13.

49 See *infra* Part IV for a complete discussion on this principle.

In addition, Carnivore has such precise control mechanisms imposed digitally, statutorily and judicially; there are no other systems available that can duplicate Carnivore's serious chore with comparable efficiency.[50] There are some commercially available products that can perform a similar function to Carnivore.[51] These products, however, are incapable of limiting interception as precisely as most courts require and rely on greater amounts of human intervention to minimize interception.[52] Privacy advocates argue that Carnivore is not a necessary tool because ISPs can already monitor an individual's e-mail and report back to the FBI.[53] But, to allow ISPs to monitor sensitive e-mails can pose grave risks of inappropriate disclosure.[54]

Online crime occurs with unsurpassable stealth and astounding speed. An equally powerful and sophisticated mechanism is needed to combat such an advanced level of criminal activity.[55] As a most basic principle, in the interests of protecting the citizens of this country, law enforcement must at the very least create enforcement tools that adequately match current technological standards.[56]

1. A Hypothetical Framework

To illustrate this point, consider the following hypothetical. In the distant future, a team of scientists fashion a specially crafted cloak that makes those who wear it entirely invisible. This cloak is inexpensive, easy to use, and owned by almost everyone. Most people who use this cloak have honest, good-minded reasons for employing it. Shy people wear it at crowded social functions, mothers watch children who think they are playing unobserved, and security guards don it to more effectively watch over their territories.

Like every wonderful invention that has preceded it, however, this cloak has the potential for harm. Criminals wear the cloak as well, committing crimes largely unimpeded and undetected. Robbing stores and banks is easy, rape victims cannot identify their attackers, and gang violence skyrockets in volume to an all-time high. Further, the only way to track the exact location of any criminal suspect who owns a cloak is to force the many existing invisible-

---

50 *See Independent Review, supra* note 10.

51 *See id.* (discussing "Etherpeek," a system that could not minimize interception as efficiently as Carnivore).

52 *See id.*

53 *See Senate Hearing, supra* note 13.

54 *See id.*

55 *See id.*

56 *See id.*

cloak manufacturing companies to employ their grossly inadequate tracking devices.

Law enforcement, then, to fulfill its sworn duties to protect this country, would have to construct a machine or device that could efficiently monitor those who own such cloaks and the location of criminal suspects employing one. If law enforcement agencies did not respond to the need for such a device, critics would assail their credibility, disparage their capabilities, and subject them to abuse in the press.

E-mail, once unimaginable, is today an incredibly efficient and popular way to instantaneously correspond. Almost anyone who owns a computer knows how to use it. E-mail is, for the most part, used for positive ends but, akin to our hypothetical cloak, can be abused by criminals. Further, like the cloak manufacturing companies in our hypothetical, many ISPs simply do not have the capability to track criminals who use e-mail to commit devastating crimes.[57] The FBI must keep pace with advancing technological norms or face the harsh and unacceptable reality that it cannot effectively stop crime. It has thus become incumbent on the FBI to create and employ Carnivore.

2. Accountability

Criminals who commit crimes in cyberspace are very often shielded from liability because of the anonymous nature of the Internet.[58] E-mail, more than any other cyberspace convention, is the primary conduit for cyber-crime.[59] For many, it is true, the whole beauty of the Internet is its wide freedom from governmental controls,[60] but allowing criminals to remain unaccountable for

---

[57] *See Senate Hearing, supra* note 13.

[58] *See* Noah Levine, Note, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526, 1527 (1996) (outlining that anonymous Internet users, besides committing much crime, can injure individuals or companies through false or defamatory messages, or through materials infringing a copyright). *But see* McIntyre v. Ohio Elections Comm'n., 514 U.S. 334, 342 (1995) (holding that "the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry").

[59] *See* Levine, *supra* note 58, at 1527.

> The technological convention which allows the every day user to [commit anonymous crimes] is known as the anonymous remailer. A remailer is a device which allows anyone with access to a computer and an electronic mail (e-mail) account to send messages, pictures, and computer programs either to other individuals with e-mail accounts or to Internet newsgroups without the recipients knowing the origin of the communication. The introduction of such technology is already creating problems for the legal system by making it impossible to identify a responsible party when assessing civil or criminal liability.

Id.

[60] *See id.* at 1537 n.55.

their crimes simply because they are committed in cyberspace under-cuts the legitimacy of our criminal justice system and undermines consumer confidence.[61] Quite simply, it is not a healthy state of affairs when surfing the Internet becomes like "walking in a big city at night."[62]

II. HISTORY OF THE FOURTH AMENDMENT

A. *Origins and Evolution*

The Fourth Amendment has its origins in the American colonists' struggle against "heavy-handed" British law enforcement methods.[63] Its deepest origins can be traced as far back to 1609 when the presumption that an Englishman's home belonged to the king in matters of public interest was reversed.[64] Prior to 1760, intrusion by government officials was the standard method of search and seizure in colonial America.[65] The New England colonies, especially Massachusetts, engaged in search and seizures for more purposes than most other colonies.[66] For example, in mid-seventeenth century New York, the Dutch permitted constables to execute warrantless searches of "all suspicious places for stolen goods and for persons suspected of such crimes as murder, theft, drunkenness, and vagrancy."[67] The idea that a specific warrant is

---

61 *See Senate Hearing, supra* note 13.

62 *Id.*

63 *See* Tracy Maclin, *The Complexity Of The Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 926 (citing JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION 19 (1966)).

64 *See id.* at 933 (citing Semayne's Case, 5 Co. Rep. 91a, 92a (K.B. 1604) (holding that "the liberty or privilege of a house doth not hold against the King")).

65 *See id.* at 939 (citing William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* 376-77 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with author)).

> Customs laws in most of the colonies exposed all suspicious houses to perpetual search. Beyond those laws, the topics of statutory search and seizure were many: the militia, the hunting of game, alcoholic consumption; the observance of the Sabbath, the quality of food and of manufactured products, bankruptcy, debt collection, trading with the French and Indians, the regulation of servants and slaves, and, occasionally, vagrancy and dissent. Promiscuous powers of search and seizure were common to the laws [of the colonies] on all these topics.

