Virtual Search and Seizure:

How the FBI's "Carnivore" Could Devour the Fourth Amendment in Cyberspace

Gary D. Schneider

April 13, 2001

Preface:

This article was originally scheduled for law review publication in the winter of 2001. However, before this article was published, the September 11th terrorist attacks inspired the passage of the federal "PATRIOT" Act in late October of 2001. The PATRIOT Act is a voluminous piece of legislation that fundamentally changed the substantive and procedural law governing electronic surveillance in the United States. Some provisions of the PATRIOT Act are permanent, while others are subject to "sunset" provisions after several years pass. Regardless, the PATRIOT Act rendered much of the discussion of statutory authority within this article obsolete, at least with respect to its application to the Carnivore system.

While the long-term effects of the PATRIOT Act remain to be seen, any subsequent review of the expanded authority granted to law enforcement by the PATRIOT Act must be evaluated in light of the delicate balance that exists between the legitimate surveillance needs of law enforcement and the individual liberty each of us enjoys because we are generally free from excessive government intrusion into our lives. In spite of the September 11th terrorist attacks, our nation must still pay heed to a prophetic statement made by Benjamin Franklin more than two hundred years ago:

> "Those who would trade essential liberty to purchase a little temporary safety deserve neither liberty nor safety."

- Gary D. Schneider – January 12, 2002.

> **I CONTINUE TO BELIEVE THAT AN UNGRUDGING APPLICATION OF THE FOURTH AMENDMENT IS INDISPENSABLE TO PRESERVING THE LIBERTIES OF A DEMOCRATIC SOCIETY."**
>
> **–JUSTICE THURGOOD MARSHALL [1]**

I. An Introduction to the Search and Seizure Boundaries of the Fourth Amendment

The Fourth Amendment[2], and the body of law that has grown out of it, are designed to balance two diametrically opposed interests: (1) the legitimate investigative needs of law enforcement and (2) personal privacy, which is made possible by freedom from unreasonable government intrusion. The balance between these two interests is a zero sum analysis. By whatever amount we increase the protection of our personal privacy, the effectiveness of our society's law enforcement will inevitably decrease. Conversely, any increase in the extent of law enforcement's ability to conduct electronic surveillance

[1] *Rawlings v. Kentucky*, 448 U.S. 98, 121 (1980).

[2] U.S. Const. amend. IV ("The right of 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 places to be searched, and the persons or things to be seized.").

will result in a corresponding decrease in personal privacy. As a result, any judicial or legislative action involving government surveillance authority will impact the balance of power between the legitimate needs of law enforcement and the guarantee of freedom from unreasonable government intrusion contained within the Fourth Amendment.[3]

The evolution of search and seizure law in the United States extends from early judicial interpretations of the Fourth Amendment to Resolutions that are now pending in the House of Representatives.[4] In reference to electronic surveillance, the balance established by the Fourth Amendment has been maintained by a relatively standard progression of events: as electronic surveillance technology improves, additional legal safeguards are necessarily imposed upon law enforcement's use of those technologies; thus, a relatively acceptable balance of the interests represented within the Fourth Amendment is maintained.[5] Recently, the FBI has begun making use of new electronic

---

[3] *Id.*

[4] H.R. Res. 4987, 106th Cong. § 2 (2000). (The Digital Privacy Act of 2000.); H.R. Res. 5018, 106th Cong. § 2 (2000) (The Electronic Communications Act of 2000).

[5] *See Goldman v. U. S.*, 316 U.S. 129 (1942); *Silverman v. U.S.*, 365 U.S. 505 (1965); *Clinton v. Va*, 377 U.S. 158 (1964).

surveillance technology that has never been specifically authorized by the legislature or the courts. The net result has been a shift of the Fourth Amendment balance in favor of law enforcement with no legislative or judicial restraints being implemented to offset the impact of this new technology on personal privacy.

II. The Birth of a Carnivore

In April of 2000, the existence of the Federal Bureau of Investigation's (FBI's) latest electronic surveillance tool was disclosed to the House Judiciary Committee's Subcommittee on the Constitution.[6] For some time prior to this disclosure, the FBI had quietly developed and repeatedly deployed an allegedly proprietary system of computer hardware and software that was designed to provide the government with the ability to perform covert surveillance of Internet communication.[7] The FBI computer programmers who wrote the software for this new computer system gave it the name

[6] H.R. Jud. Comm. Subcomm. on the Const., *The Fourth Amendment and the Internet*, 106th Cong. 2 (April 6, 2000) (testimony of Robert Corn-Revere).

[7] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Kevin DiGregory, Deputy Asst. Attorney General for the U.S. Dept. of Justice).

"Carnivore" because it "rapidly finds the 'meat' in large quantities of data."[8]

Carnivore was designed to intercept digital information while that information is in motion between computers linked via the Internet.[9] The Carnivore system itself is comprised of "off the shelf" computer hardware powered by advanced data filtering software, all of which operates on a Microsoft Windows based platform.[10] To deploy Carnivore, the system must be physically attached to the telephone lines in between a targeted computer, generally an Internet Service Provider's (ISP's) system, and the rest of the Internet.[11] Carnivore then intercepts ALL of the electronic data traveling to and from that specific computer in real time.[12]

After the interception of all data traveling to and from a specific

---

[8] John Schwartz, *FBI Web Monitoring Debated*, Washington Post A01 (Jul. 21, 2000).

[9] *Id.*

[10] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Tom Perrine of the San Diego Supercomputer Center).

[11] FBI Website, *Carnivore Diagnostic Tool* <http://www.fbi.gov /programs/carnivore/carnivore.htm> (Accessed Oct. 13, 2000).

