3-1-2001

A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy

Graham B. Smith

Recommended Citation
Available at: http://digitalcommons.lmu.edu/elr/vol21/iss3/7
A CONSTITUTIONAL CRITIQUE OF CARNIVORE,
FEDERAL LAW ENFORCEMENT’S NEWEST
ELECTRONIC SURVEILLANCE STRATEGY

The disciplinary institutions secreted a machinery of control that functioned like a microscope of conduct . . . . How was one to subdivide the gaze in these observation machines? How was one to establish a network of communications between them? . . . The perfect disciplinary apparatus would make it possible for a single gaze to see everything constantly. A central point would be both the source of light illuminating everything, and a locus of convergence for everything that must be known: a perfect eye that nothing would escape and a centre towards which all gazes would be turned.

-Michel Foucault

I. INTRODUCTION

Within the last two years, the Federal Bureau of Investigation (“FBI”) has implemented a surveillance tool called Carnivore to investigate people who may be using the internet to commit crimes. Clearly, a tool like Carnivore promotes better law enforcement because it gives the FBI access to an electronic medium in which criminals facilitate and engage in illegal conduct. The internet is the newest context for crime and continues to


2. Although the word “Internet” is traditionally capitalized, the central point of this Comment is that legislators and courts need to demystify the internet. See discussion infra Part IV. Thus, this Comment will not hereinafter capitalize “internet.”


5. Id.
challenge judges, legislators and law enforcement agencies that attempt to apply traditional legal standards to a digital dimension. While the government attempts to catch internet criminals by experimenting with a gamut of internet surveillance strategies, non-criminal internet users are left clutching the Fourth Amendment to balance their right to privacy against law enforcement’s need to access the internet for crime prevention. According to the FBI, Carnivore maximizes law enforcement capabilities while adhering to current federal surveillance laws. Alternately, computer privacy advocates argue that Carnivore’s broad search capabilities violate current federal surveillance laws, compromising the internet user’s Fourth Amendment right to privacy.

In response to criticism that Carnivore violates internet privacy, the United States Department of Justice ("DOJ") conducted the only official examination of Carnivore by briefly suspending the program for a strictly technical review. The DOJ confirmed that Carnivore successfully met the FBI’s claims of technical ability. With a stamp of approval, the DOJ concluded its federal inquiry into Carnivore without conducting any constitutional review. Moreover, this failure to constitutionally assess Carnivore signifies the FBI’s official initiation into boundless internet surveillance.

---

6. See ACLU v. Reno, 217 F.3d 162, 169 (3d Cir. 2000) (the court described the internet as "fundamentally and profoundly anti-spatial. You cannot say where it is or describe its memorable shape and proportions or tell a stranger how to get there. But you can find things in it without knowing where they are. The [Internet] is ambient—nowhere in particular and everywhere at once.") (citing Doe v. Roe, 955 P.2d 951, 956 (Ariz. 1998)).


8. U.S. CONST. amend. IV.


10. See discussion infra Part III.

11. See discussion infra Part IV.


The DOJ intended its technical review to address public concern that Carnivore violates internet privacy. However, Carnivore’s capacity to perform exactly as the FBI claims only magnifies public concern. Capable of exposing nearly all internet communications, only federal statutes limit Carnivore. Unfortunately, because the government principally tailored current surveillance statutes to regulate telephones, the surveillance statutes fail to adequately protect the internet user’s Fourth Amendment right to privacy.

Upon completion of the DOJ review, the courts and legislators now face two options for controlling Carnivore. First, they can stand by current federal statutes, ignoring the fact that the internet transmits more personal information than previous technology. Second, they can accept the more difficult challenge of creating new internet-specific surveillance laws that ensure less encroachment on Fourth Amendment privacy. New technologies open new avenues of abuse, both by criminals and the government. This Comment acknowledges that law enforcement has a legitimate place on the internet. However, replacing technologically insufficient surveillance laws with internet-specific surveillance laws is necessary to prohibit law enforcement from exploiting technology and infringing on individual rights to privacy.

