I. THE DEBATE SURROUNDING CARNIVORE AND ITS PERCEIVED THREAT TO FOURTH AMENDMENT RIGHTS AS IT APPLIES TO INTERNET COMMUNICATIONS

The Fourth Amendment to the United States Constitution explicitly provides individuals the right to be secure from unreasonable searches and seizures. This right to privacy is not absolute, as courts have established certain exceptions to the rule that all searches and seizures must be conducted with a court-issued warrant. For example, the Supreme Court has found that while there is a right to privacy in the contents of telephone calls, there is no right to privacy in telephone call records. Indeed, the Constitution is celebrated in part because of the Founders' intent that it be applied and construed in a flexible manner with the ability to adapt to changing circumstances. However, technology ushered in with the new millennium has brought to fruition the fears that Justice Brandeis articulated in 1928 that "[w]ays may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." More specifically, the flexible approach in delineating the extent of privacy rights under the Fourth Amendment combined with the explosion of the Internet as a unique communications medium has brought society to a crossroads where serious Fourth Amendment policy decisions must be determined.

In today's world of electronic life, the advancement of the Internet has facilitated the unfortunate development of a new area of criminal activity. As a result, issues remain unresolved concerning the application of constitutional rights to online activities, especially the privacy and security of Internet communications. The fact that existing statutes governing electronic surveillance are ill-suited to the Internet is particularly pertinent when one considers Carnivore, the against that which may become an evil. Id. "Time works changes, brings into existence new conditions and purposes. Therefore, a principal to be vital must be capable of wider application than the mischief which gave it birth." Id. at 472-73.

1 U.S. Const. amend. IV ("[T]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").


4 See Smith, 442 U.S. at 745-46.

5 See Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting). ([G]eneral limitations on the powers of government . . . do not forbid . . . meeting modern conditions by regulations which 'a century ago, or even half a century ago, probably would have been rejected as arbitrary and oppressive.' Clauses guaranteeing to the individual protections against specific abuses of power, must have a similar capacity of adaptation to a changing world.). Constitutional protections should not be limited to guarding against existing evils because to be perpetual, they must also protect

6 Id. at 475.


9 See Davidson, supra note 7.
FBI's new Internet wiretapping system. Privacy rights are threatened because as the law stands now, Internet communications receive minimal Fourth Amendment protection. The tremendous advancements in Internet technology that encourage the widespread transfer of private data have greatly affected law enforcement because more information is available that could prove to be valuable evidence in government investigations. Moreover, advanced technology has allowed law enforcement to develop improved methods and devices to track electronic communications. For example, with a court order, the FBI can use Carnivore to monitor and record the Internet traffic of suspected criminals in order to collect evidence. Carnivore possesses the ability to scan millions of e-mail messages per second—an alarming development because it may include access to more data than what is legally permissible under current law. Meanwhile, the public has little knowledge of Carnivore's full capabilities and civil rights groups are demanding a public review of the system's source code. Specifically, advocates of Fourth Amendment rights argue that electronic surveillance of Internet communications should not come at the expense of constitutional rights to privacy. Conversely, the FBI and DOJ rehash the argument that severe restrictions on Carnivore's uses will "make society suffer and give criminals greater immunity than has been known heretofore." This comment examines the government's new electronic surveillance device known as Carnivore, in particular, its effect on the Fourth Amendment's protection against unreasonable searches and seizures. First, this comment establishes that Fourth Amendment jurisprudence restricts the government's ability to use surveillance tools to intercept information contained in private communications. Next, this comment asserts that Carnivore threatens to exceed the bounds of permissible government surveillance of private Internet communications. Finally, this comment concludes that Congress must redefine the balance between an individual's Fourth Amendment rights and the needs of law enforcement by strengthening the statutory framework pertaining to electronic surveillance of private Internet communications.

II. THE FOURTH AMENDMENT AND FEDERAL LAW

A. Olmstead v. United States: Fourth Amendment Implications of Wiretapping

1. Olmstead Majority View

Olmstead v. United States was the first case that discussed the permissible scope of wiretapping in the Fourth Amendment context. The broad issue that the Supreme Court considered was whether evidence obtained through telephone wiretaps constituted a violation of the Fourth Amendment. In convicting Olmstead, the government had relied on information obtained

---

\[10\] See id. To date, Carnivore has not been implicated in an actual case of a Fourth Amendment violation, but the threat of a potential violation is substantial enough to make examining this issue worthwhile.

\[11\] See id.

\[12\] See id.

\[13\] See id.

\[14\] See Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program: Oversight Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong., at http://www.house.gov/judiciary/corn0724.htm (2000) (testimony of Robert Corn-Revere, Partner, Hogan & Hartson, LLP) [hereinafter Corn-Revere] (expressing concern that Carnivore will be able to capture the content or headers of e-mail messages from both the targeted user and other peripheral users exceeding the permissible scope of a trap and trace order); see also Davidson, supra note 7. Proponents argue that using Carnivore to obtain such information as e-mail contents or headers is analogous to a pen register or trap and trace device that can be obtained under a low legal standard, but opponents argue it is equivalent to a wiretap, which requires a showing of probable cause and includes judicial oversight.

\[15\] See Davidson, supra note 7.

\[16\] See D. I. Hopper, An Internet 'Carnivore,' ABCNEWS.com, at http://www.abcnews.go.com/sections/tech/dailynews/carnivore000727.html (July 27, 2000)" (["T"]he concept of an 'incidental' search cannot readily be extended to include surreptitious surveillance of an individual either immediately before, or immediately after, his arrest." (citing United States v. Rabinowitz, 339 U.S. 56, 71–79 (1950) (Frankfurter, J., dissenting))). Exceptions to Fourth Amendment protections include searches and seizures conducted incidental to the arrest or in hot pursuit. Katz, 389 U.S. at 358.

\[18\] Olmstead, 277 U.S. at 468; see also Kerr, supra note 8 (noting that lawful electronic surveillance is an important tool because it allows law enforcement entities to collect and present evidence of the suspect's own words).

\[19\] 277 U.S. 438.

\[20\] Olmstead, 277 U.S. at 438.

\[21\] Id. at 455–56. Private telephone conversations between the defendant and others led to a conviction for conspiring to violate the National Prohibition Act. The defendants were convicted of unlawfully possessing, transporting, importing and selling intoxicating liquors. Defendants ran a lucrative
from telephone conversations intercepted with wiretaps.\textsuperscript{22} The intercepted phone conversations revealed the nature of the defendant's illegal activity, including the identity of partners, subordinates and customers.\textsuperscript{23} The information obtained by government officials formed the basis for an indictment and subsequent conviction for criminal conspiracy.\textsuperscript{24}

Chief Justice Taft, writing for the \textit{Olmstead} majority, recounted the basis of Fourth Amendment case law.\textsuperscript{25} Chief Justice Taft's discussion included \textit{Weeks v. United States},\textsuperscript{26} in which the Court held that a search or seizure without a warrant violates the Fourth Amendment.\textsuperscript{27} Most evidence obtained without a warrant is inadmissible and must be returned to the aggrieved party.\textsuperscript{28} Without such a rule, the \textit{Weeks} Court held that the Fourth Amendment would be meaningless and ineffective in protecting individual liberties.\textsuperscript{29} The \textit{Olmstead} Court considered this rule in light of the fact that the defendants had made continued and voluntary use of their telephones without knowing about the wiretaps that the government officials had used to intercept their conversations.\textsuperscript{30} In contrast to previous Fourth Amendment cases, \textit{Olmstead} presented a situation in which there was no actual entry into a defendant's private home or office, and no tangible items were seized or searched.\textsuperscript{31}

Based on the distinction that telephone conversations are unlike pieces of mail, which are tangible personal effects and to which the Fourth Amendment provides protections, the \textit{Olmstead} Court held that the evidence obtained by wiretapping defendants' telephones did not violate the Fourth Amendment.\textsuperscript{32} The Court refused to find that the wiretaps involved a search or seizure because there was no actual entry onto defendant's private property.\textsuperscript{33} The Court did note, however, that Congress has the power to make a law banning the admission into evidence of intercepted telephone conversations.\textsuperscript{34} Courts have no such power and in the absence of such a law, they could not find the government's actions in \textit{Olm-
stead to be in violation of the Fourth Amendment. Therefore, Chief Justice Taft reasoned that the Court could not expand unilaterally the Fourth Amendment's scope to include searches and seizures of intangible material that is freely available outside the home. The ultimate result in Olmstead was a declaration that, within the rule set out in Weeks v. United States, using a wiretap without a warrant is constitutional.

