The Richmond Journal of Law and Technology

Volume VIII, Issue 3,

Spring 2002

FBI INTERNET SURVEILLANCE: THE NEED FOR A NATURAL RIGHTS APPLICATION OF THE FOURTH AMENDMENT TO INSURE INTERNET PRIVACY

By: Catherine M. Barrett[*].

Cite As: Catherine M. Barrett, *FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy*, 8 RICH. J.L. & TECH. 16 (Spring 2002) *at* http://www.law.richmond.edu/jolt/v8i3/article16.html.

TABLE OF CONTENTS

I. INTRODUCTION

{1}Last year, the Federal Bureau of Investigation ("FBI") acknowledged that it used an Internet electronic surveillance system called Carnivore to investigate and prosecute criminal suspects in more than two dozen cases. Carnivore is a software program developed by the FBI that can be installed on the network of an Internet Service Provider ("ISP"), such as America Online, to monitor, intercept and collect e-mail messages and other Internet activity made and received by individuals suspected of criminal activity.[1]. To date, the full capability of Carnivore remains a secret—the FBI refuses to disclose the source code (computer language) that would reveal how Carnivore operates, noting that disclosure of the source code would compromise the utility of the system to prosecute criminal activity on the Internet. The FBI's use of Carnivore has raised concerns that it violates privacy rights, including the right to be free of unreasonable searches and seizures guaranteed by the Fourth Amendment to the U.S. Constitution.[2].

{2}The FBI contends that the government's use of Carnivore does not violate the Constitutional protection against unreasonable search and seizure because the FBI complies with established standards of proof in place to protect the privacy interests of certain information. The FBI likens the information collected by Carnivore to the information collected by pen registers and trap-and-trace devices.[3]. Pen registers record telephone numbers of outgoing calls and trap-and-trace devices record telephone numbers from which incoming calls originate, much like a caller-ID system.[4] Pen registers and trap-and-trace devices capture what is known as "transactional information," such as the digits comprising a telephone number, but do not capture the content of a communication. Pen registers and trap-and-trace devices operate under a "reasonable suspicion" standard of proof, as further discussed below. [5] Reasonable suspicion is a suspicion based upon the totality of the circumstances whereby activities give rise to the probability of wrongdoing.

{3}In contrast, the information collected by wiretaps is subject to a higher standard of protection under existing Fourth Amendment jurisprudence. This is because wiretaps are used not only to collect transactional information but also to intercept the content of a conversation over telephone wires or cables.[6] Content includes any information concerning the "substance, purport, or meaning of a communication."[7] Wiretaps operate under a "probable cause" standard of proof. Probable cause requires that a search be narrowly focused on the interception of a specific targeted conversation, based upon a special showing of need, and approved by a judge in advance.[8] Probable cause requires the government to meet a more difficult standard than does reasonable suspicion. To meet the probable cause standard, the government must show not only a probability of wrongdoing, but facts and circumstances "sufficient in themselves to warrant a man of reasonable caution" to believe that an offense has been or is being committed.[9] In short, the reasonable suspicion standard offers a lower level of privacy and is a less legally demanding standard of proof than the probable cause standard. The distinction between the

two standards rests with the notion of probability versus possibility. Reasonable suspicion relies upon a process that does not deal with hard certainties, but with probabilities. In contrast, probable cause relies upon certain facts and evidence to form the standard of proof necessary to secure a warrant for government intrusion of personal privacy.[10]

{4}The FBI maintains that existing federal statutory law permits the use of Carnivore under the reasonable suspicion standard of proof that is needed for the government to operate a pen registers and trap-and-trace devices.[11] This article argues that the FBI's contention is wrong. The problem with the FBI's use of Carnivore under the lower reasonable suspicion standard lies with Carnivore's likely ability to capture and copy communication content in addition to transactional information, thus exceeding the scope and intent of the reasonable suspicion standard. This article will argue that since Carnivore is capable of capturing content, law enforcement agents should have to meet the higher probable cause standard that is already required for the use of electronic surveillance such as wiretaps.

{5}This article further argues that the FBI's use of Carnivore and similar Internet surveillance technology under a reasonable suspicion standard demonstrates the danger that new technologies will eviscerate the privacy protections of the Fourth Amendment. Current jurisprudence under the Fourth Amendment recognizes a privacy interest if an individual believes he has a legitimate expectation of privacy *and* society is willing to recognize that expectation of privacy. This paper examines the underlying circular reasoning that characterizes this Fourth Amendment jurisprudence—i.e., that individuals have a right to privacy only if their expectation of privacy is reasonable in context and validated by society. This context-based jurisprudence becomes particularly troublesome as technological advancements produce more intrusive surveillance techniques that reveal communication content. As such technologies become widely implemented, it is no longer reasonable for individuals to retain an expectation of privacy when using means of communication that these technologies may intercept. In this way, electronic surveillance technology comes to control privacy expectations rather than the expectation of privacy rights controlling the use of such technology.

{6}I will refer to this current Fourth Amendment jurisprudence regarding the right to privacy as a "context-based" approach. This approach, I argue, is inferior to a natural rights based test, which treats privacy rights as inherent and not subject to change with changes in social conditions. As I will demonstrate below, this natural rights theory of privacy rights sets forth criteria resistant to subjective interpretation and thus social change upon which the Court should rely in evaluating the standards that should apply to the use of modern electronic surveillance technologies, such as Carnivore.[12]

{7}Part I of this paper describes the current constitutional and statutory laws regarding electronic surveillance of communication. Part II examines an alternative natural rights test to the current context-based test used to determine whether a right to privacy exists in a communication. Part III applies this alternative test to Carnivore and similar technology to show that natural rights jurisprudence better protects a person's right to privacy in communication. Part IV concludes that the probable cause standard protects a person's natural right to privacy in communication and argues that the probable cause standard should apply to the use of Internet electronic surveillance tools such as Carnivore.

II. CONSTITUTIONAL AND FEDERAL STATUTORY LAW REGARDING THE RIGHT TO PRIVACY AND THE USE OF ELECTRONIC SURVEILLANCE

{8}The Fourth Amendment provides a framework of privacy protections for personal communication.[13] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizure, 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.[14]

The Fourth Amendment does not provide a "general constitutional right to privacy," rather, it protects individual privacy against certain kinds of government intrusion.[15]

A. The *Katz* Standard

{9}As noted earlier, current constitutional jurisprudence for electronic communications as established by case law and the Fourth Amendment distinguishes between the *content* of a communication—protected by a high probable cause standard—and the *transactional* information—protected by a lower reasonable suspicion standard.[16] In *Katz v. United States*, the Supreme Court held that government intrusions in the form of electronically monitoring and recording words spoken into a telephone receiver in a public telephone booth "violates the privacy upon which [a person] justifiably relie[s] while using the telephone booth, and thus constitute[s] a 'search and seizure' within the Fourth Amendment."[17] The Court further held that the use of an electronic device that did not penetrate the wall of the booth had "no constitutional significance."[18]

{10}*Katz* established a two-pronged, context-based test by which courts may determine whether an individual has a right to privacy in a communication.[19] The *Katz* test requires that in order to prove a privacy right protected by the Constitution, "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[20] *Katz* established that the Fourth Amendment protects people, not places.[21] In his concurring opinion, Justice Harlan argued that while "a man's home is, for most purposes, a place where he expects privacy," he does not find that same level of privacy in "objects, activities, or statements that he exposes to the 'plain view' of outsiders."[22]