Id.

Maclin notes that Justice O'Connor declared Cuddihy's work to be the "one of the most exhaustive analyses of the original meaning of the Fourth Amendment ever undertaken." *Id.* at 928 n.14 (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 669 (1995) (O'Connor, J., dissenting)).

66 *See id.* at 939.

67 *Id.* (quoting Cuddihy, *supra* note 65, at 411).

> A Delaware vagrancy of 1739 permitted the arrest of "any suspicious person . . ." as a runaway if he lacked a pass or was unable to render "a good and satisfactory account" of himself. In the mid-1700s, New Jersey permitted general warrantless excise searches of private homes. Its sheriffs had authority "to break open any House, Chamber, Shop, Door, Chests, or Trunks" believed to conceal the

required to enter a person's private dwelling sprung out of Massachusetts' response to the Excise Act of 1754.[68] Such early warrant requirements would surely fail today's constitutional standards but nevertheless had safeguards that are reflected in the Fourth Amendment itself.[69] At the time of enactment of the Fourth Amendment, it is clear, the only way to seize an item was to search an individual's home and physically capture it. The notion that the Fourth Amendment was designed to protect against physical invasions would remain intact until the latter half of the twentieth century.

In the 1900s, the Supreme Court presented two major models outlining the scope of protection granted by the Fourth Amendment. The first was the "property-based model," which naturally stemmed from the historic origins of the Fourth Amendment and was illustrated by the Court in *Olmstead v. United States.*[70] In *Olmstead,* the Court held that federal agents did not violate the Fourth Amendment when they tapped the office and home phones of a suspected bootlegger.[71] The Court reasoned that, since the Fourth Amendment applied only to places and tangible items, it could not be triggered because the conversations recorded were not tangible.[72] Moreover, since the agents did not physically trespass the borders of the office or home, the Fourth Amendment did not protect Olmstead's rights.[73] Over thirty years later, in *Silverman v. United States,*[74] the Court unanimously held that the Fourth Amendment had been violated where a microphone was inserted into an

---

property of an absconding debtor. Constables were also required "to examine, search, and see what [poor] persons were entering" the state.

Id. at 940 (quoting Cuddihy, *supra* note 65, at 416).

68 *See id.* at 943.

This act allowed collectors of the tax "to interrogate any citizen under oath concerning his annual consumption of spirits." Merchants and residents resisted "vehemently protest[ing]" that the measure would allow "a petty Officer to come into a Gentleman's House, and with an Air of Authority, demand an Account upon Oath of the Liquor he has drank in his Family for the year past . . . ."

Id. (quoting Cuddihy, *supra* note 65, at 721-722).

69 *See id.* at 944. Among the requirements of the early warrants were: searches had to be carried out in daylight hours only, the warrants had to specify a particular place as the target of the search, and such a warrant had to be made under oath. *See id.* In short, an antiquated version of probable cause presented itself. *See id.* The law "required informants to swear that they possessed knowledge of lawbreaking at the targeted premises. Thus, the law required officers seeking warrants to search for military deserters to allege 'vehement' suspicion of the specific whereabouts of a deserter." *Id.*

70 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

71 *See id.* at 465.

72 *See id.* at 475-76.

73 *See id.* at 477-78.

74 365 U.S. 505 (1961).

individual's basement heating duct.[75] The Court reasoned that because the electronic device physically intruded into a protected area, the Fourth Amendment right attached.[76]

Under this property-based Fourth Amendment model, Carnivore would not violate the Fourth Amendment because the informational packets that it sniffs are collected, if at all, in transit. The informational packets are not in a person's home. This argument would be weakened, however, if, in a hypothetical instance, the e-mail was seized after it had reached a home destination. Moreover, cyberspace is not really a physical medium at all. Since Carnivore does all of its work from designated ISP stations, it could not be said to physically trespass into a suspect's home, and would not violate a property-based construction of the Fourth Amendment.

B. *The Fourth Amendment is Transformed: The* Katz *Model*

In the landmark Fourth Amendment case, *Katz v. United States*,[77] the Supreme Court dramatically altered Fourth Amendment jurisprudence, expressly overruling *Olmstead*.[78] In *Katz*, the defendant was convicted of transmitting wagering information over a public payphone from Los Angeles to Miami and Boston.[79] The prosecution presented evidence at trial that included conversations gathered from an electronic device FBI agents had attached to the outside of the telephone booth where the suspect had engaged in private conversations.[80] The majority stated:

> [T]he Fourth Amendment protects *people, not places.* What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[81]

As Justice Harlan mapped out in his now famous concurrence, the test for determining whether a person is entitled to Fourth Amendment protection is two-fold.[82] First, that person must have an actual (subjective) expectation of privacy, and second, that expectation must be one that society recognizes as reasonable.[83] The Fourth Amendment, by responding to technological advances of

---

75 *See id.* at 512.
76 *See id.*
77 389 U.S. 347 (1967).
78 *See id.* at 353.
79 *See id.* at 348.
80 *See id.*
81 *Id.* at 351-52 (emphasis added).
82 *See id.* at 360 (Harlan, J., concurring).
83 *See id.* at 361.

the past, has been forced to undergo a radical transformation. By becoming malleable in its response to new forms of communication, it appears the Fourth Amendment is committed to the bold task of keeping pace with rapidly advancing technology.

III. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

A. *Purpose and Scope*

Carnivore is governed by the Electronic Communications Privacy Act ("ECPA") of 1986,[84] an amendment to the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[85] Under the ECPA, anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" may be subjected to fines and imprisonment.[86] The ECPA was enacted to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[87] The main goal of the ECPA was to provide a fair balance between privacy expectations and the legitimate needs of law enforcement agencies.[88] When the ECPA was enacted, Congress was well aware of ongoing law enforcement intelligence activities, including those involving electronic surveillance, and

---

84 18 U.S.C. § 2510 (1994 & Supp. 1999).

85 *See Independent Review*, *supra* note 10. When Carnivore intercepts an actual e-mail message, it is governed by both the ECPA and the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1829 (1994). Yet when Carnivore intercepts only the headers of e-mails, it is governed by both the Federal Wiretap Act, 18 U.S.C. §§ 3121-3127 (1994), and the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1841-1846.