2. Olmstead Dissent

Justice Brandeis dissented from the majority's view in Olmstead and wrote that the government's wiretapping constituted an unreasonable search and seizure in violation of the Fourth Amendment. Justice Brandeis cast the issue as whether the wiretapping constituted a search and seizure within the meaning of the Fourth Amendment. An affirmative answer would make wiretapping, in the absence of a warrant, unlawful and would have the effect of making evidence obtained with a wiretap inadmissible.

Justice Brandeis wrote that the Founders designed the Constitution to last for eternity and intended it to have the "capacity of adaptation to a changing world." Brandeis reasoned that the Founders knew that unanticipated threats to constitutional rights would arise; therefore, they had intended that the Constitution be flexible so that it could remain an effective protection against both present and future threats to individual liberties. In keeping with the Founder's intent, Justice Brandeis stressed that Supreme Court precedent "in giving effect to the principle underlying the Fourth Amendment, has refused to place an unduly literal construction upon [the Fourth Amendment]." In this light, the wiretapping in Olmstead presented only one of many new methods by which the government might be more capable of infringing on personal liberties. Therefore, according to Brandeis' dissent in Olmstead, courts must fulfill the Founders' primary goal of preserving the essence of the Fourth Amendment's protection of personal liberties against government infringements, no matter what their form.

Brandeis also argued that when considering the degree of Fourth Amendment protection to afford telephone conversations, such conversations are analogous to pieces of mail. Both telephone and mail services are publicly available means of communication, however, "the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed, and the other unsealed, but these are distinctions without a difference." Therefore, to preserve the principles underlying the Fourth Amendment and to maintain its effectiveness, courts should find a violation of Fourth Amendment rights whenever the government intrudes unjustifiably on an individual's privacy, even when there is no physical seizure of personal effects. Brandeis' dissent stressed that an infringement of Fourth Amendment rights is inexcusable even when government is performing law enforcement duties because "[e]xperience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent." If the cost is the loss of individual liberties, Brandeis believed that it is better that some criminals go free rather than all criminals be caught by government encroachment on Fourth Amendment rights.

35 Id. at 466.
36 Id. (holding that telephone use involves passing messages outside the home and thus is outside the scope of Fourth Amendment protection).
37 Id. at 465.
38 Id. at 478 (Brandeis, J., dissenting).
39 Id. at 471-72 (Brandeis, J., dissenting).
40 Id. (Brandeis, J., dissenting).
41 Id. at 472-73 (Brandeis, J., dissenting) (relying on Weeks v. United States, 217 U.S. 349, 373 (1910), for the idea that the Constitution "must be capable of wider application" and "should not, therefore, be necessarily confined to the form that evil had theretofore taken").
42 Id. (Brandeis, J., dissenting) ("Time works changes, brings into existence new conditions and purposes . . . . [S]o our contemplation cannot be only of what has been but of what may be." (quoting Weeks, 217 U.S. at 373)).
43 Id. at 474, 476 (Brandeis, J., dissenting) (noting that the principles underlying the Fourth Amendment "apply to all invasions on the part of the government . . . . of the sanctities of a man's home and the privacies of life") (quoting Boyd v. United States, 116 U.S. at 616).
44 Id. at 473 (Brandeis, J., dissenting).
45 Id. at 475 (Brandeis, J., dissenting) (relying on Boyd, 116 U.S. at 616).
46 Id. (Brandeis, J., dissenting).
47 Id. (Brandeis, J., dissenting).
48 See id. (Brandeis, J., dissenting) (citing Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920) (holding that an officer's reading of a private paper is a Fourth Amendment violation even though the officer did not seize or touch the paper, and therefore the paper is inadmissible as evidence)).
49 Id. at 479 (Brandeis, J., dissenting).
50 Id. (Brandeis, J., dissenting).
Justice Butler also dissented in Olmstead, finding the government's use of a wiretap without a warrant to be a violation of the Fourth Amendment. Justice Butler saw the issue as whether the government could, in keeping with the Fourth Amendment, intercept private telephone conversations without a warrant. In reaching this conclusion, Justice Butler rejected the government's claim that wiretaps do not constitute a search for evidence. Justice Butler interpreted liberally the Fourth Amendment's protection of individual liberties, finding that wiretaps violate individual constitutional rights.

B. Katz v. United States: Warrantless Wiretaps Violate the Fourth Amendment

Nearly forty years passed before the Supreme Court reconsidered its position in Olmstead on the permissible scope of wiretapping under the Fourth Amendment. In Katz v. United States, petitioner was indicted for violating a federal statute forbidding the transmission of wagering information by telephone. The conviction turned on the government's introduction of evidence by using an electronic listening and recording device. The recordings were of Katz's side of telephone conversations made from a public telephone booth. Katz presented two vital questions for Supreme Court review. One issue was whether, under the Fourth Amendment, a public telephone booth is a constitutionally protected area requiring the government to obtain a warrant before recording telephone conversations made from the booth. The second issue was whether, under the Fourth Amendment, physical intrusion of a protected area is a necessary element in establishing an unconstitutional search and seizure. The Court stated that "the Fourth Amendment protects people, not places," and "what [Katz] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." The government claimed that because the telephone booth was constructed of transparent glass, Katz was as visible inside as he would have been outside the booth. The Court found this assertion irrelevant because the purpose of entering the enclosed telephone booth was to preserve the privacy of the spoken word and not to prevent visibility. Moreover, the Court held that a person carries with them into a public telephone booth the full panoply of Fourth Amendment protections.

The government also asserted that even if a person in a public telephone booth carries with them Fourth Amendment rights, these rights were not implicated because the recording device did not involve a physical intrusion of the booth. Based on Olmstead, this argument stated that Fourth Amendment protections are not implicated when there is no search or seizure of tangible effects. In finding no merit to this argument by the government, the Katz Court stated that "the underpinnings of Olmstead and Goldman have been so
eroded... [that they] can no longer be regarded as controlling.\textsuperscript{68} Subsequent cases "have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any technical trespass."\textsuperscript{69} This proclamation makes the presence or absence of a physical intrusion irrelevant to the consideration of whether a search or seizure violates the Fourth Amendment.\textsuperscript{70} As a result, the Court held that recording Katz's phone conversations made from the public telephone booth "constituted a search and seizure within the meaning of the Fourth Amendment."\textsuperscript{71} In so doing, the Court reasserted that it was irrelevant to constitutional considerations that the recording device did not physically intrude the area within the telephone booth.\textsuperscript{72}

Having found that the recording of Katz's telephone conversations constituted an unlawful search and seizure, the next issue that the Court addressed was whether the government had complied with the Fourth Amendment in conducting the search and seizure.\textsuperscript{73} In its analysis, the Court noted that a magistrate could have issued a lawful warrant to search and seize Katz's telephone conversations using an electronic recording device.\textsuperscript{74} The fact that government agents failed to get this kind of warrant made the search and seize an unjustified violation of Katz's Fourth Amendment rights.\textsuperscript{75} Therefore, the Court held that the recording of Katz's telephone conversations constituted a violation of the Fourth Amendment and overturned his conviction.\textsuperscript{76}

C. What Does the Law Provide on Government Use of Electronic Surveillance?

1. Title III of the Omnibus Crime Control and Safe Streets Act of 1968\textsuperscript{77}

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 set forth procedures by which government officials could obtain federal court authorization for real-time interception of the content of electronic communications.\textsuperscript{78} Congress wanted to enact strict limitations on the use of electronic surveillance to ensure the protection of individual privacy rights.\textsuperscript{79} Under Title III, au-