{11}In 1967, the Supreme Court in *Berger v. New York* held that wiretapping is a "search and seizure" within the scope of the Fourth Amendment and established that the government must meet a probable cause standard of proof prior to obtaining a warrant authorizing the use of a wiretap.[23] As noted earlier, a wiretap is a form of electronic eavesdropping in which the content of a conversation is recorded.[24] In *Berger*, the Court held that in addition to a prior showing of probable cause, an application for a warrant to use a wiretap must meet a high privacy standard by particularly describing "the place to be searched, and the persons or things to be seized."[25] The Court defended the use of the probable cause requirement, noting that its purpose is to "keep the government out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed."[26] The Supreme Court further requires electronic surveillance of telephone calls to specify the person whose communications are to be recorded, "particularly describ[e] the place to be searched and things to be seized," and obtain approval from a judge prior to the use of such technology.[27]

{12}On the other hand, three years later in *United States v. Miller*, the Court utilized the *Katz* test to

dismiss any legitimate expectation of privacy concerning the content of banking records, reasoning that such records are negotiable instruments to be used in commercial transactions and that they contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.[28] The Court held that there is no constitutional right or protection against the government's warrantless acquisition of banking information, such as checks, microfilm, deposit slips and other banking records, that have been disclosed to a third party financial institution by the consumer.[29] The Court reasoned that there is "no legitimate expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential, private communications but instead are negotiable instruments to be used in commercial transactions and the business records of the bank.[30] Following *Katz*, the Court concluded, "what a person knowingly exposes to the public is not a subject of Fourth Amendment protection."[31]

{13}Similarly, nearly a decade later in *Smith v. Maryland*, the Supreme Court established that no probable cause standard[32] is needed to acquire transactional records of information that a consumer conveys or transmits to a third party, such as a bank or a telephone service provider.[33] The Supreme Court reasoned that there is "no actual expectation of privacy in the phone numbers he dialed" because the caller had willingly transmitted these numbers to a third party—the telephone company—and thus cannot reasonably expect privacy with regard to them.[34] Thus, the government does not need a warrant grounded in probable cause to search or seize transactional information.[35] Under the lower reasonable suspicion standard of review, "law enforcement need only show, through 'specific and articulable facts,' that 'there are reasonable grounds to believe' that the information is 'relevant and material' to an ongoing criminal investigation."[36]

{14}The Court further reasoned that the installation and use of a pen register by a telephone company does not constitute a "search" within the meaning of the Fourth Amendment, and therefore, "because there was no 'search,' the court concluded no warrant was needed."[37] Again, the Court applied the *Katz* test to determine whether the government's use of a pen register invaded a valid expectation of privacy. In applying the test, the Court reasoned that (1) "the pen register was installed on telephone company property," not the suspect's property, so that the suspect "cannot claim that his property was invaded or that police intruded into a constitutionally protected area;"[38] (2) "a pen register differs significantly from the listening device employed in *Katz* because pen registers do not capture the *contents* of communications,"[39] just transactional information (telephone numbers that have been dialed); (3) "people in general" do not "entertain any actual expectation of privacy in the numbers they dial;"[40] and (4) society is not prepared to recognize an expectation of privacy in telephone numbers dialed.[41] The Court concluded, therefore, that a pen register's limited capabilities do not constitute a "search" within the meaning of the Fourth Amendment.[42]

{15}There is very little constitutional jurisprudence regarding the government's use of Internet electronic surveillance to date. The Supreme Court recently held in *Kyllo v. United States* that government use of a surveillance device "not in general public use to explore details of a private home that would previously have been unknowable without physical intrusion is a search and is presumptively unreasonable without a warrant."[43] This bright line rule is a product of the Court's reasoning that privacy expectations are heightened in the home where "*all* details are intimate details, because the entire area is held safe from prying government eyes."[44] The Court reasoned that if, without sense-enhancing technology, police

cannot gather information without being actually present in the home, a search has occurred.[45] The Court concludes, "to withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[46] In light of the Supreme Court's ruling, some in Congress have called upon the U.S. Attorney General John Ashcroft to consider whether the FBI's use of Carnivore constitutes an illegal search and thus violates a person's Fourth Amendment right against unlawful search and seizure.[47]

{16}In addition, the United States Court of Appeals for the District of Columbia Circuit recently held in *United States Telecom Association v. Federal Communications Commission* that law enforcement might not obtain content information without a prior showing of probable cause.[48] In *Telecom*, the court noted that "a law enforcement agency may receive all post-cut-through digits with a pen register order, subject to [a] requirement that the agency uses 'technology reasonably available to it' to avoid processing digits that are content," and concluded that "no court has yet considered that contention and it may be that a Title III warrant is required to receive all post-cut-through digits."[49] The court described "post-cut-through dialed digits" as "a list of all digits dialed after a call has been connected. Such digits include not only the telephone numbers dialed after connecting to a dial-up long-distance carrier (e.g., 1-800-CALL-ATT), but also, for example, credit card or bank account numbers dialed."[50] In other words, the court held that law enforcement agencies may be required to show probable cause in order to obtain a Title III warrant to access transactional information (dialed digits) because the nature of the information revealed may be detailed and descriptive enough to be deemed content.[51]

{17}In another case, the Court of Appeals of New York addressed the privacy implications of pen registers that may be capable of capturing the content of communications. In *People v. Bialostok* the Court held that under state electronic surveillance law, a pen register capable of being used as a listening device required a warrant based upon a showing of probable cause, rather than a judicial order obtainable based upon a showing of reasonable suspicion.[52]

{18}Thus, the limited case law that exists on point suggests that electronic listening devices such as a pen register capable of capturing conversation content should be held to the same legal standard governing wiretaps—a probable cause standard. As will be discussed further below, Carnivore appears to be capable of capturing more information about a user than a pen register's record of telephone numbers dialed, thus compelling the question of what legal standard transactional information gathered from the Internet should be accorded.

B. Critique of the *Katz* Privacy Standard

{19}As shown above, the Courts have used the *Katz* test to determine whether a privacy right exists under the Fourth Amendment since 1967.[53] The discussion in this section will show that the *Katz* test is a deeply flawed approach to determining whether a right to privacy exists.

{20}There are many problems with the *Katz* context-based approach to evaluating whether a privacy right exists in any given circumstance. A central problem with the *Katz* test is that it is inherently subjective. The *Katz* two-pronged test requires that in order to prove a privacy right protected by the Constitution: "first that a person have exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[54] Thus, in order for a privacy right to exist, society must agree with an individual who asserts a privacy right. Society is

charged with deciding Constitutional rights rather than the Constitution defining the privacy rights society must grant individuals. The *Katz* test allows the courts to "hedge their bets or duck principled analysis" in pursuit of defining what is reasonable.[55]

{21}In addition, the Court's applications of the *Katz* context-based test to new technologies allows the scope of an individual's privacy rights to depend on the state of existing technology. The current Court's context-based jurisprudence focuses attention on a technology's operation and application. As the Court wades through the technical aspects of new technologies in order to determine whether the individual in question reasonably believes he has a right to privacy, the Court reduces a right to privacy secured by the Fourth Amendment to an analysis of the expectation of privacy residing in a specific technology. This becomes a tautology. The Court decides whether a person reasonably *believes* he has a right to privacy in relation to the capacity of new government surveillance technology X, Y, or Z to invade that privacy.