[12] *Id.*

ISP computer, Carnivore then "filters" the intercepted data in order to exclude all but the information that is legally authorized for electronic surveillance.[13] In theory, the Carnivore system can distinguish the email traffic of one person from that of another; additionally, Carnivore is alleged to be capable of distinguishing between a surveillance subject's email communication and, for example, his on-line shopping information.[14] Any data that is not filtered out by Carnivore is electronically copied and stored on removable disks for later retrieval.[15]

The intent of Carnivore's filtering capability is actually two-fold: (1) to limit the data that is copied as closely as possible to only that information legally authorized for interception and (2) to ensure that all of information authorized for interception is actually captured.[16] While significant questions remain regarding the effectiveness of Carnivore's ability to actually filter electronic data with the specificity claimed by the FBI, presumably, the system can perform its basic functions with

---

[13] *Id.*

[14] *Id.*

[15] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Tom Perrine of the San Diego Supercomputer Center).

some level of effectiveness.[17]

According to Donald Kerr, the Asst. Director of the Federal Bureau of Investigation (FBI), Carnivore has been deployed in two separate capacities: (1) as the internet equivalent of a telephone wiretap and (2) as the internet equivalent of a telephone "pen register".[18] Depending upon which of these two ways in which Carnivore can be is used, the legal restraints applicable in each context are vastly different.[19]

When used in its internet wiretap capacity, Carnivore captures and copies the entire content of all information sent to and from a specific surveillance subject.[20] When used in its pen register capacity, Carnivore allegedly limits the data it copies to specific internet routing

---

[16] *Id.*

[17] *Id.*

[18] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Kevin DiGregory, Deputy Asst. Attorney General for the U.S. Dept. of Justice).

[19] *Id*; *see*18 USC §§ 3121 *et. seq.*

[20] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Kevin DiGregory, Deputy Asst. Attorney General for the U.S. Dept. of Justice).

information, which the FBI contends to be something roughly comparable to the "number dialed" on a telephone.[21] The flaw in the FBI's analogy of comparing what Carnivore captures to that which is captured by a telephone pen register is explained in later sections of this article.[22]

In order to analyze the limitations that are currently imposed or even those that could be imposed on the use of high tech surveillance systems such as Carnivore, one must understand the basics of the technology to which these legal limitations are to be applied. Only by examining both the technology behind Carnivore and the laws that govern its use can the Fourth Amendment balance between the needs of law enforcement and personal privacy be fully evaluated. For this reason, the following section is broken into two portions: (1) a basic description of the technology behind Internet communications as well as (2) the development of legal restrictions placed upon electronic surveillance within United States.

---

[21] *Id.*

[22] *See infra. n.97-99.*

III. The Technology Behind Internet Communications

Judge Paul L. Friedman of the US District Court for the District of Columbia has suggested that, "[it] is probably safe to say that more ideas and information are shared on the Internet than in any other medium," and that it may only be a slight overstatement to conclude that "the Internet represents the brave new world of free speech."[23] In the history of mankind, only the invention of the printing press has revolutionized human communication more than the development of the Internet. Not only has the Internet accelerated the pace at which people can communicate with one another, it has fundamentally changed the manner in which they do so.

The Internet is essentially comprised of a massive network of computers linked together by telephone lines; this connection gives each computer attached to the internet the theoretical ability to communicate in a uniform manner with every other computer also linked to the Internet.[24] Subject to certain limitations, any computer

---

[23] Blumenthal v. Drudge, 992 F. Supp. 44, 48 n. 7 (D.D.C. 1998).

[24] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July

attached to the Internet has the potential to actively seek out and retrieve any information that is stored on any other computer that is also attached to the Internet. [25] The flip side of this coin is that any computer attached to the internet also has the potential to passively receive information sent from any other computer also attached to the internet. Whether actively retrieving or passively receiving information, the manner in which internet communication flows requires that the information be sequentially routed through a potentially large number of computers with each acting as a relay station for the transfer of information.

Some computers in this relay network are specifically dedicated to the Internet and are thus capable of constant information exchange. For the most part, these specific Internet-dedicated computers (servers) are generally high capacity computers owned by government interests,

---

24, 2000) (testimony of Tom Perrine of the San Diego Supercomputer Center)

[25] *See*, Timothy B. Lennon, *The Fourth Amendment's Prohibitions on Encryption* Limitation, 58 Alb. L. Rev. 467. (gives an in depth look at complex systems of encryption and password technology that have developed to prevent unauthorized access to information meant only for certain internet users).

educational institutions or large private organizations.[26] Some servers exist only to serve the needs of the organization that owns them, while others exist solely to function as commercial Internet Service Providers (ISPs). For most home and business users, ISP's provide the means for remote internet access via the use of a personal non-internet-dedicated computer fitted with some sort of computer modem.

Non-dedicated computers intermittently join the network of dedicated computers, primarily through the use of standard telephone "dial up" accounts. Individual home users generally pay a fee to the owner of an ISP computer in order to be able to intermittently access the information contained within the vast array of Internet connected computers.[27] With the ready availability of home dial-up accounts, and uniform flat rate billing for such services, the use of email and other

---

[26] With the availability of high-speed Internet access via DSL and Broadband Cable Service providers, many home computer users' now essentially have their own dedicated Internet connection.

[27] In theory, any dedicated computer can share its access to information with all other computers attached to the Internet. Typically, a home user gains access through a standard modem dial-up account service offered by an owner of a dedicated computer that serves as an Internet Service Providers (ISP's). Companies such as America Online, Earthlink, and the Microsoft Network serve large

forms of Internet communication within the home has grown exponentially over the last decade.[28]

IV. On-Line Communication: The Impact of a New Medium

As of December 1999, nearly 56% of American adults are "on-line"— representing a six-fold increase in the number of Americans using the internet over four years.[29] Unlike any media preceding it, Internet communication has found a way to integrate visual and audio information in order to offer a new mode of communication that can instantly reach an extremely broad audience or be targeted to just a single recipient. As with any widely used medium of communication, the Internet inevitably found itself playing host to illegal activity, both as the means of the crime and as a tool for facilitating criminal enterprise.