\textsuperscript{68} Id. at 553.
\textsuperscript{69} Id. (citing Silverman v. United States, 365 U.S. 505, 511 (1920)).
\textsuperscript{70} See id.
\textsuperscript{71} Id.
\textsuperscript{72} See id.
\textsuperscript{73} Id. at 354. The government admitted into evidence six recordings of Katz's end of the telephone conversations in which the content involved "the placing of bets and the receipt of wagering information." Id. at 354 n.14.
\textsuperscript{74} Id. To maintain safeguards against government infringements upon personal liberties requires the government to notify the magistrate of the need for the search, specify the plan of action, and indicate the precise evidence to be searched and seized. Here the search and seizure was of a narrow enough scope that the magistrate could have constitutionally granted such permission. Id. "A federal court may empower government agents to employ a concealed electronic device 'for the narrow and particularized purpose of ascertaining the truth.' " Id. at 355 (quoting Osborn v. United States, 385 U.S. 323, 329 (1966)). The Katz Court noted that the purpose of requiring court permission is to ensure that searches and seizures do not extend beyond what is necessary under the circumstances. Id. (citing Berger v. New York, 388 U.S. 41, 87 (1967)). See also Fed. R. Crim. P. 41(d). See generally Ker v. State of California, 374 U.S. 23, 37 (1963) (holding that when the government has authorization to conduct a search and seizure, advance notice to the person subject to the search and seizure is not necessary in cases where such notice would destroy the government's opportunity to search or seize evidence).
\textsuperscript{75} Katz, 389 U.S. at 356; see also Wong Sun v. United States, 371 U.S. 471, 481 (1963) (holding a search and seizure executed in the absence of proper authorization is

\textsuperscript{77} Title III, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended in scattered sections of 18 U.S.C.). This statute is commonly known as the federal wiretap statute. See 18 U.S.C. § 2510(8) (defining the contents of communications to be "any information concerning the substance, purport, or meaning of that communication")


authorization to intercept the contents of electronic communications using a wiretap is only available for certain enumerated offenses.\textsuperscript{80} Government agents seeking an order to intercept the contents of electronic communications must include in the wiretap application a statement of the facts justifying the issuance of the order, a statement showing that other investigative means have been employed and the period of time that the order will be in force.\textsuperscript{81} The statute also requires that government agents make a showing of probable cause before a court can authorize the interception of the contents of electronic communications.\textsuperscript{82} The court's order must identify the specific communications to be intercepted, the surveillance target, the location of the target's Internet Service Provider ("ISP") and the particular government agency authorized to conduct the interception.\textsuperscript{83} Courts also can require the government to provide regular progress reports detailing the type of data collected and any future need for continued use of the wiretap.\textsuperscript{84} Both the exclusionary rules of the Fourth Amendment and the wiretap statute found in Title III prohibit the use of evidence obtained in violation of the procedures for intercepting the contents of electronic communications.\textsuperscript{85}

\textsuperscript{80} See 18 U.S.C. §§ 2510-2522; see also Kerr, supra note 8 (explaining that a federal magistrate cannot authorize the use of a wiretap, and interception of electronic communications is limited to specific enumerated felonies).

\textsuperscript{81} See 18 U.S.C. § 2518(1) ("Each application for an order authorizing or approving the interception of a[n] . . . electronic communication . . . shall be made in writing upon oath or affirmation to a judge of competent jurisdiction."); see also Kerr, supra note 8 (noting that electronic surveillance has played a role in convicting more than 25,600 felons over the past thirteen years).

\textsuperscript{82} See 18 U.S.C. § 2518(3) (requiring government agents to show probable cause in three different contexts). The judge may authorize interception of wire, oral or electronic communications if the judge determines that:

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated . . . ; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) . . . there is probable cause for belief that the facilities from which, or the place where, the wire or oral communication are to be intercepted are being used, or are about to be used, in connection with the commission of such offense.

\textsuperscript{83} Id. at § 2518(3).

\textsuperscript{84} Id. at § 2518(6).

\textsuperscript{85} Id. at § 2518(4).

\textsuperscript{80} Id. at § 2518(6).

\textsuperscript{81} See id. at § 2518(10).

\textsuperscript{82} Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.)

\textsuperscript{83} 434 U.S. 159 (1977).

\textsuperscript{84} Id. at 165. The U.S. District Court for the Southern District of New York authorized the FBI to install a pen register on two telephone lines and directed the New York Telephone Co. to assist in the installation and implementation of the court's order. The order was based on probable cause that the telephones were being used in conjunction with an illegal gambling enterprise. The telephone company's refusal to comply with the court's order lead to subsequent litigation. \textit{Id.}

\textsuperscript{85} Id. at 167 (finding that a pen register decodes telephone numbers by "responding to changes in electrical voltage caused" by the dialing of numbers on a telephone).

\textsuperscript{86} Id. (noting that pen registers do not hear sound); see also Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995) (following the Court's holding in \textit{New York Tel. Co.} and reasserting that the only capability of the pen register and trap and trace devices is to intercept dialed telephone numbers).

\textsuperscript{87} \textit{New York Tel. Co.}, 434 U.S. at 167. The case's holding applies to trap and trace devices as well because of the synonymous nature of the devices. See also 18 U.S.C. § 2518(1) (governing the authorization of the interception of a wire or oral communication); S. REP. No. 90-1097, at 90 (1968), reprinted in 1968 U.S.C.C.A.N. 2112 (detailing Congress's intent that the coverage of Title III excludes pen registers).

\textsuperscript{88} \textit{Smith v. Maryland}, the Supreme Court considered whether a pen register constituted a search within the meaning of the Fourth Amendment. There, the Court held "that there is no con-

2. Amending Title III: The Electronic Communications Privacy Act of 1986 ("ECPA")

To understand why Congress found it necessary to amend Title III by passing the ECPA, one must examine how the Fourth Amendment fared under Title III. In \textit{United States v. New York Telephone Co.},\textsuperscript{87} the Court stressed the limitations on the collection of information through pen registers. It also considered the issue of whether a federal district court could order a telephone company to provide assistance to federal law enforcement agents in order to implement a court-authorized pen register.\textsuperscript{88} Pen register devices "disclose only the telephone numbers that have been dialed."\textsuperscript{89} Surveillance using pen register devices cannot reveal the contents of communications, the identities of the parties involved "[or] whether the call was even completed."\textsuperscript{90} The Court held in \textit{New York Telephone Co.} that Title III (the federal wiretap statute) does not govern the use of pen registers because these devices do not intercept the contents of communications.\textsuperscript{91} In \textit{Smith v. Maryland},\textsuperscript{92} the Supreme Court considered whether a pen register constituted a search within the meaning of the Fourth Amendment.
stitutionally protected privacy interest in the numbers one dials to initiate a telephone call." Adhering to \textit{Katz}, the Court stated that the threshold question was whether the alleged criminal suspect had a reasonable expectation of privacy that the government unf fourthly invaded by using a pen register. The government's installation of the pen register did not invade any constitutionally protected area. Furthermore, the device did not capture the content of Smith's telephone calls. Therefore, because no protected area had been invaded, the ultimate question was whether Smith had a reasonable expectation of privacy in the numbers he dialed on his telephone. The Court reasoned that there was no reasonable expectation of privacy in the numbers dialed on a telephone because telephone companies routinely record numbers dialed for business purposes. Moreover, because individuals voluntarily provide the telephone company with the dialing information, "it is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret." As a result, even if Smith did have an expectation of privacy regarding the numbers that he dialed on his telephone, this expectation was unreasonable. Consequently, the government's use of the pen register was not a search within the meaning of the Fourth Amendment and no warrant was necessary. The Court's holding in \textit{Smith}, allowing the interception of the digits of incoming and outgoing telephone calls, serves as justification for the relatively low standard governing privacy protections for pen register and trap and trace devices. More importantly, the Court's decision in \textit{Smith} created distinct classes of communications and afforded less Fourth Amendment protection to noncontent-based communications.