86 18 U.S.C. § 2511(1)(a); *see* Jackson Games v. U.S. Secret Serv., 816 F. Supp. 432, 441-42 (W.D.Tex. 1993) (holding that the Secret Service did not violate ECPA because they did not "intercept" communications they seized from a stored Bulletin Board system; rather, only a contemporaneous acquisition of a communication is prohibited). *But see* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001) (holding that defendant airline company did not violate the Stored Communications Act, 18 U.S.C. §§ 2701-2710 (1994 & Supp. 1999), which amends the ECPA, when the airline accessed plaintiff's secure web site under false pretenses, disclosed sensitive information and subsequently threatened to counter-sue plaintiff for defamation).

87 S. REP. NO. 99-541, at 3556 (1986) [hereinafter *Senate Report*]. When Senator Leahy, who is affectionately known to some as the pre-eminent "Cyber-Senator" of our time, introduced the amendment, he stated that the existing law was "hopelessly out of date." *Id.*; *see also* Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995) (explaining that the main purpose of the Electronic Communications Privacy Act was to extend to electronic communications the same protections against unauthorized interceptions that was until then only available for wiretaps).

88 *See Senate Report*, *supra* note 87, at 3559; *see also* Lam Lek Chong v. U.S. Drug Enforcement Admin., 929 F.2d 729 (D.C. Cir. 1991); United States v. Clemente, 482 F. Supp. 102, (S.D.N.Y. 1979), *aff'd*, 633 F.2d 207 (2d Cir. 1980) (stating that the protection of privacy was an overriding congressional purpose in enacting this statute, and that this statute was an attempt by Congress to establish a system of electronic surveillance subject to strict safeguards).

expected such practices to continue.[89]

One of the many changes made from the 1968 Act to the ECPA was the state of mind requirement[90] necessary to prove that the law was violated.[91] The level of intent in the 1968 Act changed from "willful" to "intentional," and this amendment was made largely to "underscore that the inadvertent reception of a protected communication is not a crime."[92] Currently, under the ECPA, a strict level of intent is necessary in order to violate the statute by a wrongful interception.[93] This level of intent requires that the interception of an electronic communication is an individual's "conscious objective."[94] Put simply, to violate the ECPA, one must intercept "on purpose."[95] To violate the ECPA, the FBI must purposely intend to capture e-mail headers not named in their search warrant.[96] The reality is that any additional headers sniffed and searched by Carnivore are headers gathered inadvertently, if at all.[97]

As the ECPA's legislative history suggests,[98] a major purpose in enacting the statute was to encourage people to use technology and businesses to develop "new innovative forms of telecommunications and computer technology."[99] This legislative purpose is consistent with the implementation of a device that not only protects the cyber-world from crime, but also stabilizes online consumer confidence. Not many individuals would purchase an

---

89 *See Senate Report, supra* note 87, at 3572 ("The minimization of information collected concerning U.S. persons will be continued.").

90 State of mind is an area that permeates criminal law. The notion that different measures of punishment apply for different levels of intent is a principle that is as ever-present and widespread as the various state and federal criminal statutes themselves.

91 *See Senate Report, supra* note 87, at 3560.

92 *Id.* In changing § 101(f) of the ECPA, Congress was careful to emphasize that the word "intentional" as meant in the statute did not have precisely the same meaning as its dictionary definition. *See id.* The word "intentional" as used in the ECPA means "more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." *Id.* Importantly, when enacting the change, Congress recognized that radio scanners that could inadvertently receive a protected communication, such as a cell-phone call. *See id.* at 3578. Even though Carnivore is a completely different medium than radio interception, the change still signified an understanding by Congress that with new technology there are always greater powers of inadvertent interception.

93 *See id.* at 3577.

94 *Id.*

95 *Id.* (stating that "[a] common means to describe conduct as intentional, or to say that one causes the result intentionally, is to state that it is done or accomplished 'on purpose'").

96 *But see id.* at 3578 ("The term intentional is not meant to connote the existence of motive. Liability for intentionally engaging in prohibited conduct is not dependent on an assessment of the merit of the motive that led the person to disregard the law.").

97 *See* Motta Interview, *supra* note 40.

98 *Senate Report, supra* note 87, at 3577.

99 *Id.* at 3559.

expensive item over the Internet if they knew that law enforcement was legally powerless in cyberspace. Congress thought that the lack of clear legal standards could endanger the admissibility of evidence and possibly expose law enforcement to liability,[100] and Carnivore is a strong demonstration of this Congressional fear.

B. *Statutory Safeguards*

Before Carnivore can be used to intercept wire or electronic communications, the FBI must obtain approval for the Title III application from the Department of Justice.[101] The Office of Enforcement Operations in the Criminal Division of the Justice Department then examines each application to make sure that the proposed interception satisfies Fourth Amendment requirements and is in compliance with all governing statutes and regulations.[102] If a proposal gains approval from the Office of Enforcement Operations, a deputy assistant attorney general in the Criminal Division must then approve the interception.[103] Generally, the interception may not last longer than thirty days without a court-granted exception.[104] For additional recourse to a potential Fourth Amendment violation, one may bring a civil suit or, in a criminal defense, move to suppress any evidence under the exclusionary rule.[105]

Congress further exercises a measure of control over the implementation of Carnivore by imposing certain reporting requirements.[106] Under 18 U.S.C. §2519, the supervising judge of the Title III wiretap has to report to the Administrative Office of the United States the fact of interception and whether the request was granted or denied.[107] Additionally, the Attorney General must also report the same information, independently, to the Administrative Office.[108]

---

100 *See id.*
101 *See Senate Hearing, supra* note 13.
102 *See id.*
103 *See id.*
104 *See id.*
105 The exclusionary rule is a court-fashioned rule that simply bars the admission into trial of any evidence gained as a result of a constitutional violation. *See* United States v. Calandra, 414 U.S. 338, 348 (1974). However, in certain limited circumstances, for example, when the prosecution seeks to merely impeach a witness, some evidence gained unconstitutionally may be admitted into trial. *See generally* Harris v. N.Y., 401 U.S. 222 (1971).
106 *See Independent Review, supra* note 10.
107 *See id.*
108 *See id.*