Part II of this Comment begins with a brief history of how the courts and legislators balance law enforcement’s duty to protect the public from crime against society’s expectations for Fourth Amendment privacy. Part III illustrates the FBI’s design of Carnivore’s protocol with current surveillance laws in mind. Part IV criticizes Carnivore as an unconstitutional means of electronic surveillance. This section also proposes new internet-specific legislative strategies to protect users’ Fourth Amendment right to privacy. Finally, Part V concludes with suggestions for a future course of action to tame Carnivore.

---

16. See id.
17. See discussion infra Part III.
18. See discussion infra Part IV.
19. See discussion infra Part II.
II. JURISPRUDENCE AND LEGISLATION REGULATING ELECTRONIC SURVEILLANCE

A. Early Foundation of Modern Surveillance Regulation: From the Supreme Court to Congress

The Fourth Amendment of the United States Constitution protects "the right of the people to be secure in their persons, houses, papers and effects." It also guards against unreasonable searches, declaring that courts may issue warrants only after law enforcement establishes probable cause. In 1928, the Supreme Court addressed the delicate balance between the Fourth Amendment's assurance of privacy and law enforcement's desire to monitor criminal suspects by phone tapping. In *Olmstead v. United States*, the Court held that federal law enforcement can forego the warrant requirement when tapping a suspect's phone line to monitor a conversation. The Court reasoned that the Fourth Amendment only guards against the government's physical trespass on a constitutionally protected area, such as the subject's home, and not against access to an outside phone line.

Justice Brandeis' dissent in *Olmstead*, however, established the Court's reasoning in subsequent decisions expanding the Fourth Amendment's reach. Brandeis boldly posited that unchecked government abuse of surveillance technologies is unconstitutional espionage. He accurately predicted the modern reality of internet surveillance when he envisioned, "the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to

20. U.S. Const. amend. IV.
21. Id.
23. 277 U.S. 438 (1928).
24. See id. at 466.
25. See id. In deciding whether the telephone owner intended to project his voice outside of his home by using the telephone, the Court found "the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment." Id.
26. Id. at 471-85 (Brandeis, J., dissenting).
27. See, e.g., Katz v. United States, 389 U.S. 347, 353 (1967) (holding the Court's decisions eroded the opinion in *Olmstead* so that the trespass doctrine, or the idea that the Fourth Amendment only protects from the government's physical invasion or trespass of a home, no longer controlled).
expose to a jury the most intimate occurrences of the home." As the foundation for judicial interpretations of the Fourth Amendment, Brandeis' specter prevails in modern legislative efforts to protect Fourth Amendment privacy while granting law enforcement access to the internet.

Overruling *Olmstead*, the Supreme Court adopted Brandeis' dissent in *Katz v. United States*. As a result, federal legislators acted quickly to regulate federal law enforcement surveillance and to protect the individual's right to privacy. Congress adopted the Privacy Act of 1974 ("Privacy Act") to broadly balance the government's collection, use and protection of personal information with the Fourth Amendment right to privacy. The Privacy Act's central theme of minimizing collection of personal information and maximizing public protection laid the foundation for a wide range of personal information laws such as electronic surveillance.

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") to regulate federal surveillance over electronic communications systems. The ECPA permits and regulates two different electronic media monitoring techniques. One technique is a wiretap that

---

29. *Id.* As internet access grows, computer users reveal more personal identity as they browse different websites. See Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 *Yale L.J.* 1093, 1095 (1996). Even under current wire-tap regulations, Carnivore gives the FBI access to any internet conduct within the bounds of their warrant. See discussion infra Part III.

30. *FBI's Carnivore Internet Sifting Software: Panel II of a Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong.* (2000) (oral statement of Rep. Spencer T. Bachus, Member, House Subcomm. on the Constitution) [hereinafter *FBI's Carnivore*]. While discussing Carnivore, Representative Bachus concluded: "I think Justice Brandeis predicted about 40 years ago that one day the government would be able to come into your home and basically determine everything you did and said. And I think maybe that day's arrived." *Id.*


33. 5 U.S.C § 552a(e) (1994).