While Internet communication began as the exclusive domain of

---

numbers of home users through a series of Internet-dedicated computers.

[28] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Alan Davidson, referencing a December 1999 Harris Poll).

[29] *Id.*

the government and a handful of academics, this technology has already moved into the mainstream and will continue to redefine the way that people communicate. By the year 2003, there are expected to be more than 350 million Internet users worldwide; the bulk of those users will be located in the United States.[30]

With such broad-based access to Internet communication readily available to the public at large, law enforcement must be allowed to employ new technology driven tools to maintain the surveillance capability that it presently enjoys. However, as law enforcement attempts to keep pace with the potentially criminal uses of new technology, law enforcement's use of electronic surveillance technology must be monitored to assure that both the Fourth Amendment, and personal privacy in general, are not eroded away altogether.

V. Electronic Surveillance Law and the Birth of the "Reasonable Expectation of Privacy"

In 1928, the Supreme Court addressed the constitutionality of one of the earliest form of electronic search and seizure, the traditional

[30] *See* Phil Harver, *LookSmart Promises to Clean up the Clutter on the Internet*, Upside Magazine, Oct. 1, 1999, at 71.

telephone "wiretap."[31] This case, *Olmstead v. U.S.*[32], represented the Court's first real foray into the law of electronic surveillance.[33] In 1928, the *Olmstead* Court held that wiretapping did NOT constitute a search as contemplated by the Fourth Amendment; the Court's logic therein stemmed from the notion that without a "physical invasion" there could be no search - without a search, the protections of the Fourth Amendment would not be triggered.[34]

To understand the limited impact that the *Olmstead* decision had on the American public at the time, the practical realities of electronic communication in 1928 must be addressed. Simply stated, telephones did not enjoy the widespread use in 1928 that they do now. While the implications of the *Olmstead* decision were considerable for a discrete number of individual defendants, Americans as a whole were largely unaffected by *Olmstead* on any practical level. In 1928, the telephone had not fully developed as a medium of mass communication. Thus, *Olmstead* acutally did very little in any real sense to tip the Fourth

---

[31] *Olmstead v. United States*, 277 U.S. 438 (1928).

[32] *Id.*

[33] *Id.*

[34] *Id.* at 458.

Amendment scale in favor of either of the diametrically opposed interests embodied therein.[35]

Because of *Olmstead* and its limited progeny, the Fourth Amendment simply did not apply to electronic surveillance for the years between 1928 until 1967.[36] During this time, under the leadership of J. Edgar Hoover, the FBI conducted a wide range of highly reported electronic surveillance of a relatively controversial nature.[37] By 1967, the use of this technology had advanced in such a way that the Court was forced to reevaluate whether *Olmstead's* "physical invasion" standard could still adequately preserve the balance between the surveillance needs of law enforcement and the personal privacy needs of the American public.[38]

With its 1967 *Katz* decision, the Supreme Court redefined the

---

[35] U.S. Const. amend. IV.

[36] *See Katz v. US*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438 (1928)

[37] The FBI's covert surveillance of celebrities, civil rights leaders, and "suspected communists" throughout the 1940's and 1950's has been widely reported. This type of surveillance during J. Edgar Hoover's administration of the FBI was an integral part of the American political scene during the McCarthy era.

[38] *Olmstead*, 277 U.S. 438 (1928).

threshold of the Fourth Amendment.[39] Since 1967, the Fourth Amendment has protected "people, not places."[40] In *Katz*, the Supreme Court held that "the Fourth Amendment governs not only the seizure of tangible items, but additionally extends to the recording of oral statements overheard without any 'technical trespass under…local property law.'"[41] Since then, wiretaps have been legally authorized only after a magistrate or judge issues a valid search warrant supported by a finding of probable cause.[42]

Through *Katz*, the judicial analysis required for the Fourth Amendment was given a new starting point.[43] In his concurrence in *Katz*, Justice Harlan set forth the "reasonable expectation of privacy" standard.[44] In order to merit Fourth Amendment protection, one must have a reasonable expectation of privacy. This "reasonable expectation

---

[39] *Katz v. U.S.*, 389 U.S. 347 (1967)

[40] *Id.* at 351.

[41] *Id.* at 353, *citing Silverman v. U.S.*, 365 U.S. 505, 511.

[42] *See Id.*; 18 USC § 2520 *et. seq*

[43] *Katz*, 389 U.S. at 359. (Justice Harlan's concurrence in *Katz* was eventually adopted as the starting point for judicial search and seizure analysis in *Smith v. Md.*, 442 U.S. 735 (1979)).

[44] *Id.*

of privacy" requires a two-step analysis. First, the person subjected to electronic surveillance who seeks the protection of the Fourth Amendment must possess a "subjective expectation of privacy."[45] Second, that subjective expectation of privacy must be such that "society is willing to recognize [it] as reasonable."[46] Thus, the reasonable expectation of privacy standard is simultaneously subjective and objective. In other words, an individual must hold a subjective expectation of privacy that is objectively reasonable in the eyes of society.[47]

VI. The Judicial Approach to Pen Register Surveillance

From 1967 until 1979, little was done with Justice Harlan's concurrence in *Katz*. However, in 1979, the Court was once again forced to evaluate the Constitutionality of a new form of electronic surveillance – the pen register.[48] Perhaps ironically, the first Supreme Court case that found a majority willing to adopt Justice Harlan's "reasonable expectation of privacy" standard as the starting point of

---

[45] *Id.*

[46] *Katz*, 389 U.S. at 359.

[47] *Id.*

[48] *Smith v. Md.*, 442 U.S. 735 (1979).