{22}Finally, the *Katz* test only grants protection against government intrusion of privacy rights *if the society,* i.e. people in a given community, are willing to agree that he *deserves* such protection. The Court's use of subjective criteria to determine whether privacy rights exist in the context of increasingly advanced surveillance of communication results in an atmosphere in which people's expectations are driven by what the government has the technological capacity to do. This results in an increasingly lower expectation of individual privacy, which is inherently subjective and therefore unreliable.

{23}In another case, the Eighth Circuit Court of Appeals in the *United States v. Pinson* held that any subjective expectation of privacy that a person may have in the heat that radiates from his house is not one that society would find objectively reasonable; thus, Fourth Amendment rights are not violated by the government's warrantless use of a forward looking infrared device ("FLIR") to detect differences in surface temperatures of a person's house.[56] In this case, the defendant was convicted of manufacturing over 100 marijuana plants; police officers used the FLIR to detect differences in surface temperature of the house where the marijuana was grown under high-intensity lights.[57] In applying the *Katz* test, the court found that "any subjective expectation of privacy Pinson may have had in the heat radiated from his house is not one that society is prepared to recognize as reasonable" and "that the detection of the heat" by the FLIR "was not an intrusion into the home because no intimate details were" revealed through its use and there was "no intrusion upon the privacy of the individuals within."[58] The court stated that thermal imaging does not threaten any of the interests in need of protection with regard to the home, specifically "the intimacy, personal autonomy, and privacy associated with the home."[59] Thus, the court concluded the defendant failed to show an objectively reasonable expectation of privacy.[60] But, this analysis of privacy rights is unconvincing. The court's argument is grounded in an analysis of privacy rights in the context of a given technology—FLIR.[61]

1. Statutory Law

{24}In addition to constitutional jurisprudence, three federal statutes provide law enforcement with a legal framework to obtain authorization for electronic surveillance. In order to intercept telephone conversations, law enforcement agencies must obtain a warrant pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[62] Title III imposes specific limitations on the use of electronic surveillance.[63]. Before issuing a warrant, law enforcement agents must show probable cause. [64] A judge may issue a warrant only if there is a showing of probable cause, if the target of surveillance is substantially linked to the alleged offense, and if the targeted communication will likely

be captured through this surveillance.

{25}Advancements in scientific development and technology have led Congress to enact the Electronic Communications Privacy Act of 1986 (“ECPA”). Consistent with federal constitutional requirements, ECPA created a lower standard for capturing telephone numbers through the use of pen registers and trap-and-trace devices.[65] The ECPA allows the use of a pen register or trap-and-trace device where law enforcement shows that the “information likely to be obtained is relevant to an ongoing criminal investigation.”[66] In contrast, an order to intercept the content of electronic communication requires a showing of probable cause that the target of an investigation has committed a specific criminal activity. This is commonly sought under Title III. As noted, the FBI contends that current federal statutory laws permit the government’s use of Carnivore under the pen register and trap-and-trace laws.[67]

{26}In 1994, Congress passed the Communications Assistance for Law Enforcement Act (“CALEA”) in response to emerging telecommunications technologies. CALEA requires telecommunications carriers and equipment manufacturers to provide technical capabilities within their networks to assist law enforcement with authorized interception of communications and acquisitions of “call-identifying-information.”[68] As the D.C. Circuit Court explained in *U.S. Telecom*, CALEA preserve[s] the government’s ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.[69] CALEA does not alter the existing legal framework for obtaining wiretap and pen register. In addition, CALEA does not extend to “information services” such as e-mail and Internet access.[70]

III. ANALYZING CARNIVORE UNDER EXISTING FEDERAL LAW

{27}The FBI asserts current laws governing pen register and trap-and-trace devices under the ECPA provide the statutory legal protection for the use of Carnivore.[71] Under a pen register and trap-and-trace device, the government must meet a reasonable suspicion standard of proof, which is below the high probable cause standard. The government must only prove that information likely to be captured through the use of electronic surveillance devices is relevant to an ongoing criminal investigation. This is a low threshold of privacy protection, considering that the type of information Carnivore is suspected of collecting far exceeds the transactional information the ECPA intended to permit law enforcement access to.

{28}The FBI maintains Carnivore only collects transactional information and that it is programmed to filter out all content, including the subject line and “re” information. This does not appear to be accurate.[72] According to the Department of Justice’s independent review of Carnivore, conducted under contract by IIT Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law (“IITRI”), Carnivore appears to be capable of collecting content-based information, such as the “addressing” portion of e-mail messages.[73] The “addressing” portion of an e-mail refers to the “to” and “from” lines of an e-mail message, but not the “subject” or “re” lines of the message. According to industry experts, e-mail addresses often carry a person’s name, place of employment or other personal information. E-mail addresses often identify a person’s place of work and ISP provider. For example,

JaneDoe@mci.aol.com reveals that Jan Doe appears to be an MCI employee and uses America Online as her ISP provider.

{29}Carnivore's searches are also believed to have the capability to collect Uniform Resource Locator ("URL") information. "A URL can disclose specific webpages downloaded, websites visited, or even items purchased" on the Internet.[74] An URL address can also reveal "the search terms that may have been entered in an Internet search."[75] The FBI's use of Carnivore is akin to someone following you around a bookstore tracking your every move, taking notes on every book you browse through and collecting data from every person you speak with. The personal information revealed by the "URLs and e-mail messages seem less like a pen register and more like the search of a diary or a phone tap."[76]

{30}In addition, Carnivore reportedly collects and copies e-mail messages and website information of whoever uses the same Internet Service Provider ("ISP") as the criminal suspect. Thus, observers fear that when the FBI attaches Carnivore to an ISP in pursuit of a suspected criminal's online activity, the FBI actually records and reads every e-mail message that enters that particular ISP; it does not effectively isolate the suspect's messages and Internet activities from the general mass of e-mail messages that flow through an ISP.[77] Innocent people who are not the targets of an FBI criminal investigation could have their e-mail messages and Internet activities captured and recorded by the technological capabilities inherent in Carnivore.

{31}Carnivore's suspected ability to keep a record of someone's Internet searches and record copies of someone's personal e-mail messages goes beyond the scope of the law governing pen registers. The President's Working Group on Unlawful Conduct on the Internet has recognized the dissonance between ECPA's language and current technology and noted:

> [A]dvances in telecommunications technology have made the language of the statute obsolete. The statute, for example, refers to a "device" that is "attached" to a "telephone line," [18 U.S.C.]. § 3127(3). Telephone companies, however, no longer accomplish these functions using physical hardware attached to actual telephone lines. Moreover, the statute focuses specifically on telephone "numbers," *id*., a concept made out-of-date by the need to trace communications over the Internet that may use other means to identify users' accounts.[78]

{32}A trap-and-trace device or pen register installed on an ISP network is similar to the application of Carnivore on an ISP network in that the Carnivore software is not installed on a telephone line; rather, it is installed on the data network and the information which may be intercepted is not limited to that transmitted over a single telephone line.[79]

{33}Thus, a key difficulty with the FBI's use of Carnivore under the low reasonable suspicion standard is that the potential quality and quantity of information Carnivore can search and secure transcends the scope of transactional information. Transactional information is devoid of content, such as a telephone number; if the technology is *capable* of capturing content, the probable cause standard should apply.