Responding to these developments in Fourth Amendment jurisprudence, Congress passed the ECPA with the intention that this new law would create a balance "between the privacy of citizens and the needs of law enforcement" that had become tipped too far in favor of the government. Improving electronic technologies had created new methods of electronic surveillance, and the increasing use of electronic communications, including the transportation of personal data, had created more opportunities for government to infringe upon constitutionally protected privacy rights. Congress enacted the ECPA to

\begin{itemize}
  \item \textit{Id.} While investigating a robbery and subsequent threatening phone calls, police installed a pen register on Smith's telephone line. Evidence gathered by the pen register formed the basis for a warrant to search Smith's home. Further evidence gathered during the search lead to Smith's arrest. At trial, Smith argued that the evidence gathered by the pen register should be inadmissible because it was obtained without a search warrant. Smith appealed his subsequent conviction on the basis that the pen register information had been improperly admitted into evidence. \textit{Id.} at 737.
  \item \textit{Id.} at 740.
  \item \textit{Id.} at 741.
  \item \textit{Id.} (finding that pen registers, which do not capture content like wiretaps, require a different analysis of the constitutional issues); \textit{see also} \textit{New York Tel. Co.}, 434 U.S. at 167.
  \item \textit{See Smith}, 442 U.S. at 742.
  \item \textit{Id.} (finding that telephone companies need access to phone numbers to complete calls through their switchboard, tabulate billing records for long-distance toll calls and service telephone lines, which includes facilitating law enforcement functions).
  \item \textit{Id.} at 743. The site from where the call is placed is irrelevant because it only reflects a desire to protect the privacy of content and not dialing information.
  \item \textit{Id.} (noting that one cannot have a reasonable expectation of privacy in the information voluntarily given to third parties (citing United States v. Miller, 425 U.S. 435, 442-45 (1976))).
  \item \textit{See id.} at 745-46.
  \item \textit{18 U.S.C.} § 3127(3)-(4).
  \item \textit{See The Center For Democracy & Tech., Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections, at http://www.cdt.org/security/000404amending.shtml (Apr. 14, 2000) [hereinafter Amending the Pen Register].
  \item \textit{Corn-Revere, supra} note 14 (quoting The Office of Technology Assessment that "[o]vertime, the cumulative effect of widespread surveillance for law enforcement, intelligence, and other investigatory purposes could change the climate and fabric of society in fundamental ways").
  \item \textit{See S. Rep. No. 99-541, at 2 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. Title I of the ECPA amends Chapter 119 of Title 18 governing the interception of communications "to bring it in line with technological developments and changes in the structure of the telecommunications industry." The Fourth Amendment and the Internet: Oversight Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong. 71, 76 (2000) (statement of Gregory T. Nojeim, Legislative Counsel, Am. Civil Liberties Union, Washington Nat'l Office) [hereinafter Nojeim] (citing DOJ studies that find nearly 75% of Americans oppose wiretapping and that the loss of personal privacy in the new millennium is the predominant concern of Americans), available at http://www.aclu.org/congress/104060a.html; Amending the Pen Register, supra note 103. Government agents use pen register and trap and trace devices about ten times more frequently than wiretaps. For instance, in the year 1996, 4,569 pen register and trap and trace orders were obtained by the DOJ covering over 10,520 telephone lines. Amending the Pen Register, supra note 103. See also \textit{Corn-Revere, supra} note 14. In the 1970s, the Church Committee investigations documented the FBI's unjustified use of wiretaps on people like Dr. Martin Luther King, Jr., Congressman Harold Coo-
preserve the Fourth Amendment protection against unreasonable searches and seizures of an individual's electronic communications. Congress defined the term “electronic communication” in the ECPA broadly to provide statutory protections for individual Fourth Amendment rights against future advancements in technology.  

Despite congressional intent to increase protections for electronic communications, the ECPA does not offer as much constitutional protection for electronic communications as Title III offers for voice communications. Authorization for an application to intercept electronic communications can be made by any government attorney, whereas authority to apply for a wiretap can only be granted by a high-ranking Justice Department official. Moreover, authorization for intercepting electronic communications can be made in conjunction with any federal felony by merely showing that the information sought is relevant to a criminal investigation. In contrast, telephone wiretaps may only be used for certain felonies enumerated in Title III. In addition, the ECPA provides greater protection against real-time interception of electronic communications than it does against government access to stored electronic communications. To make real-time interceptions of electronic communications, government agents must obtain a court order based on probable cause. However, government agents may obtain, without notice to the affected party, the content of stored electronic communications with a search warrant issued by a federal magistrate rather than a federal district court judge. Therefore, the statutory protections provided to real-time electronic communications in the ECPA are irrelevant once the communication becomes stored data. Law enforcement officials have exploited this loophole in the ECPA, making it easier to obtain lawfully intercepted electronic communications from suspected criminals.

3. The Pen Register and Trap and Trace Statute Enacted as Part of the ECPA

The ECPA also amended Title III’s provisions for issuing a pen register or trap and trace device. A pen register surveillance device is capable of capturing in real time the numbers dialed on outgoing telephone calls. Trap and trace devices capture in real time the numbers of incoming telephone calls. Unlike the interception of the content of electronic communications, government agents do not need to show probable cause in order to obtain court authority for a pen register or trap and trace device. A court will grant authorization upon certification “that the

age for less than 180 days, the only means to obtain its content is with a warrant. However, the legal standard to justify issuance of the warrant is whether the communication is relevant to an ongoing investigation rather than the probable cause required for real-time interceptions of electronic communications. To get a list of phone calls made to and from a certain telephone number. The usable information is limited to the 10 digit telephone number and the time of the call.” Smith, 442 U.S. at 743 (holding that the numbers dialed on a telephone are not private).
information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.” It is important to note that the pen register and trap and trace statute does not have any safeguards to prohibit the admission of evidence obtained in violation of the Fourth Amendment.


Congress made another attempt to redefine the balance between individual Fourth Amendment privacy rights and the government’s need to conduct electronic surveillance of criminal activity with the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). CALEA required telecommunications carriers to provide law enforcement officials with assistance in responding to criminal use of improving technologies. Surveillance techniques did not advance at the same pace as communications technology, making it more difficult for law enforcement agents to monitor criminal activity. CALEA clearly did not extend to information services, including online service providers. However, CALEA did not totally exempt Internet communications from electronic surveillance because the government’s ability to conduct electronic surveillance under the ECPA was unaffected.

Specifically, CALEA required that while carrying out statutory obligations, such as assisting government agents with installation of wiretaps, telecommunications carriers must restrict the government’s access to only the information for which courts have authorized interception. CALEA also reinforces limitations on information that the government can obtain using pen register and trap and trace devices. In addition, CALEA required that government agents obtain a court order before obtaining information relating to electronic mail or online profiles.

The Center for Democracy and Technology ("CDT") argued that the J-Standards violated CALEA and petitioned the Federal Communications Industry Association to end their cooperation with the government in preserving government’s wiretapping capabilities because without a uniform law requiring such cooperation, those carriers who did cooperate were put at a competitive disadvantage to those carriers who did not cooperate, available at www.fcc.gov/judiciary.

See Pub. L. No. 103-414, 108 Stat. 4279 (1994) ("An act to . . . make clear a telecommunications carrier’s duty to cooperate in the interception of communications for law enforcement purposes."); see also 18 U.S.C. § 2518(4) (providing that an order can be issued to enforce the assistance requirements as set out in CALEA); Corn-Revere, supra note 14 ("CALEA is the first statute to impose upon telecommunications carriers an affirmative obligation to modify and design their equipment, facilities, and services to ensure that new technologies and services do not hinder law enforcement’s access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance.").
nifications Commission ("FCC") to remove the offending provisions. The FBI and DOJ also petitioned the FCC, but argued that the J-Standard fell below CALEA's requirements. The DOJ provided the FCC a list ("FBI punch list") of surveillance capabilities that it wanted added to TIA's J-Standard. The FCC added four of the FBI punch list capabilities to the J-Standard and refused to remove from the J-Standard the two provisions to which the CDT objected. The matter was appealed to the United States Court of Appeals for the District of Columbia.