Fourth Amendment jurisprudence, provided an early example of how easily a "reasonable expectation of privacy" can be defeated.[49]

In *Smith v. Maryland*, the Supreme Court found that no one in the United States possesses a reasonable expectation of privacy in the number that they dial to initiate a telephone conversation.[50] In the rationale of the *Smith* opinion, the Supreme Court drew a legal distinction, albeit perhaps an arbitrary legal distinction, between the number dialed to initiate a telephone conversation and the "communication" imparted by the call itself.[51]

The Court justified the *Smith* decision based partially on the nature of pen register surveillance as the fruits of pen register surveillance provide limited information: a the list of numbers dialed from a specific targeted telephone. Additionally, the *Smith* court also placed a great deal of weight on the notion that pen register surveillance gives the government virtually no opportunity to obtain access to the "content" of the communication imparted by the telephone

[49] *See Id.*

[50] *Id.* at 742 (1979).

call, because "investigators have no knowledge of whether a conversation had even taken place."[52] With the *Smith* decision squarely supporting this new form of electronic surveillance, law enforcement acquired free reign to implement pen register surveillance without the being subject to any kind level judicial review or any concern that Fourth Amendment may be violated.

VII. The Congressional Approach to Pen Register Surveillance

The Supreme Court's decision in *Smith* left law enforcement with absolutely no restriction upon the use of pen register surveillance.[53] Eventually, Congress weighed in on the pen register issue and in doing so tipped the Fourth Amendment scale slightly in favor of personal privacy by enacting the "Pen Register Act" as part of

---

[51] *Id.* (The *Katz* decision's removal of the "number dialed" from the rubric of "communicative content" truly appears to be a result oriented approach to the questions legal issues raised in *Smith*.)

[52] *Id.* at 741, *citing U.S. v. New York Tel. Co.*, 434 US 159, 167 (1977).

[53] *Id.*

the Electronic Communications Privacy Act of 1986 (ECPA).[54] In general, the ECPA prohibits the installation or use of a "pen register or tap and trace devices"[55] without first obtaining a "court order."[56] However, the legal standard that must be met for federal law enforcement to obtain a "pen register" order is significantly lower than that which is required for other forms of electronic surveillance.[57]

Both "pen register" orders and "tap and trace" orders may be issued via an *ex parte* proceeding before a federal magistrate; this magistrate is statutorily bound to a lesser threshold than is required for other forms of electronic surveillance. Specifically, the Pen Register Act, applicable to pen register as well as "tap and trace" orders, mandates that a court "SHALL enter an *ex parte* order authorizing the installation and use of a pen register or tap and trace device" where a

---

[54] 18 USC §§ 3121 *et. seq.*, (The Pen Register Act was included in a series of acts collectively know as the Electronic Communications Privacy Act of 1986.)

[55] 18 USC § 3123(a). (A "tap and trace" order is the functional converse of a pen register order in that it gives law enforcement access to the phone number of people who have initiated a call to a subject of surveillance (surrepticious caller ID) whereas pen registers give access to the numbers dialed by the subject of surveillance.)

[56] *Id.*

[57] *Id.*; 18 U.S.C. §§ 2510-22.

law enforcement officer certifies that the "information likely to be obtained is relevant to an ongoing criminal investigation."[58]

In a very real sense, the only judicial review that a magistrate presented with a pen register order exercises is only to verify that a law enforcement official is certifying that the pen register to have potential relevance in an on-going investigation. As a practical matter, such, Congress's response to the pen register *carte blanche* granted by the Smith case[59] actually offers very little in the way of judicial oversight of law enforcement's use of pen register surveillance.

Conversely, in order to obtain an order for electronic surveillance of communicative content, i.e. a traditional wiretap of phone calls, government investigators are required to obtain a warrant supported by a finding of probable cause as determined by a federal judge.[60] When applied to telephone surveillance, "pen register" and "tap and trace" surveillance provide government investigators with access to a list of outgoing phone numbers dialed or incoming phone

[58] 18 USC § 3123(a).

[59] 442 U.S. 735 (1979).

[60] 18 U.S.C. §§ 2510-22.

numbers of callers—and nothing more.[61]

The entire distinction between the legal requirements for pen registers and traditional wiretap orders is based on the Court's dicta in *Smith.*[62] Had *Smith* not declared in 1979 that a "number dialed" is somehow separate from the communicative content of a telephone call, all clandestine government telephone surveillance would likely be subject to the same standard, the warrant requirement. By analogy, all uses of Carnivore would also require a warrant authorizing its use.

VIII. Applicability of Current Restrictions on Electronic Surveillance to Carnivore

When applied to existing forms of electronic communication beyond telephones, "pen register" and "tap and trace" orders become something significantly more than mere "content neutral" surveillance. To implement something akin to a "pen register" or a "tap and trace" order for email and other Internet communication, the FBI now has the Carnivore system. However, this new technology is being implemented

---

[61] *Smith v. Md.*, 442 U.S. 735, 741 (1979), *citing U.S. v. New York Tel. Co.*, 434 US 159, 167 (1977).

[62] See *id.*

under a framework that was designed to shield personal privacy only from the fruits of telephone pen register surveillance.[63]

The Carnivore system, when attached to an ISP's computer system, filters all of the electronic data that passes into or out of an ISP's computer. To understand the extent of Carnivore's surveillance capabilities, the deployment of which requires virtually no judicial review,[64] the common uses of internet communication must be examined.

Communication via the Internet can roughly be divided into two categories: (1) directed communications, i.e. information that is actively distributed by a sender to specifically designated recipients and (2) posted communications, i.e. information that is electronically "posted" for display by a sender and then sought out by the recipients of the communication. For the most part, directed communications consist of standard email and private internet "chat" systems. The second category, posted communications, consist primarily of

---

[63] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Donald M. Kerr, Asst. Director of the Federal Bureau of Investigation).