IV. THE CONSTITUTIONALITY OF THE CARNIVORE SEARCH

A. *Why the Analogy to Regular Mail is Appropriate*

E-mail, like regular mail, encourages its users to develop the fine art of writing by transforming thoughts into print.[109] Both e-mail and regular mail have private mailboxes controlled by the recipient of the incoming mail.[110] Both forms of mail generally involve at least some time of delay between the reception of the message and any response.[111] Just as pen pals may communicate with someone they have never met, e-mail users often start correspondence with those whom they do not know.[112] Both forms of mail are relatively cheap and allow the recipient to know "either who a communication is from, or at least where it originated, before reading it."[113] These two forms of mail are both subject to similar problems as well. For example, mass junk-mailings proliferate in the real world, just as they do online.[114] As noted by one author, the only real distinctions that exist between e-mail and regular mail are the different speeds and costs of transmission.[115] As the same writer is quick to point out however, such small distinctions are "hardly a sound basis for making such a significant legal distinction."[116]

B. *Mail Covers*

Sometimes, it is necessary for law enforcement officials to monitor a suspect's mail as it passes through the post office.[117]

---

109 *See* Megan Connor Bertron, *Home is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 182 (1996).

110 *See id.*

111 *See id.* at 183.

112 *See id.* (citing *Lawyers Say E-Mail Sex Not Adultery*, L.A. TIMES, Feb. 8, 1996, at A19 (reporting a divorce case where a wife sent sexually explicit e-mail to an Internet pen pal whom she had never met in person)); Nancy Schaadt, *Women Link Up on Internet for Computer Klatch*, DALLAS MORN. NEWS, Dec. 27, 1995, at 5C (reporting the formation of various online support groups for women).

113 Bertron, *supra* note 109, at 183.

114 *See id.* at 184.

115 *See id.*

116 *Id.*

117 This search, known as a "mail cover," is by no means a new tactic employed by law enforcement agents in their fight to protect the United States from criminal activity. In fact, postal regulations first authorized the use of mail covers in 1879. *See* Von Cotzhausen v. Nazro, 107 U.S. 215 (1882) (commencing a suit against two defendant customs inspectors who had seized a woolen scarf in the mail that had arrived from Germany to Milwaukee). The *Von Cotzhausen* court relied on an 1874 statute, which stated in part, "there shall not be admitted for conveyance by the post any letter or *other packet* which may contain either gold or silver money, jewels, precious articles, or any article whatever liable to customs duties." *Id.* at 217. Interestingly, the statute chose to emphasize that suspicious contraband could arrive in a form other than a letter. The statute seemed to imply that other packages, in whatever form they come, can be inspected from the outside and seized if

When law enforcement agents instruct a postal agency to record the information on the outside of an envelope, the process is commonly referred to as a "mail cover."[118] This unobtrusive search is generally not considered a search under the Fourth Amendment.[119] In *Vreeken v. Davis*,[120] for example, plaintiffs sought relief from the IRS and a post office superintendent for injuries allegedly arising from placement of a mail cover on plaintiff's mail in a tax fraud case.[121] Relying on *Smith v. Maryland*,[122] the court reasoned that the mail cover was not a Fourth Amendment search because an individual "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[123] The court reasoned that it could find nothing conceptually different between a mail cover and a pen register,[124] for Fourth Amendment purposes.[125] The Court further stated that "[t]he persons who sent or received mail knew or ought to have known that postal employees must examine the outside of the mail in order to deliver it. Furthermore, even if the plaintiffs did harbor a subjective expectation of privacy, that expectation was unreasonable."[126]

In *United States v. Choate*,[127] where a special agent instructed the post office to monitor the mail of a suspected drug smuggler and tax evader for thirty days, the Ninth Circuit unequivocally struck down the district court's ruling that the mail-cover violated defendant's Fourth Amendment rights.[128] The court noted that in "all post-*Katz* decisions except this, the courts have again sustained mail covers on the ground that there is no reasonable expectation that such information will remain unobserved."[129] Further, the

---

necessary. *See id.* There are many modern cases permitting the use of a mail cover as well. *See* Vreeken v. Davis, 718 F.2d 343 (10th Cir. 1983).

118 *See Vreeken*, 718 F.2d at 345 n.1.

119 *See id.* at 348.

120 718 F.2d 343.

121 *See id.* at 344-45.

122 442 U.S. 735 (1978). The *Smith* case, discussed in detail later in this Note, is a major building block in Fourth Amendment jurisprudence, establishing that people do not have a reasonable expectation of privacy with regard to numbers dialed on their telephones. *See id.*

123 *Vreeken*, 718 F.2d at 347; *see also* Canady v. United States, 354 F.2d 849, 857 (8th Cir. 1966) (stating explicitly that mail cover in question "did not violate any of defendant's constitutional rights"); United States v. Costello, 255 F.2d 876 (2d Cir. 1958) (emphasizing that since the mail in question was neither removed from the post office premises nor unreasonably delayed in its delivery as a result of the search, the seizure did not violate the controlling statutory provisions).

124 For a definition of a pen register, see *Senate Report*, *supra* note 87, at 3564. *See also infra* Part IV.C.

125 *See Vreeken*, 718 F.2d at 347-48.

126 *Id.* at 348.

127 576 F.2d 165 (9th Cir. 1978).

128 *See id.*

129 *Id.* at 175.

Choate court stated that the Fourth Amendment did not "prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, *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.*"[130]

ISPs thus find themselves in a situation analogous to postal employees and inspectors in that the administrators of the various ISPs have access to all e-mail streaming through their provider systems and are forced by the Carnivore attachment to "sniff" the e-mails. The suspect who claims, therefore, that he has a "reasonable expectation" of privacy to the headers and addresses of his e-mail actually is incorrect under the language of *Vreeken* and *Choate.* The e-mail sender, like the regular-mail sender, *voluntarily* places his confidence in a third party, namely, the ISP. The *Choate* court also pointed out that since "an established federal agency was requesting the mail cover," the claim of "unreasonable search and seizure" was additionally weakened.[131] It is undisputed that the FBI is considered one of the most established federal agencies in the country.