Once there, the appeals court considered the validity of the FCC provisions imposing duties on telecommunications carriers under CALEA. The petitioners alleged that the FCC's implementation of the punch list items exceeded the scope of CALEA. The appeals court quoted a state law in which the FBI punch list capabilities to the J-Standard and refused to remove from the J-Standard the two provisions to which the CDT objected. The matter was appealed to the United States Court of Appeals for the District of Columbia.

III. THE INTERNET TODAY

Today, the Internet is quickly becoming the major vehicle for global communications and social activity. The Internet is constantly evolving and accessible, drawing more and more people who desire to make use of its virtually unlimited applications. The uses for which people employ the Internet are vastly increasing; they include electronic mail, shopping and electronic commerce, as well as transferring "financial statements, medical records, and information about children." As uses for the Internet continue to evolve, more personal data will be transferred online. The unintended, and potentially harmful, byproduct of this development is that it makes a massive amount "of sensitive data available to government investigators." The interception of Internet communications will likely increase as digital technology improves and becomes more widely used. Digital technology allows government agents to capture and process more communications than what was possible with analog communications. With analog communications, "a single circuit is opened between caller and recipient and all electronic signals that make up the communication travel along the circuit." In contrast, digital commu-

139 Id.
140 Id. at 456.
141 Id.
142 Id.
143 Id. at 456-57. Appeals by the petitioner, Cellular Telecommunications Industry Association, CDT, Electronic Frontier Foundation, Electronic Privacy Information Center and the American Civil Liberties Union were consolidated into this case.

144 See id. at 457 (reviewing the FCC's provisions requiring that carriers make available the location of antenna towers, signaling information from custom calling features, numbers dialed after calls are connected and packet mode data).
145 See id.
146 See id. at 454–55.
147 See id. ("CALEA permits the telecommunications industry, in consultation with law enforcement agencies... to develop its own technical standards for meeting the required surveillance capabilities." (citing 47 U.S.C. § 1006)).
148 See ACLU v. Johnson, 4 F. Supp. 2d 1029, 1031 (D.N.M. 1998) (making a finding of fact that the Internet is a "global medium of communication that links people, institutions, corporations and governments around the world"); see also Davidson, supra note 7. Davidson referred to a Harris poll from December 1999 revealing that 56%—six times more than just four years ago—of American adults use the Internet. This statistic does not include the widespread use of the Internet in schools. See Davidson, supra note 7.
149 See Davidson, supra note 7 (commenting that the Internet promises to "promote expression, spur economic opportunity, and reinvigorate civic discourse").
150 Id. Indeed, this explosion of online activity has come to be known as the Internet revolution.
151 See id. (noting that electronic communications increasingly contain sensitive content relevant to an individual's "actions, relationships, and thoughts").
152 Corn-Revere, supra note 14 (stating that the electronic wiretap has replaced the telephone wiretap as the most common form of surveillance).
154 See id. (contrasting the labor intensive practice of intercepting analog communications with the use of computers that can assist government agents in processing intercepted digital communications).
155 United States Telecom Ass'n, 227 F.3d at 450.
communications are broken into data packets that travel independently across networks and "are then reassembled in the proper sequence" at the communication's destination. Each data packet consists of two components. One component is the address information, which appears in the packet's header and, like an envelope address, ensures that the communication arrives at the proper location and is reassembled in the correct sequence. The second component is the body, or payload of the communication, which contains the communication's content.

A. How Carnivore Works

Increasingly, criminals are using the Internet to commit crimes. The FBI claims that it has had a difficult time pursuing cyber criminals because its agents lack vital support technology necessary to catch this new breed of criminal suspects. As a result, the FBI developed the diagnostic tool Carnivore to conduct electronic surveillance of electronic mail messages and other online communications. The FBI plugs a personal computer running the Carnivore software into the surveillance target's ISP network. The system's operator then uses a Graphical User Interface, such as a touch screen, to set the system's filters. Carnivore, classified as a "packet filter" or "packet sniffer," searches, intercepts and then collects the digital data packets identified as the surveillance target's electronic communications, while ignoring all other communications that the government has no authority to intercept. The captured data is then stored on a removable disk.

Functioning like a pen register or trap and trace device, Carnivore can provide the origin and destination of all communications traveling across the ISP's network going from and coming to the alleged criminal suspect's computer. However, Carnivore also is capable of performing wiretap functions because it can monitor and record the content of Internet communications, such as e-mail messages. Therefore, the government can use Carnivore pursuant to either a wiretap order, which allows the interception of content, or under a pen register and trap and trace order that only authorizes interception of numbers related to communications from or to specified targets.

The potential that data mining can take place under pen register and trap and trace orders poses an unreasonable threat to Fourth Amendment rights. Questions abound concerning who controls the filter settings on Carnivore and who oversees the FBI in order to assure that government agents only make lawful use of the system. The threat is made more dangerous when one considers that the FBI can control Carnivore from a remote location in order to monitor the data collected and to change the filter settings. Additionally, not having an opportunity to review Carnivore's program code has created a fear among ISPs of the possible side affects that Carnivore may have on their network operations and

156 Id.
157 See id.
159 See Davidson, supra note 7. However, recent advancements in technology have greatly improved the government's ability to conduct electronic surveillance. So much so that in the next decade the FBI predicts a 300% increase in the use of wiretaps. However, the reality is that the Internet benefits both criminals and law enforcement agents. Id.
160 See Kerr, supra note 8.
162 See id.
163 See id.
164 See id. (operating as a packet sniffer, Carnivore can capture downloaded files, online conversations and e-mail messages).
165 See id.
166 See Davidson, supra note 7.
167 See id.
168 AMENDING THE PEN REGISTER, supra note 103. E-mail addresses are unique to individual users—unlike telephones that can be used communally—so it is likely that a pen register will reveal the identity of the message's recipient. Additionally, if Carnivore can capture URLs, website addresses or file names, the information the government obtains will likely reveal the substance of the communication's contents. Id.; see also Brown, 50 F.3d at 294 (holding that numbers dialed into digital pagers are considered to be content and therefore subject to government interception only through properly authorized wiretaps).
169 See Corn-Revere, supra note 14 (arguing that using pen register and trap and trace capabilities in this instance violates congressional intent to protect Fourth Amendment rights through the ECRA).
170 See Davidson, supra note 7.
security systems.\textsuperscript{172} Pen register devices and trap and trace orders are obtained under a "standard of approval so low as to be nearly worthless,"\textsuperscript{173} and there are no provisions for judicial or ISP oversight of Carnivore when used under this kind of authority.\textsuperscript{174} For example, when the government employs Carnivore under a pen register or trap and trace order, the system maintains its potential to conduct wiretapping functions.\textsuperscript{175} Moreover, pen register and trap and trace devices were designed to intercept telephone dialing information, and it is not clear what the Internet equivalent is to numbers dialed on a telephone.\textsuperscript{176} Those concerned with preserving Fourth Amendment rights question whether packet headers (the addressing information) can be separated from packet bodies or payloads (the contents of Internet communications).\textsuperscript{177} The letters in an e-mail address are not analogous to the numbers used for making telephone calls because e-mail addresses, Internet protocol addresses, header information and URLs can reveal more information (such as the identities of the parties and the contents of the communication) than incoming or outgoing telephone numbers reveal under a "normal" pen register or trap and trace device.\textsuperscript{178} There is a very real threat that, when applied to Internet communications, pen register and trap and trace devices will intercept the communication's content unlawfully.\textsuperscript{179} Carnivore's ability to capture vast amounts of data has the potential to provide a detailed picture or profile of a person's associations, habits, contacts, interests and activities, which are all outside the permissible scope of government surveillance under the Fourth Amendment.\textsuperscript{180}