[64] 18 USC § 3123(a).

information accessible on web sites, electronic bulletin boards or public "chat" systems. While the distinction between these two categories is certainly blurred at the middle, directed communications are arguably subject to the "reasonable expectation of pricvay. However, posted communications are most likely not subject to Fourth Amendment analysis because such communications have been knowingly exposed to the public.[65] Once a communication is openly disclosed in such a public manner, the sender of the communication clearly retains no objective expectation of privacy because the information has been voluntarily disclosed to the public. In the absence of a either the subjective or objective elements of one's expectation of privacy, communication does not merit the protection of the Fourth Amendment because the sender has "assumed the risk" that a third party may disclose the communication to the government.[66]

Most frequently, ISP's serve large numbers of home and business users of internet dial-up accounts. When one of those users is the subject of an on-going federal criminal investigation, all of the data

[65] *U.S. v. Miller*, 425 U.S. 435 (1976).

[66] *Id.*

traffic from an ISP used by a suspect is subject to seizure by Carnivore. The software end of Carnivore then filters through every piece of information sent by ALL of the users of the same ISP as the individual who is the subject of the FBI's surveillance. This information, which must pass through the ISP on its way to the Internet, is intercepted in real-time and digitally filtered in order to find electronic communications that contain data identifying that they are either to or from the subject of the investigation.[67] Once such information is located and tagged, through a process known as "packet sniffing," the information is then recorded and stored on high-density removable disk drives for later retrieval by FBI agents.

In theory, and much of this is speculation based on the minimal disclosure offered by the FBI,[68] Carnivore allegedly has the capacity to be programmed to filter out all unrelated communications, as well as the bulk of the "content" portion of the intercepted communications.

---

[67] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Steve Bellovin and Matt Blaze).

[68] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Donald M. Kerr, Asst. Director of the Federal Bureau of Investigation).

The FBI is then left with only a record of something loosely resembling the Internet equivalent of "numbers dialed" on a telephone, i.e. email addresses or the Internet addresses of any web sites visited by a criminal suspect.[69] From a "content" standpoint, the collection of the internet equivalent of "pen register" information is problematic because internet web-site addresses often contain a portion of the communicative content.[70] Additionally, there is currently no statutory requirement for the review of the quantity or quality of the information retrieved by Carnivore when deployed in its "pen register" capacity. In addition to the level of secrecy necessarily surrounding Carnivore[71], the lack of real statutory controls on the potentially far-reaching use of the system has led the FBI to adopt a position that can essentially be summarized as, "Trust us, we're the FBI."

---

[69] *Id.*

[70] S*ee infra* n. 94-97.

[71] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Steve Bellovin and Matt Blaze who propose that if the Carnivore system would be threatened by public disclosure of its source code, then the effectiveness of a system that can be so easily defeated must be called into question).

IX. Statutory Authorization and Control of Electronic Surveillance

Law enforcement derives much of its electronic surveillance power from the Crime Control and Safe Streets Act of 1968 (Title III).[72] Title III specifically authorizes law enforcement to intercept a variety of wire and electronic communication but limits such surveillance with a warrant requirement. The warrant must be based on probable cause and state with specificity the place to be searched and the things to be seized.[73]

The Electronic Communications Privacy Act of 1986 (ECPA) further clarified law enforcement's authority regarding electronic surveillance.[74] The ECPA contains two particularly relevant sections: (1) the Wiretap Act[75] and (2) the Stored Information Act[76]. The Wiretap Act makes it unlawful to listen to or observe the contents of private communication without the permission of at least one party or a

---

[72] 18 USC §§ 2510-22.

[73] U.S. Const. amend. IV.

[74] 18 USC §§ 2510 *et. seq.* (ECPA title I, "Wiretap Act").

[75] *Id.*

[76] 18 USC §§ 2701 *et. seq.* (ECPA Title II, "Stored Information Act").

valid warrant.[77] The Stored Information Act generally prohibits the disclosure of the content of electronically stored communications or user information to the government unless an appropriate warrant, court order or subpoena is obtained; however, this applies to only the first 180 days of storage.[78]

The ECPA was collectively designed to serve two ends: (1) to protect the privacy of wire and oral communications and (2) to delineate on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.[79] Because of the nature of developing technology, the ECPA was intended to extend the authorization of electronic surveillance beyond the realm of merely wire and oral communication, thus including all electronic communication intercepted in "real-time."[80] However, in 1968, wire and oral communications were all that the authors of Title III had contemplated.

---

[77] 18 USC §§ 2510 *et. seq.*

[78] *Id.*

[79] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Kevin DiGregory, Deputy Asst. Attorney General for the U.S. Dept. of Justice)

It must be noted that the ECPA does not apply to any electronic communication that has been stored over 180 days.[81] The logic driving this distinction is that after 180 days, the holder of such information is no longer acting in a "postal carrier" type of capacity and is instead acting as a third party who stores any business record.[82] As such, after 180 days this information becomes subject to law enforcement's subpoena power through the doctrine surrounding voluntary disclosure of information to a third party.[83]

When seeking to compel either electronic or physical data from an unwilling party, the government must satisfy the warrant requirement in order to seize information. Part of the warrant requirement is the mandate that the warrant state with *particularity* the place to be search and the things or persons to be seized. Thus, when one document is the target of a search, a warrant can be challenged as overly broad when it authorizes the seizing of several rooms full of file

---

[80] 18 U.S.C. §§ 2510-22.

[81] 18 U.S.C. § 2703(a) (Both of the pending House resolutions in this area, H.R. 4987 and H.R. 5018 would extend the statutory minimum set forth in 18 U.S.C. § 2703(a) from 180 days to one year).