{34}This argument is vulnerable, however, because of the context-based nature of the *Katz* approach to recognizing privacy rights. In applying the *Katz* test to determine whether a right to privacy exists in the Internet information collected and copied by Carnivore, the court is forced to evaluate the technical capabilities of this Internet surveillance tool and weigh those capabilities against whether "[1] a person . .

. exhibited an actual (subjective) expectation of privacy and [2] that the expectation be one that society is prepared to recognize as 'reasonable'."[80] This context-based approach to determine whether a privacy right exists under the Fourth Amendment essentially holds that a privacy right exists *if* the collective society believes it exists. Therefore, even if an individual demonstrated that he had a reasonable expectation of privacy in a given context, the court would deny him that right if he failed to demonstrate that this expectation of privacy would be accepted as "objectively reasonable" by society.

{35}Another key difficulty with the FBI's use of Carnivore under the low reasonable suspicion standard is that the nature of the information gathered using pen registers and trap-and-trace devices in a telephone environment is far different from the information collected from the use of Carnivore in an ISP environment. The telephone system is a circuit-switch network, meaning that there is a single, unbroken connection between sender and receiver (as with a telephone call, for example). In contrast, the Internet is a "packet-switched" network, meaning "there is no single, unbroken connection between sender and receiver."[81] Instead, when information is sent, it is broken into small packets, sent over many different routes at the same time, and then reassembled at the receiving end.[82] Carnivore is believed to enable law enforcement to compile a detailed, substantive profile of a suspect's Internet activity by accessing these packets. According to the Federal Communications Commission, packet information contains call routing information (such as telephone numbers) and content. Thus, packet information could allow the government to receive both transactional information and content, all under the low criminal standard governing a pen register (reasonable suspicion).[83]

{36}An argument can be made that like other forms of communication such as a telephone conversation. Internet communication involves private content and ought to be protected under the Fourth Amendment probable cause standard. However, if the courts were to evaluate Carnivore utilizing the *Katz* test, it is not clear whether a privacy right would be found. For example, in applying the *Katz* test to determine whether the government's use of Carnivore invaded a valid expectation of privacy, the court might follow the logic established in *Smith v. Maryland*, discussed *supra* at part I, and reason that (1) Carnivore is installed on an ISP's property, not the suspect's property; thus, the suspect cannot claim that his property was invaded or that police intruded into a constitutionally protected area; (2) Carnivore differs significantly from the listening device employed in *Katz* because Carnivore is allegedly not intended to capture the *content* of communications, just transactional information; (3) there is no expectation of privacy in transactional information, such as telephone numbers dialed; and (4) society is not prepared to recognize an expectation of privacy in telephone numbers dialed.[84] The court would likely conclude, therefore, that Carnivore's capabilities do not constitute a "search" within the meaning of the Fourth Amendment.

{37}The Supreme Court has traditionally enforced the Fourth Amendment against physical intrusions into person, home, and property by law enforcement officers.[85] But, the context-based privacy rights analysis inherent in the *Katz* test eviscerates the Fourth Amendment right to privacy by allowing technological advances to "outflank" the existing legal framework. The Fourth Amendment must stand guard to ensure that Internet and electronic surveillance by federal agents are not "contributing to a climate of official lawlessness and conceding the helplessness of the Constitution and [the Supreme] Court to protect rights 'fundamental to a free society'."[86]

{38}.There is, however, an alternative theory of the Fourth Amendment that provides a better, more comprehensive protection of privacy rights even in the face of technological change. That theory is

premised on a natural rights approach to privacy. One of the chief proponents of this theory is legal theorist Richard Epstein, who shares this author's critique of the Supreme Court's reasoning in *Katz*, noting that the "focus on the subjective expectations of one party to a transaction does not explain or justify any legal rule, given the evident danger of circularity in reasoning. More specifically, the legal result should not change because states have habitually practiced snooping, so that no one has any reasonable expectation that their conversations will go undetected."[87] Thus, Epstein argues, the court should concentrate on the communication itself, not the medium in which it is delivered, whether by mail, telephone, Internet or other means.[88] The act of communication, unlike the means of communication, should not be subject to changes which result from successive improvements in technology.

IV. ALTERNATIVE NATURAL RIGHTS FRAMEWORK FOR ANALYSIS OF THE RIGHT TO PRIVACY

{39}Philosophers have thought of privacy as "some immutable categor[y] of a person's nature and activity that [is] inherently private and should not be revealed to anyone."[89] The ability "to exercise or experience privacy" refers to control—control over actions, activities and/or information deemed private.[90] The books a person buys, the videos a person rents, and the social activities a person engages in are examples of what type of information should be protected under this definition of privacy. "[P]rivacy involves a struggle to control information. Personal privacy is one's desire, right or ability to control, withhold and reveal at will information about one's person and activities."[91]

{40}The essence of privacy may also be thought of in terms of a liberty. Philosopher John Stuart Mill defined human liberty as "doing as we like, subject to such consequences as may follow."[92] Others refer to privacy as "the most fundamental of all liberties," "the right to be left undisturbed," and the "right not to have one's personal information exploited without consent."[93] If privacy is a fundamental liberty, akin in nature to such protected liberties as the freedom of religion and the freedom of press, then it follows that privacy is deserving of a similar level of protection as accorded fundamental freedoms by law.

{41}Privacy can also be understood as a property right held by individuals.[94] John Locke's theories established the idea that "every man possesses property in the form of his own person."[95] Libertarians[96] assert that no form of behavioral freedom can exist without a foundation of property rights because property rights "induce people in a free society to behave in ways that benefit the community as a whole."[97]

{42}"A natural right is defined as an independent right not contingent on any situational or environmental factors. If privacy is a natural right, that right would apply to both the real and online worlds, equally to employees, students, library users, browsers, and consumers."[98] In contrast, privacy construed as a context-based right, as in *Katz*, allows for "trade-offs between personal privacy and public interests." The individual must surrender some privacy for the common good and social advancement. Claims of privacy cannot be protected absolutely because of changes in facts, conflicts between the needs of individuals and society, changes of circumstances or developments which may give rise to new claims, and failure to assert certain claims."[99] Privacy defined as a subjective right means that privacy is an idea wedded to the underlying "basic task being undertaken, rather than to the

individual."[100] If one adopts a context-based definition of privacy then "an individual's right to privacy waxes and wanes based on what one is doing."[101]

{43}Epstein introduces privacy rights grounded in natural rights jurisprudence as a superior approach to evaluate questions arising from the use of increasingly advanced technologies because it focuses on the act of communication, rather than focusing on the means or content of communication.[102] As already noted, natural rights jurisprudence is grounded in the premise that individuals, because they are natural beings, have certain inherent rights. Therefore, individual privacy is not a subjective expectation that leads to the belief that there is a "right to privacy;" rather, it is fundamental that every human being has certain natural rights, chief among them the right to be secure in one's own thoughts, words, and actions, so long as they do not infringe on the rights of others or harm others. Epstein rejects the notion that privacy rights are created by the state and says that, "rights are justified in a normative way simply because the state chooses to protect them, as a matter of grace." [103] To illustrate the point, Epstein notes "a common example of personal liberty is that the state should prohibit murder because it is wrong; murder is not wrong because the state prohibits it."[104]