Moreover, unlike wiretap orders, pen register and trap and trace devices do not have a minimization rule. This rule requires that, in executing a wiretap order, law enforcement agents must minimize the interception of nonincriminating communications.\textsuperscript{181} The lack of a minimization rule for pen register and trap and trace devices becomes more notable when one considers that, regardless of whether it is authorized by a wiretap, pen register or trap and trace device, Carnivore scans the contents of every single communication traveling on the ISP's network.\textsuperscript{182} This gives the government access to the communications of the targeted suspect, nontargeted subscribers and every person who communicates with that ISP's customers.\textsuperscript{183} In effect, this capability makes Carnivore a maximization tool rather than the minimization tool required by the Fourth Amendment because "Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers."\textsuperscript{184}

Questions also remain unanswered about the system's technical capabilities because the FBI has refused to reveal Carnivore's source code.\textsuperscript{185} In fact, there was no public oversight in developing Carnivore.\textsuperscript{186} Constitutional scholars and industry experts are among the many who argue that granting the public access to its source code (the technical blueprint behind a software program like Carnivore) would end the controversy surrounding Carnivore by increasing public understanding and allowing for review by independent experts.\textsuperscript{187} "[I]solating network traffic can be

\textsuperscript{172} See Davidson, \textit{supra} note 7 (arguing that without a review of Carnivore's source code, questions remain unanswered about the accuracy of the audit trails and system's safeguards against tampering).

\textsuperscript{173} Id.

\textsuperscript{174} See id. (finding that the lack of judicial oversight creates a potential for misuse).

\textsuperscript{175} See id. (noting that this additional capacity is what makes Carnivore different from the trap and trace and pen register devices used in connection with telephone surveillance because Carnivore has the capability to scan headers, subject lines and content information).

\textsuperscript{176} See Steinhardt, \textit{supra} note 155 ("On the Internet, the only time numbers are literally 'dialed' by a telephone is when a user connects to an ISP using a dial up modem.").

\textsuperscript{177} See AMENDING THE PEN REGISTER, supra note 103.

\textsuperscript{178} See Steinhardt, \textit{supra} note 153.

\textsuperscript{179} See AMENDING THE PEN REGISTER, supra note 103.

\textsuperscript{180} See id.

\textsuperscript{181} See id.

\textsuperscript{182} See Steinhardt, \textit{supra} note 153.

\textsuperscript{183} See High Tech Investigations, Hearing Before the House Judiciary Comm. Subcomm. on the Constitution, 106th Cong., at http://www.house.gov/judiciary/stei0724.htm (2000) (statement of Barry Steinhardt, Assoc. Dir., Am. Civil Liberties Union) [hereinafter ACLU]; see also Noejim, \textit{supra} note 105. This is the type of search and seizure the Fourth Amendment protects against. Statistics for 1969–1973 detail that over 50% of intercepted electronic communications were incriminating. In contrast, from 1994–1998, statistics reveal that only 20% of intercepted electronic communications were incriminating. For each electronic surveillance interception, 1,608 innocent conversations are intercepted. The data for 1998 shows that as the use of electronic surveillance has risen to an all-time high, the percent of innocent communications intercepted has risen as well. Id.

\textsuperscript{184} ACLU, \textit{supra} note 183.

\textsuperscript{185} See Davidson, \textit{supra} note 7.

\textsuperscript{186} See id.

\textsuperscript{187} See id.
technically difficult," and it may not be possible for the government to obtain the e-mail addresses of incoming and outgoing messages for a particular subscriber.\(^1\)\(^8\) Additionally, it may not be possible to separate the source or destination information of a communication from the communication's content.\(^1\)\(^9\)

B. The Government’s Position on Carnivore

The government counters Carnivore's critics by arguing that the potential capabilities of Carnivore are irrelevant because court orders specify the extent to which the wiretap device can intercept data from electronic communications.\(^1\)\(^9\)\(^0\) Moreover, the government claims that it will only use Carnivore for cases in which the ISP is unable to obtain the information or when the ISP requests that the government use its own equipment to obtain the information.\(^1\)\(^9\)\(^1\) The FBI justifies its refusal to reveal Carnivore’s source code by arguing that doing so would allow criminals to develop methods to defeat the system.\(^1\)\(^9\)\(^2\) However, this argument is strained because the government is asking the public to accept its word that government agents will not exceed the scope of a court order authorizing the interception of electronic communications.\(^1\)\(^9\)\(^3\) Nevertheless, the government asserts that there are substantial safeguards to discourage and punish unlawful uses of Carnivore.\(^1\)\(^9\)\(^4\) In addition to judicial oversight and court authorization, the DOJ, which includes the FBI, has installed what it argues are sufficient internal oversight mechanisms for Carnivore’s use.\(^1\)\(^9\)\(^5\) For example, although Carnivore scans every communication on the ISPs network, the system’s filters are configured to record only the communications of the surveillance target.\(^1\)\(^9\)\(^6\) Moreover, Carnivore logs the filter settings and reports its activity in audit trails,\(^1\)\(^9\)\(^7\) and agents who misuse Carnivore are subject to both civil and criminal penalties.\(^1\)\(^9\)\(^8\) The government also claims that an individual agent acting alone is unlikely to abuse Carnivore because the system’s installation and operation require support from both technical experts and the ISP.\(^1\)\(^9\)\(^9\)

Accepting the government’s word is an implicit rejection of the Fourth Amendment and the principles on which it stands.\(^2\)\(^0\) Historically, the FBI has failed to uphold the promises it has made regarding self-imposed limitations on law enforcement capabilities.\(^2\)\(^0\)\(^1\) Therefore, the reality is that Congress should take action to update the statutory scheme governing electronic surveillance and enact further protections for individual privacy on the Internet.\(^2\)\(^0\)\(^2\) The consequences of congressional inaction concerning the scope of electronic surveillance and Carnivore could very well create an individual’s right to speak anonymously).

\(^1\)\(^8\) Id. (commenting that Internet protocol addresses, the numbers making up an e-mail address, may be changed overtime and result in a failure to intercept the targeted communications or the interception of communications from the wrong user).

\(^1\)\(^9\) See id. Source or destination information varies depending “on what layer of the Internet protocol stack one looks at [sic].” Id. Source and destination information can be found in the header Ethernet address of the local network; the “IP address of an ISP’s mail server; [and] the To: line of an e-mail message.” Id. For example, a URL only provides the location of the data’s source, but having obtained that URL, a government agent can visit the same site and view the contents of the communication. Id.

\(^1\)\(^1\)\(^0\) See Gregory, supra note 158.

\(^1\)\(^1\)\(^1\) See id.

\(^1\)\(^1\)\(^2\) See Michael J. Sniffen, Chewing Out ‘Carnivore,’ ABCNEWS.COM, Aug. 25, 2000, available at http://more.abcnews.go.com/sections/tech/dailynews/carnivore000825.html. The Justice Department selected a private organization to review Carnivore. The review will consider whether Carnivore provides all the information the government should see but none of the information the government should not see; or if it poses risks to the ISP’s network or contains effective safeguards against unauthorized use. Id.

\(^1\)\(^1\)\(^3\) See generally McIntyre v. Ohio Elections Comm’n, 514 U.S. 334 (1995) (holding that the First Amendment protects an individual’s right to speak anonymously).

\(^1\)\(^9\)\(^4\) See Kerr, supra note 8. But see ACLU, supra note 183 (noting that the government’s “trust us” approach is inadequate to preserve the principles underlying the Fourth Amendment).

\(^1\)\(^9\)\(^5\) See Kerr, supra note 8.

\(^1\)\(^9\)\(^6\) See Davidson, supra note 7 (stating that in theory, Carnivore is a minimization tool that is programmed to store only specific communications). But see Steinhardt, supra note 153 (stating that in effect, the government “asks you to trust it with unsupervised access to the entire stream of communications over an ISP’s network”).

\(^1\)\(^9\)\(^7\) See Gregory, supra note 158.

\(^1\)\(^9\)\(^8\) See Kerr, supra note 8.

\(^1\)\(^9\)\(^9\) See Bridis & King, supra note 171; see also Kerr, supra note 8.