34. *Id.*

35. See generally *Cody*, supra note 22, at 1197–1202. Cody discusses the diverse federal legislation protecting personal information privacy in an array of public and private sectors such as electronic communications, cable television and modems, banking, video rentals and, of course, the government. *Id.*


37. *Id.* § 2510(14) (defining an electronic communications system as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications").

38. *Id.* §§ 2510–22, 3121–27.
enables the FBI to intercept the electronic communication and record the content for evidence. The other technique allows the FBI to identify the source information with a pen register.

Both techniques have numerous requirements the FBI must satisfy before conducting the surveillance. If the FBI deviates from these restrictions, the ECPA mandates procedural penalties, such as excluding the evidence. However, these two surveillance techniques vastly differ in their approval requirements because court authorization for pen register surveillance has fewer bureaucratic hurdles and a significantly lower criteria for judicial approval. Additionally, pen register surveillance triggers less severe penalties for unlawful monitoring than content interception.

B. The Strict Legislative Hurdles Regulating Content Interception Surveillance

To monitor and record the contents of electronic transmissions, the FBI agent first submits an application to the Attorney General’s office to obtain court authorization. If the Attorney General finds that the surveillance will provide evidence of a crime under one of the enumerated felonies, the agent must further justify this request by submitting a

39. Id. §§ 2510–22.
40. Id. §§ 3121–27. A pen register is “a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.” Id. § 3127(3). A trap and trace device “captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.” Id. § 3127(4) (1994 & Supp. IV 1998). Because both devices accomplish the same goal, namely capturing the number dialed or providing the number of the person who dials, this Comment hereinafter refers to both devices as a pen register device.
41. Id. §§ 2516, 2518, 3121–23.
42. 18 U.S.C. §§ 2511–12, 2516, 2520–22, 3121.
43. See id. § 3122.
44. See id. § 3123(a).
45. See id. § 3121(d).
46. See §§ 2516, 2518, 2520.
48. See id. § 2516(1).
detailed writing to a court "of competent jurisdiction," typically a federal district court.  

The court will grant approval if it finds: 1) probable cause for the agent's belief that the suspect committed or will commit the particular crime; 2) probable cause for the agent's belief that they will obtain information relating to the crime by the interception; 3) the alternatives have failed or reasonably appear likely to fail in the future and 4) probable cause for the agent's belief that the suspect leases, owns or commonly uses the premises to be monitored.  

Judicial approval requires probable cause for three out of four of the elements noted above. Therefore, the statute remains consistent with the Katz probable cause requirement for a lawful warrant to search a suspect's person, property, papers or effects. The judge’s order strictly limits the surveillance to a specific individual, location and communication for a period no longer than necessary to gather the information, with a statutory maximum of thirty days.  

In addition to the strict civil and criminal ramifications for the illegal interception of electronic transmissions, regulations further punish the agents who overstep their bounds by suppressing illegally obtained evidence. The regulations also allow the criminal suspect to appeal a prior judgment based on the illegal transmission.  

Indeed, authorization for electronic content surveillance presents the FBI with a time-consuming and onerous burden because of the procedural hurdles, high constitutional threshold for judicial approval and steep  

49. Id. § 2518(1) (1994 & Supp. IV 1998). Among the many requirements, an FBI agent's statement must include: a complete statement of the facts identifying the suspect and justifying the need to monitor the suspect's electronic transmissions, any failed alternative attempts made to gather the information, the reason why alternative means are too dangerous and probable cause to believe the suspect will conduct similar subsequent transmissions. Id.  


52. Id. § 2518(3)(b).  
53. Id. § 2518(3)(c).  
54. Id. § 2518(3)(d).  
55. See id. § 2518(3).  
56. Katz v. United States, 389 U.S. 347, 358–59 (1967); see also U.S. CONST. amend. IV.  
59. Id. § 2518(10)(a).  
60. Id. § 2518(10)(b).
consequences for violation of the order. Conversely, approval to gather source information with a pen register is significantly easier for the FBI to obtain.