{44}Extending Epstein's logic to Carnivore would suggest that the government ought to be restricted from using Carnivore before proving probable cause and securing a search warrant because to do otherwise would infringe on a person's privacy in communication. The government can use Carnivore to collect content about an individual *before* obtaining a search warrant, thus circumventing the protections offered under the Fourth Amendment and the need to show probable cause. The underlying rationale for the probable cause standard is that an individual's right to privacy ought not be violated *unless* there is reason to believe a specific crime has been or is being committed. The Supreme Court has historically interpreted the Constitution to impose a higher legal standard—probable cause—for search warrants seeking to reveal content than for search warrants seeking to review non-content or transactional material. The probable cause standard recognizes that communication is a human activity deserving a privacy standard grounded in natural rights ideology rather than one determined by a subjective "reasonable suspicion" standard.[105] Private communication "merit[s] the most exacting Fourth Amendment protection," from government intrusion and it is settled law that the probable cause standard of proof is the highest privacy standard available to protect fundamental liberties.[106]

{45}The probable cause standard of proof is the standard needed to evaluate the privacy implications of new technology because it offers the highest form of protection from government intrusion, regardless of what form that intrusion takes. What is important under the probable cause standard is the communication itself, not the medium in which it is delivered, whether by phone, computer or other technology. The probable cause standard refocuses the courts to concentrate on an individual's utterances—the communication—rather than the means used to transmit the communication. The court must look to see that law enforcement officers provide several factual details to prove probable cause, including: a detailed affidavit alleging the commission of a specific criminal offense, the communications facility regarding which subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted.[107] Alternate standards of proof do not require the government to show such an array of factual findings and thus grant the government too much power by leaving much to the discretion of law enforcement agents to use Carnivore to obtain information otherwise protected under the Fourth Amendment.

{46}The FBI maintains that it uses Carnivore to identify and combat an array of criminal activity on the Internet, including terrorism, espionage and information warfare.[108] “Information warfare” refers to foreign military attacks on U.S. critical infrastructures, such as the telecommunications network and satellites, through the use of computer viruses or by other means.[109] The FBI and foreign intelligence services view the Internet as a useful tool for obtaining sensitive U.S. government and private sector information.[110] This may be true, but regardless of the genuine intentions expressed by the FBI, the Fourth Amendment was designed to protect individual privacy, even when the government believes there is good cause to encroach upon it. This paper does not argue against the merits of lawful use of Internet surveillance tools, such as Carnivore; rather, it argues that the FBI’s attempt to extend pen registers and trap-and-trace device orders to the Internet goes beyond the intent of the existing law and violates constitutionally protected privacy rights found in an individual’s content of a communication. The FBI’s use of Carnivore should be permitted under a high-privacy level protected by the probable cause standard of proof.

V. CONCLUSION

{47}Carnivore illustrates the need to amend existing electronic surveillance laws to require probable cause prior to the use of any Internet surveillance tools capable of capturing content. While there may be a legitimate law enforcement need for Carnivore and other Internet surveillance technologies, the Fourth Amendment requirements are not “unreasonably stringent; they are the bedrock rules without which there would be no effective protection of the right to personal liberty.”[111]

{48}The Fourth Amendment is not a mere formality; rather, it is a “rule that has long been recognized as basic to the privacy of every home in America” and thus it is not beyond the scope of law enforcement officers “to comply with the basic command of the Fourth Amendment before the innermost secrets of one’s home or office are invaded.”[112] If the FBI wants to use Carnivore in an ongoing criminal investigation to aid law enforcement efforts, it ought to secure a warrant through a showing of probable cause. In this way, the government is appropriately shouldered with the burden to prove an individual should be deprived of their natural right to privacy in communication—whether by mail, telephone or Internet.

ENDNOTES

[*]. The author would like to thank Professor Susan Carle of American University Washington College of Law for her legal expertise and counsel in the editing of this paper. The author would also like to thank Professor Julian Cook III of American University Washington College of Law for his comments. The author would like to dedicate this article to Basil Howell for his generous support of the author’s legal and business education. Catherine M. Barrett is a former Congressional legislative specialist for Weil, Gotshal and Manges, LLP and is currently a JD/MBA candidate at the American University Washington College of Law.

[1]. The FBI describes Carnivore as a “diagnostic tool,” a device that provides the FBI with a “surgical” ability to intercept and collect the communications that are the subject of a lawful search order. Federal Bureau of Investigations, The Carnivore Diagnostic Tool, *at*

http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited November 14, 2001).

[2]. *See Internet and Data Interception Capabilities Developed by the FBI, Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division of the FBI), *at* http://www.fbi.gov/congress/congress00/kerr072400.htm (Sept. 6, 2000). Assistant Director of the Laboratory Division of the FBI Donald M. Kerr testified that the FBI performs interceptions of criminal wire and electronic communications, including Internet communications, pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), and portions of the Electronic Communications Privacy Act of 1986 ("ECPA"). Kerr testified that under Title III, applications for interception of wire and electronic communications require the authorization of a high-level DOJ official before the local United States Attorneys' offices can make an application for a warrant to a federal court. *See id.*

[3]. *See Carnivore and the Fourth Amendment, Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (statement of Kevin V. DiGregory, Deputy Associate Attorney General, Criminal Division of the Department of Justice), *at* http://www.house.gov/judiciary/digr0724.htm (July 24, 2000).

[4]. *See* U.S. Telecom Ass'n v. Fed. Communications Comm'n, 227 F.3d 450, 454 (D.C. Cir. 2000).

[5]. *See* United States v. Cortez, 449 U.S. 411, 417-18 (1981). The Supreme Court set forth the following test for determining reasonable suspicion:

> the whole picture must be taken into account. Based upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person. [P]articularized suspicion contains two elements, each of which must be present: First, the assessment must be based upon all the circumstances. The analysis proceeds with various objective observations, [such as] information from police reports; [The] second element contained in the idea that an assessment of the whole picture must yield a particularized suspicion is the concept that the process just described must raise a suspicion that the particular individual being stopped is engaged in wrongdoing. *Id*.

In contrast, a search for law enforcement purposes requires probable cause and cannot be satisfied by reasonable suspicion.

[6]. *See* 18 U.S.C.§ 2511 (2000)(contemplating the interception of content over various media).

[7]. *See* 18 U.S.C. § 2510 (8)(2000).

[8]. *See generally* U.S. v. Miller, 425 U.S. 435 (1976).

[9]. Carol v. United States, 267 U.S. 132, 162 (1925).

[10]. *See Cortez*, 449 U.S. 411.

[11]. *See* 18 U.S.C. § 3123 (2000). According to this statute, which governs the issuance of a pen register order and trap-and-trace device, the court shall authorize the installation and use of a pen register or a trap-and-trace device if the court finds that the government official has certified to the court that the

information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. 18 U.S.C. § 3123(b)(1) notes the content of an order shall specify:

> (A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap-and-trace device is to be attached;(B) the identity, if known, of the person who is the subject of the criminal investigation;(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap-and-trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap-and-trace device under subsection (a)(2), the geographic limits of the order; and (D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

[12]. Natural rights are grounded in a political theory that maintains that an individual enters into society with certain basic rights and that no government can deny these rights. Columbia University Press, The Columbia Encyclopedia, *Natural Rights* (6th ed. 2001), *at* http://www.bartleby.com/65/na/natrlrig.html (last visited November 18, 2001).

[13]. There are two additional Constitutional Amendments that have been interpreted to provide some form of privacy rights. The First Amendment "imposes limitations upon governmental abridgement of 'freedom to associate and privacy in one's associations'." Katz v. United States, 389 U.S. 347, 351 (1967) (citing NAACP v. Alabama, 357 U.S. 449, 464 (1958)). In addition, the Third Amendment prohibits the peacetime quartering of soldiers, thereby protecting a right to privacy in one's home from uninvited governmental intrusion. *See id*.