The defense in *Choate* argued that since mail covers have the potential for abuse, they should be declared unconstitutional.[132] But this argument is grounded more on apprehension than logical or legal reasoning. The court recognized this potential for abuse and stated, "When such a case occurs, the Fourth Amendment may be implicated, but . . . there was no such abuse here."[133] Libertarians argue that since the system has the potential to be abused, Carnivore runs counter to the purpose of the Fourth Amendment.[134] It is certainly true that Carnivore has the potential to be abused but, as *Choate* demonstrates, a mere potential alone cannot render the system unconstitutional.

1. Search of Sealed Mail and the "Border Exception"

As a general rule, letters and sealed packages sent in the mail can be opened and examined only under the authority of a valid search warrant.[135] This principle was first embodied in the seminal

---

130 *Id.* (emphasis retained).
131 *See id.* at 178.
132 *See id.* at 177.
133 *Id.*
134 *See* Chiu Interview, *supra* note 9.
135 *See* 1 CHARLES E. TORCIA, WHARTON'S CRIMINAL PROCEDURE § 151, at 574. A valid search warrant in general must:

> (1) usually be in writing and signed, setting forth *facts, not conclusions,* (2) describing the place to be searched and the things to be seized; (3) contain a

case of *Ex parte Jackson*,[136] in the late nineteenth century and has endured until the present day. The exceptions to this rule are mainly the inspection of suspicious packages by customs border officials.[137] For example, in *United States v. Ramsey*,[138] a New York customs officer was inspecting a sack of incoming mail from Thailand and, suspecting that eight bulky envelopes contained contraband, he opened them and found heroin.[139] The Supreme Court ruled that opening the envelopes without a warrant constituted a valid search because it fell under the "border search" exception, which allows customs officials much discretion in deciding whether to search a person or package.[140] The border search exception is a

---

> statement in the affidavit of *recent* facts sufficient to show *probable cause* to believe that the search will reveal the item(s) sought; (4) the affidavit must not have any statement which is either false or reckless; and (5) the affidavit must be submitted to a neutral, detached magistrate.

Id. § 152 at 579.

In the specific context of Carnivore, however, the wiretap warrant must contain the following:

> (1) the identity of the interceptee, if known; (2) the nature and location of the communications facilities to which the authority to intercept is granted; (3) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (4) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and (5) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall be automatically terminated when the described communication is first obtained.

Independent Review, supra note 10.

136 96 U.S. 727 (1878).

137 *See* United States v. Mayomi, 873 F.2d 1049 (7th Cir. 1989) (holding that FBI agent's detention of three letters addressed to defendant at his private mailbox service did not violate defendant's Fourth Amendment rights when the agent had a reasonable suspicion that such envelopes contained heroin); United States v. Aldaz, 921 F.2d 227 (9th Cir. 1990) (detailing that a seizure of express delivery packages did not violate defendant's Fourth Amendment rights where available information led the inspector to have a reasonable suspicion that defendant was involved in criminal activity); United States v. Various Articles of Obscene Merchandise, 395 F. Supp. 791 (S.D.N.Y. 1975) (holding that customs officer had reasonable cause to suspect an air mail envelope from England contained obscene material); United States v. Swede, 326 F. Supp 533 (S.D.N.Y. 1971) (holding that an envelope mailed to defendant from Switzerland and containing LSD but no letter was subject to a lawful search when it aroused suspicion in customs border officials). *But see* State v. Kelly, 708 P.2d 820 (Haw. 1985) (dealing with the following circumstances: a narcotics officer, without a warrant, seized a photograph album from international mail after a drug-sniffing dog indicated the album may have contained drugs. The officer then installed an electronic beeper to the package, which the court held constituted an unreasonable search and seizure); United States v. Dass, 849 F.2d 414 (9th Cir. 1988) (holding that where government agents, without a search warrant, detain packages for up to three weeks, even if there is indication such packages may contain marijuana, such an action constitutes an unreasonable seizure in violation of the Fourth Amendment).

138 431 U.S. 606 (1977).

139 *See id.* at 607.

140 *See id.* at 619 (stating "[t]here has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause . . . are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself"). This is an impor-

major, perhaps even radical, departure from Fourth Amendment principles. The Supreme Court has thus been willing to forego Fourth Amendment protection in light of overwhelming policy concerns.[141]

The outer expanses of the vast, formless world of cyberspace may not be analogous to this country's physical borders, but the public policy of protecting this country's citizens from cyber-terrorists, drug smugglers and embezzlers is no different than it is in real, physical dimensions.[142] It is unreasonable to paralyze law enforcement officials in the potentially terrifying world of cyberspace just as it would be to stop them from patrolling our country's physical borders.[143]

2. "Reasonableness" of Privacy in E-Mail

There have been a few recent employment cases suggesting that e-mail senders do not enjoy a reasonable expectation of privacy. In *Bourke v. Nissan Motor Corp.*,[144] an employer retrieved and printed e-mails that employees wrote from work.[145] Plaintiff employees sued Nissan for common law invasion of privacy, intrusion of their constitutional right to privacy, and violation of the criminal

---

tant function for national protection. There have been Fourth Amendment concerns raised not only with mail but with searches of vehicles, baggage and persons at the border as well. These searches are usually upheld. *See* Almeida-Sanchez v. United States, 413 U.S. 266 (1973). When a search requires a suspect to undress, and when his or her most private cavities are probed, government officials must present a stronger showing that the suspect is concealing contraband.

However, that is not always the rule. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 544 (1985) (Marshall, J., concurring) (outlining a shocking scenario where customs agents suspected a woman of being a "balloon-swallower," or someone who smuggles drugs by concealing them in her alimentary canal. The woman had made many quick short trips into the United States, always carried cash, and her flight originated from a primary source for narcotics. But these facts still did not amount to probable cause. The humiliating search and seizure, which lasted a total of twenty-seven hours and in which she was forced to choose between being X-rayed or being detained until she produced a bowel movement, was deemed reasonable in part because the detention occurred at the international border, "where the Fourth Amendment balance of interests leans heavily to the government").