C. More Lenient Legislative Guidelines Regulating Pen Register Source Information Surveillance

The Supreme Court’s decision in *Smith v. Maryland* forged the critical distinction between the two modes of surveillance—content interception and source information collection. In *Smith*, the Court held that a pen register surveillance is not a search under the Fourth Amendment, and thus does not require a warrant based on probable cause. The holding prompted legislators to create specific pen register laws that vastly differed from content interception regulations.

Unlike the content surveillance authorization, the pen register surveillance requires neither approval from the Attorney General’s office, nor restriction of information collection to limited enumerated felonies. The agent need only file an application in court, certifying that the information is “relevant to an ongoing criminal investigation.”

The standard for judicial approval is equally low. *Smith* determined that the Fourth Amendment does not protect source information gathered by installation and use of a pen register. Therefore, the judge need only

---

61. Because they are the most relevant to Carnivore, this Comment only discusses five of the twelve subsections of § 2518. The remaining seven sections present the FBI with similarly stringent requirements and equally harsh penalties. See id. § 2518.


63. 442 U.S. 735 (1979).

64. Id. at 745 (holding phone number collection with a pen register does not require a warrant because the “petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not ‘legitimate’”).


66. Compare § 3122 (stating that the agent may request the source or address information order if the information sought is “relevant to an ongoing criminal investigation being conducted by that agency”), with § 2516 (requiring the agent submit an application to apply for a content interception court order, and that the information sought may provide evidence of a list of limited enumerated felonies).

67. Id. § 3122.

68. Compare § 2518(3) (requiring the judge find probable cause related to criminal suspicion and surveillance for three of the four judiciary conclusions before issuing a content interception order), with § 3123(a) (1994 & Supp. IV 1998) (ordering the judge find that the pen register order is relevant to an ongoing criminal investigation).

find that the information sought by the FBI relates to its criminal investigation.\textsuperscript{70}

Like the content interception warrant, the pen register order is limited to a specific person and place.\textsuperscript{71} Yet, unlike content interception orders, pen register orders allow a maximum of sixty days of surveillance, which is twice as long as the thirty days of surveillance permitted under content interception orders.\textsuperscript{72}

Finally, the penalties are less severe for illegal pen register surveillance than illegal content interception surveillance.\textsuperscript{73} Pen register laws fail to provide civil damages similar to those imposed for content interception regulations.\textsuperscript{74} Further, pen register laws also fail to include an express evidentiary provision to suppress illegally obtained evidence or allow an appeal for a conviction based on such evidence.\textsuperscript{75}

The critical legislative difference between the ease of obtaining a pen register order and the difficulty of obtaining a content interception order evolved from the \textit{Smith} ruling that excludes source collection from Fourth Amendment protection.\textsuperscript{76} It is bureaucratically easier for the FBI to apply for a pen register surveillance order.\textsuperscript{77} The courts may also grant an order based on a finding that the information gathered would be relevant to the criminal investigation.\textsuperscript{78} Coupled with the lack of civil, evidentiary or severe criminal penalties,\textsuperscript{79} pen register surveillance is an easily implemented and powerful weapon in the FBI’s arsenal against crime.