[14]. U.S. Const., amend. IV.

[15]. *See* Katz, 389 U.S. at 350.

[16]. Barbara A. Dooley & Ronald L. Plesser, Commercial Internet eXchange Association, *The Legal Standard for Government Tracing of Internet Communications: The Misuse of Pen Register Court Orders for Real-Time Acquisition of Transactional Information* 4-5 (October 2000), *available at* http://www.carnivorewatch.org/documents.html (last visited February 13, 2002) (emphasis added).

[17]. Katz, 389 U.S. at 353.

[18]. *Id.*

[19]. *Id.* at 361 (Harlan, J., concurring).

[20]. The second element turns on "whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment." LaFollette v. Commonwealth, 915 S.W.2d 747, 749 (Ky. 1996)*(*citing Oliver v. United States, 466 U.S. 170, 182-83 (1984)).

[21]. Katz, 389 U.S. at 351.

[22]. *Id.* at 361 (Harlan, J., concurring).

[23]. 388 U.S. 41, 59 (1967). For further clarification, *see* 18 U.S.C. § 2518(1) (2001). According to the

statute, a law enforcement agent's application for a wiretap warrant must state: (a) the identity of the officers making and authorizing the request; (b) the complete facts and circumstances the officer believes justify the interception, including details about the alleged offense, a description of the types of communications to be intercepted, and the identity of the person allegedly committing the offense and whose communications are to be intercepted, (c) a complete description of whether other investigative techniques have been attempted or why they shouldn't be attempted; (d) the period of time the interception will be conducted; and (e) whether there have been previous applications and what action a judge took on those applications.

[24]. *See* U.S. Telecom Ass'n v. Fed. Communications Comm'n, 227 F.3d 450, 454 (D.C. Cir. 2000).

[25]. Berger, 388 U.S. at 55.

[26]. *Id.* at 59.

[27]. *Id.* at 55.

[28]. 425 U.S. 435, 442 (1970) (The defendant was convicted of possessing an unregistered still, carrying on the business of a distiller without giving bond, intending to defraud the Government of whiskey tax, and possessing whiskey upon which no tax had been paid. The defendant moved to suppress copies of checks and other bank records obtained by means of allegedly defective subpoenas).

[29]. *Id.*

[30]. *Id. Cf.* Boyd v. United States, 116 U.S. 616, 622 (1886) (describing the Fourth Amendment as providing protection against "compulsory production of a man's private papers.") *Miller* is distinguished from *Boyd* in that banking records are not private papers and are therefore not entitled to the protections afforded private papers under the Fourth Amendment.

[31]. *Miller*, 425 U.S. at 442 (citing *Katz*, 389 U.S. at 351).

[32]. 442 U.S. 735, 745-46 (1979). *Cf.* United States v. Byrd, 31 F.3d 1329 (5th Cir. 1994). In determining whether probable cause exists, "a magistrate must make a practical, common-sense decision as to whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id*. at 1340 (citing *United States v. Peden*, 891 F.2d 514, 518 (5th Cir. 1989)).

[33]. *Smith*, 442 U.S. at 743-44 (1979) (Defendant sought to suppress all the recorded telephone numbers derived from the pen register on the ground that the police had failed to secure a warrant prior to its installation).

[34]. *Id.* at 745.

[35]. *Id.* at 745-46.

[36]. Dooley, *supra* note 16, at 10-11; *see also* 18 U.S.C. §§ 2703(c)(1)(B)(ii), 2703(d) (2001).

[37]. *Smith*, 442 U.S. at 738.

[38]. *Id.* at 741.

[39]. *Id.*

[40]. *Id.* at 742.

[41]. *See id.* at 743. The Court reasoned that it has consistently found that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. *Id*. at 744. *See also United States v. Miller* 425 U.S. 435, discussed *supra* note 28.

[42]. *See Smith*, 442 U.S. at 745-56.

[43]. *See generally,* 533 U.S. 27 (2001) (Plaintiff was accused and convicted of growing marijuana in his home based in part on information police gathered by using a thermal imaging device—a device that converts thermal radiation to fuzzy images of black and gray based upon relative warmth).

[44]. *Kyllo,* 121 S.Ct. at 2045.

[45]. *See Id.* at 2043-2044.

[46]. *Id.* at 2043.

[47]. *See* Letter from Representative Dick Armey, Majority Leader, United States House of Representatives, to John Ashcroft, United States Attorney General, Department of Justice, (June 14, 2001) *available at* http://www.freedom.gov/library/technology/ashcroftletter.asp (last visited June 20, 2001).

[48]. *See* United States Telecom Ass'n v. Fed. Communications Comm'n, 227 F.3d 450, 466 (D.C. Cir. 2000).

[49]. *Id*. at 463.

[50].*Id.* at 456.

[51]. *Id.* at 465.

[52]. *See* People v. Bialostok, 610 N.E.2d 374, 376-77 (N.Y. 1993).

[53]. See *supra* section I(A).

[54]. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., *concurring*).

[55]. Erik G. Luna, *Sovereignty and Suspicion*, 48 DUKE L.J. 787, 794 (1999).

[56]. *See* United States v. Pinson, 24 F.3d 1056, 1059 (8th Cir. 1994).

[57]. *Id.* at 1056.

[58]. *Pinson*, 24 F.3d at 1059.

[59]. *Id.*

[60]. Joy Archer Yeager, *Permissibility and Sufficiency of Warrantless Use of Thermal Imager or Forward Looking Infra-Red Radar (F.L.I.R.)*, 78 A.L.R.5th 309 (2000) at 13 (citing U.S. v. Pinson, 24 F.3d 1056 (8th Cir. 1994)).

[61]. *But see United States v. Cusumano*, 67 F.3d 1497 (10th Cir. 1995) ((1) defendants had subjective and reasonable expectation that government would not have access to heat signatures of activities within their home; thus, thermal imaging was subject to warrant requirement; (2) heat signatures of activities were not within the "plain view" exception to warrant requirement; and (3) affidavit was sufficient to support search warrant, even excluding tainted evidence obtained from thermal imager).

[62]. *See* 18 U.S.C. § 2516(1). The Attorney General or any Assistant Attorney General may authorize an application for a wiretap to a Federal Judge, and the judge may grant authority to intercept the transmissions. *Id.*

[63]. *See* 18 U.S.C. § 2518(3). Pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, a judge issuing a warrant for surveillance of communication content must find that: normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and that there is probable cause for believing that an individual is committing, has committed, or is about to commit to one of a list of specifically enumerated crimes, that the wiretap will intercept particular communications about the enumerated offense, and that the communications facilities to be tapped are either being used in the commission of the crime or are commonly used by the suspect. *Id.*

[64]. *See* 18 U.S.C. § 2518(1). A law enforcement agent's application for a Title III warrant must state: (1) the identity of the officers making and authorizing the request; (2) the complete facts and circumstances the officer believes justify the interception, including details about the alleged offense, a description of the types of communications to be intercepted, and the identity of the person allegedly committing the offense and whose communications are to be intercepted; (3) a complete description of whether other investigative techniques have been attempted or why they shouldn't be attempted; (4) the period of time the interception will be conducted; and (5) whether there have been previous applications and what action a judge took on those applications. *Id.*