Another wrinkle to the border search is the "fixed-checkpoint" exception. The Supreme Court has held that where a fixed checkpoint is set up in the *interior* of the country, all cars that pass it may be stopped. *See* United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (holding that authorities did not have to obtain a warrant before setting up the checkpoint and that officials were allowed to direct particular motorists to a side inspection area where they can be interrogated and, if necessary, have their cars searched).

141 *See Martinez-Fuerte*, 428 U.S. at 562.

142 *See* John Schwartz, *Fighting Crime Online: Who is in Harm's Way?*, N.Y. TIMES, Feb. 8, 2001, at G1. Marcus C. Thomas, the head of the FBI's cyber-technology section declared, "What would you have us do? . . . Stop enforcing laws because it's on the Internet?" *Id.* at G8.

143 *See id.*

144 No. B068705 (Cal. Ct. App. July 26, 1993).

145 *See id.* at 1.

wiretapping and eavesdropping statutes.[146] The court held that the employees had no reasonable expectation of privacy in their e-mail messages because they had signed a company form declaring they would restrict their e-mail usage to company purposes only.[147] Further, they were advised that their e-mails could be read by others on occasion.[148] The court also posited that even though the employees had individual passwords they were told to keep secret, reading their e-mail still did not violate the employees' right to privacy.[149]

In *Smyth* v. *Pillsbury Co.*,[150] plaintiff employee claimed he was wrongfully discharged for sending inappropriate comments over the defendant company's e-mail system.[151] The company repeatedly assured its employees, including plaintiff, that e-mail communications could not be intercepted and used against employees of the company as grounds for termination or reprimand.[152] The Pennsylvania court held that plaintiff did not state a claim upon which relief could be granted because an employee does not have a reasonable expectation of privacy in e-mail communications made over a company's e-mail system.[153] The court further decided that, even if the employee could be said to have a reasonable expectation of privacy, the company's interest in preventing such unprofessional comments outweighed any privacy interest that an employee may have.[154]

---

146 *See id.*

147 *See id.* at 4.

148 *See id.*

149 *See id.*

150 914 F. Supp. 97 (E.D.Pa. 1996).

151 *See id.* at 98-99.

152 *See id.* at 100.

153 *Id.* at 101. The *Smyth* court, however, did not rely on the constitutionally implied expectation of privacy. Rather, the *Smyth* court interpreted the facts of the case under common law invasion of privacy, which is a tort. *See id.* at 100; RESTATEMENT (SECOND) OF TORTS § 6652(b) (1992) (stating that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person").

The *Smyth* court ultimately held that the defendant's interception did not rise to a "highly offensive" intrusion. *See Smyth*, 914 F. Supp. at 100. The common law tort of invasion of privacy is a doctrine that provides relatively little protection against private sector use of personal information. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2388 (1996) (claiming that "[t]he tort of invasion of privacy is probably best described as alive, but on life support"); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 221-26 (1991) (outlining four categories of privacy rights in the context of data processing); George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 531-41 (1990) (analyzing various issues of privacy in the private sector).

154 *See Smyth*, 914 F. Supp. at 101.

Libertarians seeking to establish Carnivore's unconstitutionality may point to *United States v. Maxwell*.[155] In *Maxwell*, FBI agents received several e-mails and graphic files depicting child pornography from a concerned citizen, the screen names of users who had sent the messages and material, and the screen name of the defendant.[156] Upon receiving this information, an FBI agent sought a search warrant that would permit him to discover the true identities of the users by obtaining a master list of users and screen names from the ISP.[157] The agent subsequently discovered that the defendant was a member of the Air Force, whereupon the Air Force Office of Special Investigations, with a search warrant, searched the defendant's computer files.[158] The court ruled that e-mail was similar to first-class mail in that "if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause."[159] Additionally, the court found that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission."[160] The *Maxwell* court further noted that the fact that an unauthorized hacker might intercept the e-mail message does not diminish the legitimate expectation of privacy in any way.[161]

The constitutionality of Carnivore, however, does not present a problem under *Maxwell* simply because the searches with which *Maxwell* dealt concerned the *actual content* of e-mail, and not that of e-mail headers. The reasonable expectation of privacy notions that the *Maxwell* court discussed are thus not directly applicable to Carnivore's constitutionality since Carnivore generally does not scan content. Further, by recognizing the strong conceptual similarities between e-mail and regular mail, the court implicitly adopted the notion that there are various exceptions to the e-mail and regular mail search, namely, mail-covers that do not require a warrant.

C. *The Pen Register and Trap-and-Trace Device*

A pen register is a mechanical device that records the num-

---

155 45 M.J. 406 (C.A.A.F. 1996).
156 *See id.* at 417-18.
157 *See id.* at 413.
158 *See id.* at 414.
159 *Id.* at 417.
160 *Id.* at 418.
161 *See id.* The court also noted that messages sent to the public at large, for example, in a "chat room" or an e-mail that is forwarded to many individuals loses, any semblance of privacy. *See id.* at 417.

bers dialed on a telephone but does not monitor the actual phone conversation itself.[162] It has been held that the use of a pen register or a trap-and-trace device[163] does not constitute a search under the Fourth Amendment.[164] A pen register does not fall under the auspices of Title III either.[165] Rather, pen registers are governed by their own statute,[166] and, while they still require a court order to administer, the restrictions are less strict than for wiretaps.[167] The standard for allowing a pen register is "mere relevance,"[168] that is, any court of competent jurisdiction must issue a pen register order if the applicant has demonstrated to the court that the information likely to be gathered is "relevant to an ongoing criminal investigation."[169]

The constitutionality of pen registers is clear. In the landmark case of *Smith v. Maryland,*[170] a woman reported a robbery to police and then subsequently received threatening phone calls from a person who identified himself as the robber.[171] Police found an automobile similar to the one that the robber had been driving and ultimately traced car ownership to Smith.[172] Without obtaining a warrant, police placed a pen register on Smith's telephone line to establish that it was his phone that was used to make the threatening telephone calls.[173] In a 5-3 decision, the Supreme Court affirmed his conviction, ruling that there is no expectation of privacy with respect to telephone numbers dialed from a telephone.[174] The Fourth Amendment, held the Court, does not even require the police to obtain a warrant before using the register

---

162 *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979).