\begin{itemize}
  \item[70.] § 3123(a).
  \item[71.] \textit{Id.} § 3123(b).
  \item[72.] \textit{Compare} § 2518(5), \textit{with} § 3123(c).
  \item[73.] \textit{Compare} § 3121(d) (providing the penalty for violating the pen register surveillance requirements is a fine and/or no more than one year in prison), \textit{with id.} §§ 2511–12, 2518(10), 2520–22 (imposing an extensive and detailed scheme for civil, evidentiary and significantly more imposing criminal penalties for violating content interception requirements).
  \item[74.] \textit{Id.} § 2520.
  \item[75.] \textit{Id.} § 3121(d).
  \item[76.] \textit{Smith}, 442 U.S. at 745–46.
  \item[77.] \textit{Compare} §§ 2516, 2518 (requiring more application steps than the pen register court order applications), \textit{with} §§ 3122–23 (imposing less application steps than the content interception order applications).
  \item[78.] \textit{Compare} §§ 2518(3)(a)–(d) (requiring the judge find probable cause related to criminal suspicion and surveillance for three of the four judiciary conclusions before issuing a content interception order), \textit{with} § 3123(a) (ordering the judge find the pen register order relevant to an ongoing criminal investigation).
  \item[79.] \textit{See id.} § 3121(d) (imposing a fine and/or less than one year in prison for violating the pen register order requirements).
\end{itemize}
III. FBI’S VALIDATIONS FOR CARNIVORE AND ITS CONTROVERSIAL PUBLIC HISTORY

A. Federal Law Enforcement’s Justifications and Expectations for Carnivore

Carnivore is the FBI’s newest technological weapon against crime facilitated by the internet.\(^{80}\) While law enforcement candidly admits that the name draws negative attention,\(^{81}\) Carnivore is nevertheless a voracious internet surveyor with mind boggling speed and “surgical” precision.\(^{82}\)

1. Executive Inquiry into Internet Crime

In March 2000, the President’s Working Group on Unlawful Conduct on the Internet (“Working Group”), a branch of the DOJ, released a report documenting the rise of unlawful conduct on the internet.\(^ {83}\) Focusing on crime’s growing technological sophistication,\(^ {84}\) the Working Group found that criminals used the internet to commit “traditional crimes.”\(^ {85}\)

The Working Group reported that the internet, primarily through e-mail and chat rooms, facilitates the gamut of criminal conduct because the internet offers privacy, quick file transfer speed, accuracy, “one-to-many” broadcast ability and other communications features.\(^ {86}\) The Working Group characterized the internet as a safe haven for criminal conduct such as securities and internet fraud; child pornography; illegal prescription

---

80. *Carnivore Diagnostic*, supra note 50.
82. *Carnivore Diagnostic*, supra note 50.
83. President’s Working Group, supra note 4, at 8 (providing evidence that by the end of 2003, there will be 177 million American internet users and 502 million users worldwide).
85. President’s Working Group, supra note 4, at 6.
86. Id. at 12.
drug, controlled substance, firearm and alcohol sales; gambling; software piracy and intellectual property theft.\textsuperscript{87}

Based on its own conclusions about internet crime, the FBI found that the internet facilitates more violent criminal conduct.\textsuperscript{88} The FBI advised that monitoring internet communications would help prevent terrorism, espionage, child pornography, sexual exploitation of children, serious fraud and "information warfare."\textsuperscript{89}

To meet the constitutional and regulatory requirements of the Fourth Amendment and the ECPA,\textsuperscript{90} law enforcement relies on the assumption that internet use is analogous to telephone use.\textsuperscript{91} Following from this technological analogy, the FBI and DOJ concluded that current surveillance laws under the ECPA\textsuperscript{92} are more than sufficient to safeguard the internet user's Fourth Amendment right to privacy.\textsuperscript{93}

\textsuperscript{87} See id. (emphasizing in the appendices that, except the illegal sale of alcohol, federal law enforcement agencies need more resources to conduct effective online investigations).

\textsuperscript{88} See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).

\textsuperscript{89} Id. The FBI defines information warfare as the threat that foreign militaries, "[k]nowing that they cannot match our military might," will develop programs to attack our national infrastructure. Id. The FBI fears that information warfare will be more apocalyptic to our national security than weapons of mass destruction. Id.

\textsuperscript{90} See discussion supra Part II.

\textsuperscript{91} President's Working Group, supra note 4, at 12 (emphasizing "the use of computers and modern telecommunications facilities as tools (analogous to the use of telephones as tools) to commit an offense."); David McGuire, FBI Defends 'Carnivore' Cyber-Snoop Device, NEWSBYTES, July 11, 2000 (quoting FBI spokesperson Paul Bresson who claimed that Carnivore is merely an extension of the FBI's wiretapping practices to e-mail).