[82] *Id.*

[83] *U.S. v. White*, 401 US 745 (1971).

cabinets.[84] However, this restriction on the seizure of tangible data does not translate neatly into a comparison with electronic data. The same information housed in several rooms of file cabinets can be stored on one computer hard drive. In this circumstance, a warrant authorizing the seizure of an entire computer to seek a single document within that computer may not necessarily be found to be overly broad. The disparate treatment of the same information in different forms continues because Federal Magistrates continue to authorize the wholesale seizure of entire computer systems in an effort to locate a handful of electronic files contained therein.[85]

The *Smith* decision was based on the distinction that there is no "content" in a number dialed.[86] The *Smith* Court held that the number dialed is not part of the communication undertaken through telephone call;[87] in response, Congress enacted the Pen Register Act to put some minimal level of accountability onto federal law enforcement's use of

---

[84] Note, *Keeping Secrets in Cyberspace, Establishing Fourth Amendment Protection for Internet Communication*, 110 Harv. L. Rev. 1591, 1599-1601 (1997).

[85] *U.S. v. Hunter*, 13 F. Supp.2d 574, 583 (D. Vt. 1998)

[86] *Smith v. Md.*, 442 U.S. 735 (1979).

[87] *Id.*

pen register and tap and trace technology, whether the information gained was content neutral or not.[88] However, even these legislative restrictions on pen register and tap and trace orders have never risen to a warrant requirement.[89]

Law enforcement's relatively unrestricted use of pen register and tap and trace technology was never contemplated to apply outside of telephone surveillance.[90] However, the FBI is essentially analogizing its use of Carnivore to its pen register authority so as to justify its surveillance of internet communication. This tilts the Fourth Amendment balance distinctly in favor of law enforcement. While no controlling legal authority has directly addressed whether the FBI has this authority, the FBI's use of this new technology clearly goes beyond at least the contemplated purpose of 18 U.S.C. § 3123(a).

The requirements for the internet equivalent of a pen register would be better suited to a standard above that of a traditional telephone pen register order. Because the content seized with an internet pen register is significantly more than that of a traditional

[88] 18 USC § 3121 *et. seq.*

[89] *See* 18 USC § 3123(a).

telephone pen register. In this sense, the determination of whether to allow such surveillance would be better served by federal judge who is not bound by statutory mandates requiring that he "SHALL" authorize the order so long as an agent of law enforcement believes that the info is "likely to be relevant to an ongoing criminal investigation."[91]

Without some level of judicial control over the method through which Carnivore conducts electronic surveillance, the unauthorized, or even unskilled, use of such a powerful system has huge potential for abuse. Carnivore can potentially give the FBI access to ALL of the content in a communication while traditional telephone pen registers give the government access only to the number dialed. Additionally, unlike telephone pen registers, Carnivore necessarily searches through ALL content to extract the Internet equivalent to the "number dialed."

The Department of Justice (DOJ) publicly supports the current dual standard of judicial review required to deploy the Carnivore System in its two allegedly distinctly separate capacities.[92] Recently,

---

[90] *Id.*

[91] *Id.*

[92] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July

the Deputy Assistant Attorney General Kevin V. DiGregory reported to Congress that Carnivore can only be employed with a "court order." [93] However, as discussed earlier, when Carnivore is used for its "pen register" purposes, the "court order" being referred to is merely that minimal level of judicial review required for a telephone pen register order.[94]

While the Assistant Attorney General's assertion that Carnivore's pen register capacity requires a court order is factually correct, it hardly gives an accurate picture of the minimal standard required to conduct such surveillance. While the Supreme Court has declared telephone pen register devices to be a content neutral form of electronic surveillance, Carnivore, in its internet pen register capacity, reveals significantly more information than merely the "number dialed." Even when deployed in its pen register capacity, the hardware aspects of the Carnivore system give the FBI's computers access to ALL of the content that exists in ALL communication entering and

---

24, 2000) (testimony of Kevin DiGregory, Deputy Asst. Attorney General for the U.S. Dept. of Justice)

[93] *Id.*

[94] 18 USC § 3123(a).

leaving a targeted ISP computer,[95] resulting in the FBI having unbridled access to the communications of literally hundreds of home computer users, with no judicial review and no external oversight as to the potential misuse of the Carnivore's abilities.

The software components of the Carnivore system are intended filter intercepted digital information in order to limit the seizure of information to only that authorized by the warrant or court order that supports the seizure. In theory, the filtered information that is provided to the FBI will resemble what the court in *Smith* would have called "content" more than the mere "number dialed" on a telephone. Internet communication is a "packet swap" system, wherein a single email message or click of a mouse that grants access a particular website address is broken into a multitude of tiny packets of information that are sent off in a variety of different directions, with each packet taking a different path to its final destination, where they are reassembled. However, when the packets are intercepted and "sniffed" the FBI potentially gains access to all of the content of the communication

[95] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Steve Bellovin and Matt Blaze).

because each of these packets contains both routing information (which actually is only *roughly* equivalent to the "number dialed") and a portion of the "content" of the message itself. Any analogy between what Carnivore does and what a telephone pen register does is virtually pointless; this is truly a comparison of apples and oranges.

However, even if the fruits of a Carnivore search could be limited to show only the number dialed (e.g. email address or web site address) that internet "number dialed" has a significant likelihood of containing content that a phone number never could. For example, common internet search engines and other web sites routinely include subject matter in the internet equivalent to a "number dialed."[96]

A website's address can be any string of characters used to identify that specific web page.[97] Often there is not much of what the Supreme Court would call content contained therein. However, sometimes the address of a web page address is more complex and can

---

[96] The internet equivalent to a number dialed, with regard to web traffic, is the Universal Remote Lookup (URL) or web page address which is commonly displayed as "http:// <specific web address>.com."