163 *See Senate Report, supra* note 90, at 3564. Trap and trace devices are defined by Congress as devices that "[r]ecord the numbers of telephones from which calls have been placed to a particular telephone." *Id.* Congress defines pen registers as devices that "[r]ecord the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones." *Id.*

164 *See Smith,* 442 U.S. at 745.

165 Since Title III of the Omnibus Crime Control and Safe Streets Act of 1968 is concerned only with orders authorizing or approving the "interception" of a wire or oral communication, pen registers are not governed by that statute. *See* 18 U.S.C. §§ 2510-2520 (1994 & Supp. 1999). Pen registers do not really intercept under the meaning of the statute because they do not record the contents of communications. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977). Additionally, the legislative history of Title III indicates that the definition of "intercept" was meant to exclude pen registers. *See id.*

166 *See* 18 U.S.C §§ 3121 et seq. (1994).

167 *See Independent Review, supra* note 10.

168 Motta Interview, *supra* note 40.

169 *Independent Review, supra* note 10.

170 442 U.S. 735 (1979).

171 *See id.* at 737.

172 *See id.*

173 *See id.*

174 *See id.* at 745.

device.[175]

A contentious issue is whether a Carnivore search of only e-mail headers is analogous to a pen register search. The ACLU and other libertarian organizations argue that Carnivore does not fit neatly into an analytical comparison with the pen register:

> In a typical day, we may talk to 20 or 30 people on the telephone, but we can send a single e-mail to hundreds or even thousands of people with a single click of a mouse. A pen register might produce a list of a few dozen of someone's friends, but a Carnivore search could possibly implicate thousands of someone's e-mail contacts.[176]

There are a few problems with such an assertion. First, as the language in *Maxwell* provided:

> Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient . . . . [E]-mail that is "forwarded" from correspondent to correspondent lose[s] any semblance of privacy. Once these transmissions are sent out to more and more subscribers, the subsequent expectation of privacy incrementally diminishes.[177]

Applying that principle, if there were thousands of e-mail contacts potentially implicated by a Carnivore search, such contacts would not likely be able to claim a reasonable expectation of privacy under the language of *Maxwell.*

Second, it is important to recognize that Carnivore does not always sniff the e-mail of a massive group of e-mail senders.[178] In fact, in some limited circumstances, "Carnivore is actually able to isolate the interception to the individual target sender, just as an individual wiretap might."[179] The range of interception depends in large part on topography and the traffic flowing through the individual ISP.[180] "Carnivore works to target the smallest possible segment of the ISP network carrying the court-ordered traffic."[181]

Further, the header of an e-mail can be analogized to the outside of an envelope where an individual lacks any expectation

---

175 *See id.* at 745-46.

176 Chiu Interview, *supra* note 9.

177 45 M.J. 406, 418-19 (C.A.A.F. 1996).

178 *See* Motta Interview, *supra* note 40.

179 *Id.* (Mr. Motta declined to discuss how often or in what circumstances Carnivore has been able to perform such precise minimization, as such information is confidential).

180 *See id.* Topography refers to the location from where the e-mail travels. *See id.* For example, if an e-mail arrives in a small town with a population of 1,000 people, it will not be hard for the local ISP to intercept only the headers or messages of that individual. *See id.*

181 *Id.*

of privacy.[182] Libertarians proffer that e-mail headers are different from covers of regular mail, because headers often contain more than just the sender's name. For example, they may contain a phrase, a question or even an answer.[183]

However, it is necessary to realize that e-mail senders themselves recognize that there is no expectation of privacy as to their e-mail headers. This is precisely why senders often leave the header section blank or phrase the header ambiguously.[184] When senders *do* add a header to their e-mail messages, it is often written for the same reason as the writing on an advertisement arriving in regular mail: to entice the reader to open it.[185] E-mail headers, for the most part, are written for the same purposes as regular mail envelopes—to identify the sender. Mail covers, as demonstrated by the *Vreeken*[186] court, are, for Fourth Amendment purposes, conceptually no different than pen registers.[187] It follows, then, that Carnivore, in sniffing e-mail headers, fits within a pen register analysis and does not run afoul of the Fourth Amendment.

D. *Refined Nature of the Search*

Libertarians argue that the scope of Carnivore's search lacks proper minimization, and therefore it is an "unreasonable search."[188] They are concerned with Carnivore inadvertently searching or seizing e-mail headers not listed in the search warrant.[189] But Carnivore has minimization filters that allow it to minimize the scope even more efficiently than a regular court wiretap.[190]

In a court-administered wiretap, minimization takes place when a human listener exercises good judgment by turning off surveillance equipment when a suspect discusses matters not central to the investigation.[191] With Carnivore's computerized filters, minimization of interception occurs automatically.[192] Additionally, Carnivore also engages in "second-stage minimization"[193] that takes

---

182 *See id.*

183 For instance, an e-mail header might read as follows: "Are you bringing the goods?" or "Tonight's meeting." These are very different from envelopes passing through the regular mail which generally have only the sender's and recipient's address information.

184 *See id.*

185 *See id.*

186 Vreeken v. Davis, 718 F.2d 343 (10th Cir. 1983).

187 *See id.* at 347-48.

188 *See* Chiu Interview, *supra* note 9.

189 *See id.*

190 *See Independent Review, supra* note 10.