\textsuperscript{92} See discussion supra Part II.

\textsuperscript{93} See, Digital Privacy, supra note 3 (prepared statement of Kevin V. DiGregory, Deputy Assistant Att'y General, Criminal Div., U.S. Dept of Justice) (claiming that current surveillance regulations, in the context of the internet, are constitutional and impose DOJ privacy protection measures that go beyond constitutional requirements); Carnivore Diagnostic, supra note 50 (detailing the application process for a content interception order pursuant to the ECPA and characterizing this process as much more difficult than attaining "typical search warrants"); Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 106th Cong., 11-12 (2000), (prepared statement of Donald M. Kerr, Assistant Dir., FBI) (emphasizing that the federal surveillance laws promote the Fourth Amendment "with deference to the privacy of intercepted subjects and with deference to the privacy of those who are not the subject of the court order") [hereinafter Fourth Amendment Issues].
2. The FBI’s Response to Internet Crime: Carnivore’s Birth

Two years ago, unbeknownst to the DOJ, the FBI implemented Carnivore to monitor criminal activities on the internet. Carnivore is essentially a commercial “sniffer,” which is a program that internet service providers (“ISP”) employ to intercept digital information passing through their servers. Consisting of both hardware, referred to as a “black box,” and software that the FBI attaches to an ISP’s system, Carnivore filters all the digital code that passes through the ISP’s server. The FBI programs Carnivore to retain information described in the court order for the amount of time the surveillance statute permits. Because the FBI can already constitutionally access information stored on a server or hard drive under other provisions of the ECPA, Carnivore collects data in real-time, or at the same time the information streams through the server. Carnivore can collect any digitally transmitted information such as the suspect’s e-mail, instant messaging, chat-room discussions, financial transactions and websites visited.

Once the FBI gains surveillance approval by a court order, the FBI agent, with help from the ISP’s representative, installs Carnivore onto the ISP’s network. Because the ECPA mandates cooperation, the ISP may

94. See Digital Privacy, supra note 3 (oral statement of Martha Stansell-Gamm, Chief, Computer Crimes, U.S. Dep’t of Justice) (responding to Sen. Hatch’s query about the DOJ’s reported lack of involvement with, or knowledge of, Carnivore until the press exposed the program: “I simply don’t know at what point the attorney general became aware of this specific tool or the name of the tool.”).

95. Id. (prepared statement of Donald M. Kerr, Assistant Dir., FBI).

96. Carnivore Diagnostic, supra note 50 (stating that private ISPs and companies regularly purchase and employ commercial sniffers to capture information on their servers). The FBI distinguishes Carnivore from the commercial sniffers in that Carnivore captures only limited information, whereas commercial sniffers capture everything transmitted through ISPs. Id.

97. Qaisar Alam, E-mail Surveillance: Carnivore Cornered, COMPUTERS TODAY, Oct. 31, 2000, at 48.

98. Digital Privacy, supra note 3 (statement of Donald M. Kerr, Assistant Dir., FBI).

99. Id.


101. See Digital Privacy, supra note 3 (statement of Donald M. Kerr, Assistant Dir., FBI).


103. See discussion supra Part II.

104. See Fourth Amendment Issues, supra note 93 (prepared statement of Donald M. Kerr, Assistant Dir., FBI) (stating that “[t]o date, Carnivore has, to my knowledge, never been installed onto an ISP’s network without assistance from the ISP’s technical personnel”).
not prevent the FBI from installing Carnivore on its system. After installing the device, the agent, without the ISP's help, programs the software to filter out all information of a suspect's internet use, restricted by the ECPA guidelines in the court order.

Once installed, Carnivore operates in four stages. First, Carnivore filters, at forty million mega-bits per second or faster, all of the digital information that streams through the ISP. Thus, Carnivore processes all information originating from non-suspect internet users. The FBI claims that while filtering the code, Carnivore detects and segregates only the surveillance information that conforms with the court order.