[97] For example, the following is the web address of the Yahoo search engine: http://www.yahoo.com

even contain references to specific user requested information.[98] Occasionally, having access to a web address provides investigators with specific information about potential activities in the real world. For example, if an internet user books an airline ticket on-line, the date, time and location of the flight that has just been booked on-line (hyphen?) may all be contained within the web address itself.[99] That law enforcement would ever be able to acquire such detailed, fact specific information through the use of a pen register was neither

---

[98] The following is the web address, the alleged equivalent in internet terms to a telephone "number dialed." This information could be collected with a mere "pen register order." For example, an ISP user's search on Yahoo for web pages referencing the subjects of "FBI" and "CARNIVORE" would display the following information: http://google.yahoo.com/bin/**query**?p=**FBI**+**CARNIVORE**&hc=0&hs=0 --**(emphasis added)**.

[99] The following is the web address (the functional equivalent in internet terms of a telephone "number dialed") that could be collected with a "pen register order." For example, an ISP user's search on the Yahoo Travel network for roundtrip flight information from Los Angeles to Phoenix departing Sept. 20 and returning Sept 21 is as follows:

http://dps1.travelocity.com/airgcobrand.ctl?smls=Y&Service=YHOE&trip_option=**roundtrp**&num_count=9&module=tripsrch&pax_cnt=1&chld_pax_cnt=0&dep_arp_cd%281%29=**LAX**&arr_arp_cd%281%29=**PHX**&dep_dt_mn_1=**Sep**&dep_dt_dy_1=**20**&dep_tm_srch_1=**deptime**&dep_tm_1=5%3a00+am&dep_dt_mn_2=**Sep**&dep_dt_dy_2=**21**&dep_tm_srch_2=**deptime**&dep_tm_2=5%3a00+am&cls_svc=YR&inp_fl

contemplated in *Smith* nor was it the result that Congress hoped to achieve when the Pen Register Act was enacted in 1986.[100]

While it should be noted that, currently, advanced encryption technology may shield a user's web traffic from view by Carnivore, this limitation is subject only to the FBI's inability to crack the encryption. As the law currently stands, the FBI would justifiably have the authority to de-crypt the fruits of legal electronic surveillance.[101] Decrypting an encrypted message has been analogized to the equivalent of translating intercepted communication from Spanish English.[102]

IX. Pending Legislation that may impact the use of Carnivore

Two pieces of legislation pending in the House of Representatives would likely offer some restrictions on the unbridled use of Carnivore in it's internet pen register capacity.[103] The pending

---

t_opt=all&pref_aln=all&aln_cd%281%29=&aln_cd%282%29=&aln_cd%283%29= --**(emphasis added)**

[100] 18 USC § 3123(a).

[101] *See generally*, Timothy B. Lennon, *The Fourth Amendment's Prohibitions on Encryption* Limitation, 58 Alb. L. Rev. 467.

[102] *Id.*

[103] H.R. Res. 4987, 106th Cong. (2000). (The Digital Privacy Act of 2000.); H.R. Res. 5018, 106th Cong. (2000) (The Electronic Communications Act of 2000.)

"Digital Communications Privacy Act of 2000" would amend the exclusionary Rule in 18 USC § 2515 so as to clarify that "electronic communications" are covered in the same manner as oral and wire communications.[104] Additionally, this pending Resolution would also require public reports by law enforcement with reference to the disclosure of any stored electronic communications that they have received.[105] This bill would also establish a warrant requirement for law enforcement's use of pen register surveillance by amending 18 USC §§ 3122(b)(2) and 3127.

Similarly, the pending "Electronic Communications Privacy Act of 2000"[106] would serve similar ends as the pending "Digital Privacy Act of 2000" but goes further in that it would also amend reporting requirements in 18 USC § 2703 as well as clarifying that the exclusionary rule in 18 USC § 2515 includes electronic communication within the same category as wire and oral communications.[107]

---

[104] H.R. Res. 4987, 106th Cong. (2000). (The Digital Privacy Act of 2000.)

[105] *Id.*

[106] *Id.*; H.R. Res. 5018, 106th Cong. (2000) (The Electronic Communications Act of 2000.)

[107] *Id.*

Additionally, this would raise the pen register requirement and additionally alter the structure of law enforcements' ability to access contents of stored electronic communications by protecting stored communications for one year as opposed to the 180 day limitation currently imposed.[108]

XI. The Problems Inherent in Finding and Effectively Using a Judicial Forum to Control the Use of Carnivore

Statutory reform is likely to be the best route for putting a halt to the use of Carnivore without the authorization of a search warrant. To wait for a judicial determination of whether the use of Carnivore is authorized in its "pen register" capacity without a warrant first being issued could potentially take years. Before a court would have the authority to review the issue, a criminal defendant would had to have been the subject of Carnivore surveillance; the fruit of that surveillance would have to be used against a defendant who was successfully resulting in a convicted at trial. Outside of this scenario, there are very few possible avenues through which the FBI's use of Carnivore as a pen register device could be judicially reviewed.

One must additionally consider that the "rights served by the

[108] *Id.*

Fourth Amendment are particularly difficult to protect because their advocates are usually criminals."[109] Keeping this in mind, the use of Carnivore as a "pen register" is going to be particularly difficult to confront in a judicial forum because the "victim" of the Fourth Amendment violation will almost always be a guilty criminal, who is slightly less than sympathetic. However, once must always remember that the decisions that determine what searches constitute a reasonable exercise of government power affect both the innocent as well as the guilty. Therefore, due to the structure of the judicial system, the Fourth Amendment scale has continually been tipped in favor of restrictions on personal privacy in the name of winning for example the "war on drugs." While these societal concern are truly genuine, they are such emotionally charged topics that they tend to foster result oriented decisions that impact privacy in the name of effective law enforcement. For that reason, the privacy of the innocent is sacrificed to combat the guilty. In this sense, when the "war on terrorism" or the "war on internet child pornography" is undertaken with the same zeal as the war on drugs, there is little indication that the courts will be willing to ease

[109] *Illinois v.* Gates, 462 U.S. 213 (Stevens & Brennan, JJ.,

the continued erosion of the Fourth Amendment.