\(^2\)\(^0\) See Steinhardt, supra note 153 (arguing that the Fourth Amendment is built on the premise “that the Executive cannot be trusted with carte blanche authority when it conducts a search”).

\(^2\)\(^0\)\(^1\) See id. (detailing the FBI’s attempts to circumvent the bargain struck by CALEA in preserving the status quo of government surveillance capabilities).

\(^2\)\(^0\)\(^2\) See Corn-Revere, supra note 14. The Omnibus Crime Control and Safe Streets Act dates from 1968, and the most recent update to surveillance laws, the ECPA, dates from 1986.
IV. PROPOSED SOLUTIONS TO ENSURE THAT CONSTITUTIONAL PROTECTIONS EXTEND TO INTERNET COMMUNICATIONS

A. The Feasibility of a CALEA Framework

In considering the scope of CALEA’s definition of call-identifying information in United States Telecom Ass’n, the court noted that CALEA does not cross-reference or incorporate the ECPA definitions or statutory provisions regarding pen register or trap and trace devices. However, the court still questioned whether the requirement under CALEA to provide call-identifying information can be used lawfully to obtain all digits dialed after a call connection has been established. The court stated that so called “dialed digit extraction” may violate Fourth Amendment privacy rights because it is just as likely that the digits comprise call content as call-identifying information. As a result, the court refused to add dialed digit extraction to the J-Standard. Despite the court’s reluctance to find information gathered by pen register and trap and trace devices analogous to call-identifying information, the decision does just that very thing.

Applying the court’s analysis to a potential legal challenge to Carnivore will lead to a similar result. Like dialed digit extraction, the information that Carnivore reveals under a pen register or trap and trace device court order may reveal the contents of Internet communications in violation of the Fourth Amendment. Unfortunately, current law “is far from clear on the use of pen register or trap and trace devices in the Internet context.”

Therefore, United States Telecom Ass’n is useful in illustrating how a CALEA-like framework—where standards developed by the telecommunications industry outline what telecommunications carriers must provide government agents employing electronic surveillance—may prevent Carnivore from invading Fourth Amendment privacy rights. This case demonstrates that even dialed digits can contain content deserving Fourth Amendment protection. Applied to electronic mail and other Internet communications, this proposition should raise concerns that even if Carnivore’s filters are set to capture only header information, the data intercepted will likely contain content.

As the congressional intent behind CALEA was to maintain the status quo in electronic surveillance, any change to the ECPA concerning Carnivore should reflect this intent. ISPs should re-
tain control over their networks. Under the equivalent of industry standards, ISPs should face the statutory duty to provide law enforcement officials, with proper court authority, access only to information to which they are legally entitled.217 Because the J-Standards in CALEA have built-in provisions for agency and judicial review, these standards should serve as the model for future statutory control of Carnivore. Not only are ISPs the most technically qualified to install and operate systems such as Carnivore on their networks but also their involvement will serve as an added check against a government agent’s unauthorized use.218 In other words, ISP’s should be responsible for protecting privacy rights against unauthorized government interception.219 Congress should require the ISP to directly oversee the separation of the surveillance target’s communications from other communications traveling across ISP networks.220 Furthermore, if ISPs are capable and willing to furnish the information that the government has authority to intercept, the government should not be permitted to reject this offer and instead use Carnivore to obtain the information.221 If an ISP refuses to assist the government, the government should still be required to satisfy Title III before conducting electronic surveillance.222 Additionally, if ISPs are compelled to assist law enforcement officials using Carnivore, the government should be required to reveal information about Carnivore’s operations and source code to the ISP.223

B. Limiting Electronic Surveillance by Strengthening Current Laws

The Katz Court declared that the Fourth Amendment’s protection against unreasonable searches and seizures applies to people wherever they may be because interpreting the Constitution to say otherwise “is to ignore the vital role that the public telephone has come to play in private communications.”224 Today, this statement applies to the Internet, making the presence or absence of a physical intrusion irrelevant to whether a search or seizure violates the Fourth Amendment.225 Individuals using the Internet as a mode of communication have reasonable expectations of privacy that require greater legal protections than current laws provide.226 Therefore, Congress should amend the ECPA to require that any information other than the equivalent of dialed numbers is only accessible with a valid wiretap order.227 This would exclude “search terms, URLs identifying certain documents, files, web pages, or other transactional information” from the definition of dialed numbers.228 Moreover, because Carnivore performs wiretapping functions, the legal standard supporting pen register orders should be raised to a probable cause standard.229 This would close the loophole through which government agents have previously been able to capture content information without a wiretap order and related judicial oversight.230

The ECPA also should be amended to contain an exclusionary rule similar to the one in Title III that prohibits the use of improperly obtained information.231 Likewise, Congress should impose requirements for reporting statistics and record keeping modeled after those in Title III.232 Currently, the ECPA only requires reporting of pen register and trap and trace orders for which the DOJ applies, not those “by other Federal law enforcement agencies or state and local authorities.”233 Requiring government agents to report use of electronic surveillance will ensure a degree of accountability currently absent in electronic surveillance.234 Finally, the ECPA should be amended to include civil and criminal sanctions—similar to those found in Title III for abus-

224 Katz, 389 U.S. at 352.
225 See id.
226 See Hearings on Electronic Communications Privacy Act, supra note 128.
227 See Amending the Pen Register, supra note 103.
228 Id.
229 See id.
230 See Davidson, supra note 7.

—
217 See Davidson, supra note 7. Rather than having Carnivore sit entirely outside the ISP’s network and control, the device should be installed similarly to a pen register or trap and trace device, both of which require phone company assistance.
218 See id. (detailing the role of ISP’s in limiting government access to only that which has been properly authorized).
219 See Steinhardt, supra note 153.
220 See id.
221 See id.
222 See id.
223 See id.
ing pen register and trap and trace devices—for abusing Carnivore.235

Updating surveillance laws strengthens privacy protections that have been eroded under current laws that do not apply easily to the Internet.236 The Constitution should not be literally construed because the Founders intended a flexible approach that would allow the Constitution to remain effective in the face of changing circumstances.237 Therefore, Congress should consider taking a stronger position on electronic surveillance by amending the ECPA to require that pen register and trap and trace orders cannot be used for intercepting Internet communications. In other words, Congress should make a properly issued Title III wiretap order the only method by which government agents receive authorization to conduct electronic surveillance of Internet communications. In effect, all Internet communications should be classified as content and therefore not lawfully accessible with pen register or trap and trace orders.238 The risk that pen register and trap and trace devices will capture content is simply too great to believe that the application of these devices to the Internet can be satisfactorily resolved in a manner that comports with the Fourth Amendment.

Congress also must boost the applicability of the Fourth Amendment’s minimization rule in order to protect the Internet communications of both surveillance targets and nontargeted private citizens communicating over the Internet.239 Carnivore functions by scanning every communication that travels over the ISP’s network.240 Therefore, the minimization rule should declare expressly that under no circumstances does the government have the authority to intercept communications that are not the subject of a proper Title III court order authorizing electronic surveillance.241

If Congress elects to remedy the situation by raising the legal standard for pen register and trap and trace devices, the wiretap minimization rule needs to be strengthened, and a minimization rule must be adopted that applies to pen register and trap and trace devices.242

Requiring the FBI to submit Carnivore’s source code for public review will let the public know that the government is capable of monitoring the electronic communications scanned by FBI agents.243 Public review of Carnivore’s source code can be useful in identifying “mistakes, bugs, or security holes unknown to the FBI.”244 This knowledge will enable the public and ISPs to serve as checks on government surveillance activities as well as alleviate the chilling effect produced by the mystery surrounding Carnivore’s capabilities.245 In addition, Congress should enact laws to require greater oversight by both the court issuing the order authorizing the interception of electronic communications and by the ISP whose network is involved in the electronic surveillance.246 ISPs rightfully claim that they should have ultimate control over their networks, including the installation and use of Carnivore by government agents.247 The protection of stored electronic communications should be equivalent to the protection currently afforded to communications intercepted in real time.248 Title III wiretap standards should apply to capturing stored electronic data because content does not change when a communication becomes stored.249 Currently, government agents can obtain the same information but under a much less stringent legal standard by making the interception a second after the communication is received and stored on the user’s system.250