Once Carnivore segregates the relevant information, the second stage begins. Carnivore further filters the data based on the type of ECPA surveillance order and court restrictions. The FBI claims that the second stage "is where some of Carnivore's key legal, evidentiary, and privacy-enhancing features really kick in." For example, the program can retain e-mail address information as permitted by a pen register order, while disposing of any other data that would violate the ECPA court order.

In the third stage, Carnivore stores the collected information for the agent's review. If properly conducted, the search provides the agent with only the information that the court expressly authorized.

Carnivore then finalizes its surveillance by recording the FBI search protocol. As a prerequisite to admitting Carnivore's search results into

---

105. See 18 U.S.C. §§ 2518(4), 3124(a)–(b) (1994) (ordering the communications provider shall furnish law enforcement with all "information, facilities, and technical assistance" to facilitate the content or source information surveillance).

106. See, e.g., Carnivore Diagnostic, supra note 50 (stating that if the court order is only for an e-mail search, the agent must program Carnivore to intercept only the suspect's e-mail).

107. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).

108. Id. To illustrate Carnivore's speed, Donald Kerr analogizes: "To visualize this, imagine a huge screen containing 40 million O's [sic] and I's flashing by on this screen for one second, and for one second only." Id.

109. Id.

110. Id.

111. Id.

112. Id.

113. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).

114. See discussion infra Part IV (casting doubt on the FBI's claim that Carnivore will consistently produce results conforming to the court order).

115. Carnivore Diagnostic, supra note 50.

116. Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).
evidence, the FBI must illustrate an unadulterated evidentiary chain. The best proof of this chain is an FBI programmer’s testimony that the search protocol adhered to the court order. Moreover, by automatically appending the search protocol to the results, Carnivore authenticates the evidence so the court will not have to speculate about over broad search results in violation of the court order.

Clearly, the Working Group’s wish for federal computer crime surveillance training, resources and tools came true when it discovered Carnivore and other similar technology. Since public discovery of Carnivore, both the FBI and DOJ continue to advance the constitutionality of Carnivore while failing to conduct a public, in-depth review. The program’s brief and controversial public history, however, reveals that other groups are skeptical of Carnivore’s ability to comply with Fourth Amendment privacy rights.

B. Carnivore’s Heavily Scrutinized Public History

To avoid facing Fourth Amendment and federal surveillance statutory criticisms threatened by this Orwellian dilemma, the FBI tailored Carnivore’s protocol to adhere to the ECPA. Because the ECPA mandates ISP submission to FBI searches, Carnivore allows the FBI unlimited, real-time access to everything that passes through the monitored

117. See id.; FED. R. EVID. 901.
118. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).
119. See id.
120. President’s Working Group, supra note 4, at 25–31; Digital Privacy, supra note 3 (statement of Martha Stansell-Gamm, Chief, Computer Crimes, U.S. Dep’t of Justice) (revealing that for the past three years, federal agencies employed many similar programs such as Omnivore, Network Intrusion Defense System and SNIFFY). Id. Martha Stansell-Gamm also admitted that these programs provided agencies with even less selection, discretion and control than Carnivore. See id. This suggests that federal agencies have already violated internet user’s Fourth Amendment privacy.
121. Compare Digital Privacy, supra note 3 (statement of Donald M. Kerr, Assistant Dir., FBI) (justifying Carnivore’s procedures as consistent with the Fourth Amendment), with Digital Privacy, supra note 3 (statement of Kevin V. DiGregory, Deputy Assistant Att’y General, Criminal Div., U.S. Dep’t of Justice) (illustrating that the DOJ and the FBI take similar positions finding Carnivore consistent with the Fourth Amendment).
122. See discussion infra Part III.B.
123. Digital Privacy, supra note 3 (oral statement of Sen. Orrin G. Hatch, Member, S. Judiciary Comm.) (predicting that “individuals who use the Internet for personal communications, purchases and hobbies are justifiably reluctant to allow an Orwellian Big Brother to monitor which web sites they visit or what messages they send through cyberspace”).
125. Id. §§ 2518(4), 3124(a)-(b).
ISP. Despite the FBI's reassurances that the program enhances internet privacy,126 privacy experts,127 the internet industry,128 the press129 and federal lawmakers voiced their fears of Carnivore. As a result, the House and Senate both held Judiciary Committee Hearings immediately after Carnivore's public exposure.130 These hearings served to clarify what Carnivore actually accomplishes and whether Carnivore protects the privacy of non-criminal internet users.131