[65]. *See* 18 U.S.C. § 3123. This statute governs the issuance of an order for a pen register or a trap-and-trace device by requiring the court to authorize the installation and use of a pen register or a trap-and-trace device only if the government official has certified to the court that the information likely to be obtained is relevant to an ongoing criminal investigation. 18 U.S.C. § 3123(b)(1) specifies that an order provide:

> (A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap-and-trace device is to be attached; (B) the identity, if known, of the person who is the subject of the criminal investigation; (C) the number and, if known, physical location of the telephone line to which the pen register or trap-and-trace device is to be attached and, in the case of a trap-and-trace device, the geographic limits of trap-and-trace order; and (D) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates. *Id.*

[66]. 18 U.S.C. § 3123(a); *See also The Fourth Amendment and the Internet: Before the House Comm.*

on the Judiciary Subcomm. on the Constitution, 106th Cong. (2000) (statement of Robert Corn-Revere, Partner, Hogan & Hartson L.L.P) *available at* http://www.house.gov/judiciary/corn0724.htm (last visited April 19, 2001). Mr. Corn-Revere's statement and insight have been utilized throughout this comment.

[67]. *See* DiGregory, *supra* note 4.

[68]. 18 U.S.C. § 1001(2). This statute defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." *Id.*

[69]. U.S. Telecom Ass'n v. Fed. Communications Comm'n, 227 F.3d 450, 455 (D.C. Cir. 2000) (citing H.R. Rep. No. 103-827, pt. 1 at 9 (1994)).

[70]. 47 U.S.C. § 1001(8)(C)(i) (excluding providers of "information services" from the definition of "telecommunications carrier").

[71]. *See* 18 U.S.C. § 3123.

[72]. The Department of Justice ("DOJ") tried to curb criticism of Carnivore last year by attempting to contract with several prominent universities to conduct an independent technical capability review of Carnivore. The DOJ hoped that these universities, which included computer-security experts at the Massachusetts Institute of Technology ("MIT"), the University of Michigan, and the University of California at San Diego among others, would conduct an independent review of the technical capabilities of Carnivore. However, these universities refused the DOJ's offer, noting that the number of restrictions placed on the reviewers and the review process would, in fact, not produce an independent review. According to Jeffery I. Schiller, network manager at MIT, the DOJ wanted to "borrow a university's reputation" to validate the FBI's use of the Carnivore system. Andrea L. Foster, *Universities Reject Opportunity to Screen Internet-Wiretapping System,* The Chronicle of Higher Education, *at* http://chronicle.com/free/2000/09/2000091501t.html (last visited September 15, 2000). Schiller further noted that DOJ would have veto power over members of the review team. *Id.*

[73]. Stephen P. Smith & J. Allen Crider, IIT Research Institute, Independent Technical Review of Carnivore Draft Report 3-14, 4-3 (Nov. 17, 2000) *at* http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (last visited June 24, 2001).

[74]. *The Fourth Amendment and the FBI's Carnivore Program: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Michael O'Neill, assistant professor, George Mason University School of Law) *at* http://www.senate.gov/~judiciary/962000_mo.htm (last visited April 19,

2001).

[75]. *The Fourth Amendment and the FBI's Carnivore Program: Hearing Before the Senate Judiciary Comm.*, 106th Cong. (2000) (statement of Jeffrey Rosen, associate professor, George Washington University School of Law) *at* http://www.senate.gov/~judiciary/962000_jr.htm (last visited April 19, 2001).

[76]. *Id.*

[77]. *Id.*

[78]. *The Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (statement of Robert Corn-Revere, partner in the office of Hogan & Hartson L.L.P) *at* http://www.house.gov/judiciary/corn0724.htm (last visited April 19, 2001)(citing Report of the President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet 37(2000)).

[79]. The FBI maintains that, like telephone numbers recorded by pen registers and trap-and-trace devices, Carnivore tracks, copies and records the numbers associated with Internet activity. The FBI has consistently denied that Carnivore "reads" e-mail content or other Internet content. *See* Federal Bureau of Investigations, The Carnivore Diagnostic Tool, *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited November 14, 2001). If the FBI is accurate in its assertions, a lower level of privacy would apply to such transactional information. However, if Carnivore does record content information, then the government is obligated under the Fourth Amendment to secure a warrant grounded in probable cause *prior* to the use of Carnivore.

[80]. Katz v. United States, 389 U.S. 347, 361 (1967)(Harlan, J., concurring).

[81]. *Id.*

[82]. *The Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (statement of Robert Corn-Revere, Hogan & Hartson L.L.P) *at* http://www.house.gov/judiciary/corn0724.htm (last visited April 19, 2001).

[83]. *Id.*

[84]. The Court reasoned that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[85] *See, e.g.*, Payton v. New York, 445 U.S. 573, 589-90 (1980) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

[86]. Lopez v. United States, 373 U.S. 427, 471 (1963) (Brennan, J., dissenting)(citing Frank v. Maryland, 359 U.S. 360, 362 (1959)).

[87]. RICHARD ALLEN EPSTEIN, PRINCIPLES FOR A FREE SOCIETY: RECONCILING INDIVIDUAL LIBERTY WITH THE COMMON GOOD, 210 (1998).

[88]. *See id.*

[89]. THOMAS A. PETERS, COMPUTERIZED MONITORING AND ONLINE PRIVACY 121 (1999).

[90]. *Id.*

[91]. *Id.* at 122.

[92]. JOHN STUART MILL, ON LIBERTY AND OTHER ESSAYS 17 (Oxford University Press 1991) (1869).

[93]. PETERS, *supra* note 90 at 122.

[94]. *Id.* at 130.

[95]. *Id.*

[96]. Libertarians believe that every person has free will and is therefore the master of his actions. David Boaz, Libertarianism: A primer 33 (1997). Libertarianism is a political philosophy defined by basic principles of liberalism, which include the idea of a higher law or natural law, the dignity of the individual, natural rights to liberty and property, and the social theory of spontaneous order. Specific ideas flow from these fundamentals: individual freedom, limited and representative government, free markets. *Id.* 41-2. The term "natural rights" means rights not granted by any other human. They are not granted by government; people form governments in order to protect the rights they already possess. *Id.* 64. Natural rights theory "asserts that the end of the state is to protect liberty and property, as these conceptions are understood independent of and prior to the formation of the state." Richard Allen Epstein, *A Tale of Two Pies*, *in* Liberty, Property and the Law: Constitutional Protection of Private Property and Freedom of Contract, 287 (2000).

[97]. CHARLES MURRAY, WHAT IT MEANS TO BE A LIBERTARIAN, 28 (1997).

[98]. PETERS, *supra* note 90, at 127.

[99]. *Id*.

[100]. *Id*.

[101]. *Id*.

[102]. *See* The Columbia Encyclopedia (6th ed. 2001), *at* http://www.bartleby.com/65/na/natrlrig.html (last visited March 15, 2001). “The modern idea of natural rights grew out of the ancient and medieval doctrines of natural law, i.e., the belief that people, as creatures of nature and God, should live their lives and organize their society on the basis of rules and precepts laid down by nature or God. With the growth of the idea of individualism, especially in the 17th cent., natural law doctrines were modified to stress the fact that individuals, because they are natural beings, have rights that cannot be violated by anyone or by any society.” *Id.* Among "the classic expressions of natural rights are the English Bill of Rights (1689), the American Declaration of Independence (1776), the French Declaration of the Rights of Man and the Citizen (1789), the first 10 amendments to the Constitution of the United States (1791)." *Id*.