In considering revisions to current electronic surveillance laws, Congress will confront the fact

---

235 See Davidson, supra note 7.
236 See id.
237 See Olmstead, 277 U.S. at 484 (Brandeis, J., dissenting).
238 See Davidson, supra note 7. In other words, do not apply the rule set out in Smith, 442 U.S. at 745–46. See also Brown, 50 F.3d at 294 (holding that numbers dialed into pagers are content and receive Fourth Amendment protection).
239 See ACLU, supra note 183.
240 See Steinhardt, supra note 153.
241 See id. (acknowledging that this would require limiting Carnivore’s ability to access nontargeted communications).
242 See ACLU, supra note 183.
243 See Steinhardt, supra note 153 (discussing the ACLU’s filing of a Freedom of Information Act request with the FBI for documents concerning Carnivore’s system operations); see also Davidson, supra note 7.
244 Davidson, supra note 7.
245 See id.
246 See Steinhardt, supra note 153.
247 See Davidson, supra note 7; see also Kerr, supra note 8. The FBI can operate Carnivore independently of any ISP involvement, but court orders require that ISP’s be notified and able to assist in the installation of the device.
248 See Hearings on Electronic Communications Privacy Act, supra note 128.
249 See id.
250 See id.
that the Cable Communications Privacy Act of 1984\textsuperscript{251} ("Cable Act") currently provides greater protections for electronic communications made using a cable modem than that provided by Title III or the ECPA.\textsuperscript{252} As a result, Congress should resolve the differences between the three different levels of protection in order to protect Fourth Amendment rights on a uniform basis for all forms of communication.\textsuperscript{253} To adopt any standard of protection for Fourth Amendment rights less than what the Cable Act provides will seriously harm the Fourth Amendment.\textsuperscript{254}

C. Justice Department Proposals

The Justice Department has proposed legislation that would allow judges to issue countrywide pen register and trap and trace orders.\textsuperscript{255} The justification offered for this proposal is that the government’s ability to track Internet communications is hampered by the need to obtain an order in each physical jurisdiction through which the communication passes in cyberspace.\textsuperscript{256} Notably, the government’s proposal also includes orders authorizing the interception of telephone call information that do not face a similar burden.\textsuperscript{257} Moreover, the proposal does not require the government to make a showing as to why the order should be effective nationwide.\textsuperscript{258} Eliminating jurisdictional limits on the use of these surveillance devices has the effect of encouraging their expanded use.\textsuperscript{259} However, before encouraging more widespread use of pen register and trap and trace devices, Congress should address the questions raised about how these devices apply to Internet communications.\textsuperscript{260} Failing to do so may lead to a further erosion of Fourth Amendment and privacy rights.\textsuperscript{261}

The Justice Department also proposes increasing the legal standard governing the issuance of pen register or trap and trace devices under ECPA.\textsuperscript{262} The proposal applies Title III standards for intercepting the content of telephone calls to the interception of the content of electronic communications.\textsuperscript{263} This change would increase ECPA protections of electronic communications to a level comparable with Title III’s protections of voice communications.\textsuperscript{264} Changes would include requiring: a high ranking DOJ official, rather than any government attorney, to approve applications for intercepting electronic communications; probable cause that an enumerated felony, not any felony, has been committed; and courts to apply the exclusionary rule to evidence obtained in violation of proper procedures.\textsuperscript{265} These changes are justifiable on the grounds that e-mail, like voice communication, is a spontaneous form of communication.\textsuperscript{266} Although this will make it more difficult for government agents to obtain court authority to conduct electronic surveillance, this provision does not address Carnivore’s ability to scan every communication of every user on the ISP’s network because requiring a higher legal standard does not address the Fourth Amendment’s requirement for minimization.\textsuperscript{267} Nor does it address the discrepancy in protection of electronic communications stored by third parties.\textsuperscript{268} Until stored electronic communications are afforded the same protections as real-time communications, government agents will be able to circumvent the law by intercepting the communication after it has become stored.\textsuperscript{269}

\textsuperscript{252} See Steinhardt, supra note 153 (noting that unlike Title III and the ECPA, the Cable Act requires the government to give prior notice to the subject of the surveillance).
\textsuperscript{253} See id.
\textsuperscript{254} See id.
\textsuperscript{255} See AMENDING THE PEN REGISTER, supra note 103.
\textsuperscript{256} See Steinhardt, supra note 153.
\textsuperscript{257} See id.
\textsuperscript{258} See AMENDING THE PEN REGISTER, supra note 103.
\textsuperscript{259} See id. (arguing that the bill’s other provisions in combination with the reduction of local judicial oversight threatens privacy rights because more personal information will be collected); Steinhardt, supra note 153 (noting that the legislation may encourage forum shopping because one order will be effective in every jurisdiction).
\textsuperscript{260} See AMENDING THE PEN REGISTER, supra note 103 (arguing that current laws covering the issuance and scope of surveillance devices should be amended to strengthen privacy protections).
\textsuperscript{261} See Corn-Revere, supra note 14.
\textsuperscript{262} See Steinhardt, supra note 153 (noting that this proposal will only be effective if the new standard is significant).
\textsuperscript{263} See id.
\textsuperscript{264} See id.
\textsuperscript{265} See id.
\textsuperscript{266} See id.
\textsuperscript{267} See id.
\textsuperscript{268} See id.
\textsuperscript{269} See id. (explaining that it is highly probable that the reason a person stores an e-mail message is because it is important; therefore, it is the one most needing privacy protections).
D. Electronic Communications Privacy Act of 2000\textsuperscript{270}

Legislation currently before Congress would establish greater protections against both the interception of real-time electronic communications and the disclosure of stored electronic communications.\textsuperscript{271} H.R. 5018, or the Electronic Communications Privacy Act of 2000, increases the reporting requirements for government agents conducting electronic surveillance using wiretaps.\textsuperscript{272} Obtaining this information is a major step in beginning to understand the extent and depth of the government's use of electronic surveillance.\textsuperscript{273} However, the bill will not have a significant impact on Fourth Amendment rights unless it also applies to electronic surveillance using pen register and trap and trace orders. As with wiretap orders, reporting information for pen register and trap and trace devices will serve to make the government accountable for its actions.\textsuperscript{274} Congress also should consider including in the amendments the Title III provision that requires notice to the suspect before the intercepted Internet communications can be used in a criminal proceeding.\textsuperscript{275} The bill, however, does include an important provision to raise the legal standard for obtaining proper authorization for a pen register or trap and trace order.\textsuperscript{276}

V. CONCLUSION

The Fourth Amendment's protection against unreasonable searches and seizures applies to private Internet communications. Carnivore, the government's new electronic surveillance device, demonstrates that current surveillance laws are outdated in today's wired world. Neither Congress nor the Justice Department advocates solutions that will resolve the issues surrounding the changing technology in electronic surveillance used by government agents.

\textsuperscript{271} See id. (proposing to amend 18 U.S.C. § 2515 to read "whenever any wire, oral, or electronic communication has been intercepted, or any electronic communication in electronic storage has been disclosed").
\textsuperscript{272} See id. (proposing to amend 18 U.S.C. § 2703(g) to require reporting the fact the an order was applied for and granted, and the information obtained, including the number of incriminating communications disclosed).
\textsuperscript{273} See Hearings on Electronic Communications Privacy Act, supra note 128. It is logical that as the government expands its use of electronic surveillance, a similar expansion of reporting should take place.
\textsuperscript{274} See id.
\textsuperscript{275} See id.
\textsuperscript{276} See ECPA 2000, supra note 270. ECPA proposes to amend 18 U.S.C. § 3122(b)(2) (1994) to require a showing of factual evidence rather than mere relevance to an ongoing criminal investigation. This is the same standard the government must meet to obtain stored electronic communications under 18 U.S.C. § 2703(d). Id.