One additional method may exist to judicially challenge Carnivore's use through a forum other than post-conviction relief. In its current form, the use of Carnivore requires that it be physically attached to ISP's computer. An ISP could potentially bring a suit challenging the constitutionality of the burden imposed on ISPs by the FBI's use of Carnivore. However, this argument seems potentially weak and is unlikely to extend to Carnivore's use in its "pen register" capacity. To date, only one ISP has taken this route. Not only was the effort unsuccessful, but the proceedings took place *ex parte* and have been sealed.[110]

Clearly, the best method for enacting control on the use of Carnivore would be statutory reform. Arguably, the best possible statutory reform would impose a warrant requirement for any use of Carnivore. Congress could do so by amending 18 U.S.C. 3123(a) so as require a warrant for ALL pen register and tap and trace orders,

---

dissenting).

[110] H.R. Jud. Comm. Subcomm. on the Const., *The Fourth Amendment and the Internet*, 106th Cong. 2 (April 6, 2000) (testimony of Robert Corn-Revere).

whether directed at telephone communications or internet communications.[111] However, because "pen register" telephone surveillance is such an effective and relatively non-intrusive tool of law enforcement, Congress is unlikely to hold all "pen registers" to a warrant requirement. In the alternative, Congress could create a legal distinction that reflects the real distinction between the fruits of pen register and tap and trace surveillance of telephones and the fruits of Carnivore in its internet pen register capacity. At a bare minimum, Congress could impose reporting requirements on the use of Carnivore such as those imposed on other forms of electronic surveillance such as wiretaps.

XII. CONCLUSION

As technology has advanced, law enforcement has acquired the power to conduct surveillance without committing a physical trespass. The Courts and the Legislature responded by imposing limitations upon law enforcement's exercise of such power, while attempting to maintain the right of the people to be secure from unreasonable

[111] *See* n. 92.

government intrusion. The Fourth Amendment is based on the understanding that limitations must be placed on the government's unbridled use of its police power. The last few years have brought with them major advances in surveillance technology. Unfortunately, the restraints upon this surveillance have not advanced in an equal fashion. Presently, the FBI uses the minimal requirements for telephone "pen register" orders to justify its warrantless surveillance of internet communications.[112] The combined impact of advancing surveillance technology and dormant legal restraints upon the use of these new technologies have tilted the Fourth Amendment scale significantly in favor of law enforcement and against the protection of personal privacy.

"Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack,

---

[112] H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Kevin DiGregory, Deputy Asst. Attorney General for the U.S. Dept. of Justice); H.R. Jud. Comm. Subcomm. on the Const., *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program*, 106th Cong. 2 (July 24, 2000) (testimony of Donald M. Kerr, Asst. Director of the Federal Bureau of Investigation).

to obtain disclosure in court of what is whispered in the closet."[113] Although Justice Brandeis wrote the preceding line in 1928, the sentiment contained therein still echoes loudly today.[114] To preserve liberty in American society and to avoid excessive government intrusion into the personal lives of American citizens, our nation has established a system of restraints upon the police power of the government. With new tools that give law enforcement heightened effectiveness at confronting crime within our society, the temptation to loosen these restraints and let law enforcement operate more effectively is faced by each generation. However, taken to its logical extreme, the result is totalitarianism. In the late 1700's, Thomas Paine understood that, "he who would make his own liberty secure must guard even his enemy from oppression; for if he violates this duty he establishes a precedent that will inevitably reach to himself."[115] Therefore, when contemplating legal restraints upon the use of electronic surveillance

---

[113] *Olmstead v. United States*, 277 U.S. 438, 473 (1928), (Brandeis, J., dissenting).

[114] *Id.*

[115] Thomas Paine, *Dissertation of First Principles of Government*, 2 The Complete Writings of Thomas Paine 588 (Philip S. Froner ed., 1945).

tools, one must consider the nature of the society in which we desire to live. The framers of our Constitution understood the necessity of the Fourth Amendment in a society such as ours; for ours is a society wherein the full power and resources of the state can be brought to bear against an individual citizen, all in support of the needs of law enforcement.

Simply stated, Carnivore's use as a pen register device is not presently subject to any level of real judicial or legislative restraint. Additionally, the minimal restraints that exist are essentially trumped by the extent of the secrecy surrounding the design and function of Carnivore, as well as being trumped by the lack of any substantive reporting requirements regarding Carnivore's use.

The FBI currently deploys Carnivore under authority that it claims is derived from the Pen Register Act.[116] This alleged authority has never been explicitly authorized by the legislature and the FBI's assumption of this authority appears to serve as an end run around the warrant requirement that the legislature and the courts actually have imposed on some forms of electronic surveillance. Because the

[116] 18 USC § 3123(a).

legislature has never specifically granted such power to the FBI, the question of whether the legislature may even do so in this circumstance without violating the Fourth Amendment remains to be seen. However, the problems with finding an appropriate forum for this challenge are nearly insurmountable. "The burden of guarding privacy in a free society should not be on its citizens; it is the Government that must justify its need to electronically eavesdrop."[117] Clearly, the best route for change in this area would be to amend the Pen Register Act so as to take the FBI's use of Carnivore outside of the realm of the minimal requirements for telephone "pen register" orders.

For an ordered society to exist, the police power of the state must also exist. However, for liberty to coexist with order in our society, the extent of the state's police power must be clearly delineated. Additionally, the state's police power must be subject to reasonable restrictions upon its use. In our society, those restrictions generally begin with the guarantees of liberty contained within the warrant requirement of the Fourth Amendment. For the FBI to continue using Carnivore without any form of real judicial review being imposed upon

---

[117] *US v. White*, 401 U.S. 745, (Justice Harlan, dissenting)

that use is tantamount to a violation of the "right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[118]

* * * * * * * * * *

[118] U.S. Const. amend. IV