[103]. Epstein, *supra* note 87 at 287.

[104]. *Id*. 287-88. (stating that the "same applies to property; trespass is not wrong because the state prohibits it; it is wrong because individuals own private property. None of these rules rests entitlements on the state, which only enforces the rights and obligations generated by theories of private entitlement.”).

[105]. *See* United States v. Byrd, 31 F.3d 1329, 1340 (1994) (determining whether probable cause exists, “a magistrate must make a practical, common-sense decision as to whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place.”)

[106]. *See* United States v. Cusumano, 67 F.3d 1497, 1500 (1995).

[107]. *Internet and Data Interception Capabilities Developed by the FBI: Before the House Comm. on*

the Judiciary Subcomm. on the Constitution, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division of the FBI) *at* http://www.fbi.gov/congress/congress00/kerr072400.htm (last visited April 18, 2001).

[108]. *Id*.

[109]. *See* 18 U.S.C. § 2518(7) (2001). This statute permits law enforcement to circumvent the probable cause standard requirement for the use of electronic surveillance if the Attorney General determines that an emergency exists in which national security is compromised or there is an "immediate danger of death or serious physical injury." *Id*. *See also* The Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801*et seq*. (2001) (providing for electronic surveillance of foreign powers and agents of foreign powers in the United States for the purpose of obtaining foreign intelligence information).

[110]. *Internet and Data Interception Capabilities Developed by the FBI, Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division of the FBI), *at* http://www.fbi.gov/congress/congress00/kerr072400.htm (Sept. 6, 2000).

[111]. Lopez v. United States, 373 U.S. 427, 464 (1963).

[112]. Berger v. New York, 388 U.S. 41, 63 (1967).

Related Browsing

1. http://www.fbi.gov/hq/lab/carnivore/carnivore.htm
Official statement of the Federal Bureau of Investigation to the US House of Representatives regarding Carnivore Diagnostic Tool. The FBI is sharing information regarding Carnivore with industry to assist them in their efforts to develop open standards for complying with wiretap requirements.

2. http://www.howstuffworks.com/carnivore.htm
In depth narrative explains what exactly the FBI's Carnivore is, where it came from, how it works.

3. http://news.cnet.com/news/0 1005 200 4769965.html
Carnivore now goes by the less beastly moniker of DCS1000, drawn from the work it does as a "digital collection system." The Illinois Institute of Technology released its analysis of the FBI's controversial email surveillance system, concluding that Carnivore technology "protects privacy and enables lawful surveillance better than alternatives."

4. http://www.aclu.org/action/carnivore107.html
An "action alert' from the ACLU. Send a free fax to "urge Congress to stop the FBI's use of

privacy-invading software."

5. http://www.theregister.co.uk/content/6/14940.html
A critical review of a report on Carnivore. The report was prepared by the IIT Reasearch Institute and the Illinois Institute of Technology Chicago-Kent College of Law under contract to the US Department of Justice.

6. http://www.epic.org/privacy/carnivore/review_comments.html
Independent Technical Review of Carnivore System by the Electronic Privacy Information Center.

7. http://cdt.org/security/carnivore/
Center for Democracy and Technolgy website contains news articles, senate and house judiciary committee hearing transcripts, and independent review of Carnivore.

8. http://www.cnn.com/2000/ALLPOLITICS/stories/09/06/carnivore.hearing/
Article - "Senate Panel Examines FBI Internet Surveillance System."

9. http://www.usdoj.gov/criminal/cybercrime/searching.html
Department of Justice website on Computer Crime and Intellectual Property Section.

10. http://www.fcw.com/fcw/articles/2001/0910/pol-carn-09-10-01.asp
Federal Computer Week - article "FCC Mulls Carnivore and Wireless." Will the Carnivore system spread to wireless communication.

11. http://usgovinfo.about.com/library/news/aa071300b.htm?iam=dpile&terms
Article - "Carnivore No Threat to Privacy FBI Says." The FBI defends its Carnivore e-mail scanning system against claims that it violates civil liberties.

12. http://netsecurity.about.com/library/weekly/aa101501a.htm
Article: "Privacy, Freedom & Security: Terrorist Attacks On The US May Change Our Concept Of Privacy." Discussing the FBI's attempts to broaden the scope and usage of Carnivore as a result of the September 11th attacks on America.

13. http://www.stopcarnivore.org/
Website providing links to news and articles about Carnivore, and information about what Carnivore is, what Carnivore should do, why Carnivore is bad.

14. http://www.eff.org/Privacy/Surveillance/Carnivore/
EFF "Surveillance: Carnivore & Internet Surveillance" Archive.

15. http://www.tilj.com/content/litigationheadline07100101.htm
Article: Does the FBI's Carnivore System Violate the Constitution?

16. http://www.zdnet.com/zdnn/stories/news/0,4586,2657115,00.html?chkpt=zdhpnews01
Article: FBI could abuse Carnivore.

17. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48349,00.html
Statement from ACLU Associate Director.

18. http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf
Independent Review of the Carnivore System - Draft Report by the IIT Research Institute (November 17, 2000).

19. http://www.alternet.org/story.html?StoryID=11520
Article: TECHSPLOITATION: How 9-11 Will Change Cyberspace.

20. http://www.house.gov/judiciary/con07241.htm
Witness list for Oversight Hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program."

21. http://www.carnivorewatch.org/
a web site dedicated to promoting public awareness of the FBI's Carnivore e-mail surveillance system (recently renamed "DCS1000").

22. http://www.wired.com/news/politics/0,1283,46747,00.html
Federal police are reportedly increasing Internet surveillance after Tuesday's deadly attacks on the World Trade Center and the Pentagon.

23. http://www.cnn.com/2000/TECH/computing/07/21/fbi.carnivore/
FBI says Carnivore will not devour privacy because it is equivalent to a telephone wiretap.

24. http://www.zdnet.com/zdnn/stories/news/0,4586,2601502,00.html
The US Federal Bureau of Investigation is using a superfast system called Carnivore to covertly search e-mails for messages from criminal suspects.

25. http://abcnews.go.com/sections/tech/DailyNews/carnivore001128.html
Article: How Big is Carnivore's Bite? Senate Panel Presses FBI for E-Mail Surveillance Tool Data.

26. http://www.matrix.net/publications/mn/mn1010_the_fbi_and_carnivore.html
Society must have the will to apply the basic precepts and protections of our cultures to the Internet. We must not be seduced into permitting these basic concepts to be undermined by technological details or related diversionary tactics in any environments, either on or off the Internet.

27. http://www.business2.com/articles/web/0,1653,15378,00.html
FBI Renames Carnivore, but email watching plan still faces fire.

28. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci508347,00.html
Definition of Carnivore.

29. http://www.pcworld.com/news/article/0,aid,18094,00.asp
FBI Offers Carnivore Data (Slowly). Privacy groups want information faster, under Freedom of Information Act request.

30. http://www.mropinion.com/index.cfm?PollID=66
Technology Poll: Do you think that the FBI's Carnivore email system, which reads through emails to see if they contain any terrorist efforts, violates individuals' privacy?

31. http://www.infowar.com/class_1/00/class1_071200a_j.shtml

Newsbytes Article: FBI Defends 'Carnivore' Cyber Snoop Device.