191 *See id.*

192 *See id.*

193 *Id.*

place when a "minimization agent" sifts through the intercepted e-mails and seals them in a special minimization file.[194] Only then, after the two separate minimizing procedures, are the files submitted to a judge.[195]

Another important distinction between Carnivore and regular wiretaps is that federal agents themselves are monitoring wiretaps. Conversely, Carnivore interceptions are performed by technicians "who could care less about intercepting specific targeted e-mails."[196] As an additional safeguard, the judge supervising the investigation must notify any party whose e-mail has been intercepted by Carnivore.[197]

Even if Carnivore inadvertently gathers people's e-mail headers, this fact would still not necessarily be a constitutionally fatal characteristic of the system. In *Wesley College v. Pitts,*[198] a former college employee inadvertently spotted an e-mail on another person's computer screen and then reported its contents to faculty members at the college.[199] The court held that when faculty members ultimately disclosed the information, they did not violate the ECPA because an unlawful interception does not result from an inadvertent glimpse.[200]

Carnivore, in its first minimization stage, may sometimes capture more information than it needs. But this is entirely analogous to regular telephone communications.[201] The only difference is that minimization on telephone wiretaps is usually done on a smaller scale.[202] For example, in *United States v. Quintana,*[203] a Cali-

---

194 *See* Motta Interview, *supra* note 40. This minimization agent, before sealing the special minimization file, first discards any irrelevant subject matter seized, for example, communications such as love letters that do not figure into the ongoing investigation. *See id.*

195 *See id.*

196 *Id.*

197 *See Independent Review, supra* note 10.

198 974 F. Supp. 375 (D. Del. 1997), *aff'd,* 172 F.3d 861 (3d Cir. 1998).

199 *See id.* at 378-79.

200 *See id.* at 384.

201 In recognizing this fact, some courts minimize the scope of the listen with precise directives. For example, officers listening in on conversations have been instructed to listen to the first two minutes of the conversation and, if no incriminating discussion takes place, to listen in only for fiftenn seconds of every minute thereafter. *See* United States v. McKinnon 721 F.2d 19, 24 n.3 (1st Cir. 1983).

202 *See* Motta Interview, *supra* note 40.

203 508 F.2d 867 (7th Cir. 1975). Anti-Carnivore advocates may argue that most of the unnecessary information gathered in a wiretap is not outside of the scope of the court-issued warrant because the search is only run over one phone line. Carnivore, they contest, can inadvertently gather vital information in the headers of thousands of e-mails, thus creating an overwhelmingly broad dragnet that catches more than necessary. *See* Chiu Interview, *supra* note 9. But, preceding ECPA's enactment, Congress discussed the scope of wiretap searches and maintained that when wiretap searches cover a few different phone lines, the search would likely be invalid under the statute. *See Senate Report, supra* note 87, at 3586. However, when law enforcement could show that a suspect was changing locations,

fornia court held that where only 153 of the 2,000 telephone calls intercepted were germane enough to transcribe, the additional interceptions nevertheless did not exceed statutory limitations.[204] The same leeway that extends to telephones should apply to Carnivore.

CONCLUSION

We live in an age of amazing technological development. Today, laser beams can pick up sound waves off of closed windows.[205] "Parabolic microphones" can eavesdrop on a conversation taking place at an outdoor restaurant hundreds of feet away.[206] A special gun can shoot a small dart with a wireless radio microphone into a distant windowpane.[207] Carnivore is no less an inevitable development than the Internet itself.

Carnivore likely will push many to use encryption over the Internet. Criminals will be able to send incriminating messages to each other, evading Carnivore with good encryption software.[208] Nevertheless, Carnivore is, and likely will remain the subject of heated debate until Congress directly recognizes its constitutional validity. The technological advances brought by the digital age demand law enforcement to keep pace with emerging developments to protect our country. Carnivore does not defy or undermine the values of the Fourth Amendment because Fourth Amendment jurisprudence allows for similar governmental searches of mail especially where compelling policy pervades.[209] Further still, limited

---

i.e., a terrorist moving from phone to phone to evade interception, a search of all those phones would be upheld. *See id.* Since e-mail messages are broken up into small packets and then sent, the situation is analogous to a suspect who cannot be precisely pinpointed in a warrant because he is floating or moving around. E-mail messages can arguably be said to behave in analogous fashion to a roving suspect, thus requiring more "leeway" in particularity requirements.

204 *See Quintana*, 508 F.2d at 882.

205 *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.2(e) (3d ed. 1996).

206 *See id.*

207 *See id.*

208 *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV., 503, 503 (2001) (citing LARS KLANDER, HACKER PROOF: THE ULTIMATE GUIDE TO NETWORK SECURITY 121-24 (Delmar Publishers 1999)); *see also* Ryan Alan Murr, Comment, *Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and Their Successors*, 34 SAN DIEGO L. REV. 1401, 1407 (1997) (discussing how using a 128-bit key would require the use of all two-hundred million computer users estimated to exist and would also take one million times the age of the universe to exhaust every possible key combination); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 830-33 (1995) (indicating that private users of encryption software are likely to be constitutionally protected from warrantless governmental intrusion).

209 *See, e.g.*, Ex parte Jackson, 96 U.S. 727 (1878); United States v. Ramsey, 431 U.S. 606 (1977).

law enforcement mail searches are nothing new, and Carnivore, in a sense, is merely "old wine in new bottles."[210] While bold technological advances sometimes appear to threaten our conceptions of privacy,[211] they should not be shunned without careful, thoughtful analysis.

*Aaron Y. Strauss**

---

[210] Kerr, *supra* note 208, at 41. Professor Kerr argues that modern courts confronted with applications of Fourth Amendment in cyberspace are likely to look to the many federal court decisions applying the Fourth Amendment in the physical world. He argues that this is an important task because it prevents creating one Fourth Amendment for the physical world and another for cyberspace.

[211] *See* Adler, *supra* note 21, at 1093 (quoting Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, THE HUMANIST, Sept./Oct. 1991, at 15, 16 ("New technologies should lead us to look more closely at just what values the Constitution seeks to preserve.")).

* Notes & Comments Editor, *Cardozo Arts & Entertainment Law Journal*; J.D., 2002, Benjamin N. Cardozo School of Law; B.A., 1999, New York University, *cum laude*. The author has accepted an offer of employment from Kelley, Drye & Warren LLP, New York, NY. The author wishes to thank Professor Yu and Professor Huigens for their insight and guidance, as well as the staff and editors of the *Cardozo Arts & Entertainment Law Journal*. This Note is dedicated to Michal Strauss, the author's wife, whose love and support know no bounds.