After the FBI revealed to the House and Senate Judiciary Committees that it had secretly used Carnivore twenty-five times in its first two years,132 Carnivore became very unpopular. Immediately proceeding the House Judiciary Committee Hearing,133 twenty-eight members of Congress wrote Attorney General Janet Reno, demanding that she shut down Carnivore.134 While the DOJ did not terminate the program, it ultimately responded to public and political criticism by suspending Carnivore for an independent135 technical review.136

126. See Carnivore Diagnostic, supra note 50.


128. E.g., Del Quentin Wilber, FBI Taps of E-mail Provoke Concerns; Privacy Issues Lead to House Hearings on 'Carnivore' Work; Name Called 'Unfortunate,' THE BALTIMORE SUN, July 24, 2000, available at http://www.newslibrary.com/deliverccdoc.asp?SMH=60919 (discussing ISP criticisms of Carnivore, including the efforts of Earthlink to prevent the FBI from installing Carnivore on its network).

129. E.g., Neil King, Jr., FBI'S Wiretaps to Scan E-Mail Spark Concern, WALL ST. J., July 11, 2000, at A3 (exposing Carnivore to the public for the first time).

130. See generally Fourth Amendment Issues, supra note 93, at 2 (opening statement of Rep. Canady, Chairman, Subcomm. on the Constitution of the House Comm. on the Judiciary) (noting the hearing was to address the interests of Fourth Amendment protection and law enforcement).

131. See id.

132. Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).

133. FBI's Carnivore, supra note 30. The hearing took place on July 24, 2000. Id.


135. Press Release, ACLU, ACLU Says Government Stacked Deck in Selection of Team to Review "Carnivore" Cyber-tapping System (Oct. 4, 2000), available at http://www.aclu.org/news/2000/n100400.html [hereinafter ACLU Press Release]. While it is a clear conflict of interest to have the DOJ review Carnivore, computer privacy advocates criticized the DOJ's "independent" review team because the team consisted of many former law enforcement agents, including a former DOJ official and President Clinton's information policy advisor. Id.

Following the hearings, the DOJ contracted with the Illinois Institute of Technology Research Institute ("IITRI") to test Carnivore in various model scenarios simulating law enforcement's likely use of the program to determine Carnivore's "design, function and method of use." Essentially, the IITRI review addressed concerns that Carnivore is a technically insecure tool, impairs an ISP's network and leaks more data than FBI surveillance court orders authorize. Computer privacy advocates expressed further concern that, if Carnivore's interceptions result in exposing too much information about the ISP's non-suspect customers, the FBI or a third party will inevitably exploit that information.

In December 2000, the DOJ released the results of the IITRI's technical review that found Carnivore operated as the FBI expected. In its conclusion that Carnivore is technically sound, the IITRI encouraged the FBI to continue using the program. Ultimately, Carnivore's successful technical review bolstered the FBI's claims that Carnivore neither leaks information outside of the court order parameters, nor interferes with the monitored ISP's network.


138. See Contract No. 00-C-0328 for Independent Technical Review of the Carnivore System, U.S. Dep't of Justice, at http://www.usdoj.gov/jmd/pss/ iitricontracttext.pdf (last visited Nov. 9, 2000). One wonders whether IITRI's use of Carnivore violated the Fourth Amendment and the federal statutes, especially because they probably did not apply for a court order with every test conducted.

139. Id. After describing the adverse reaction Carnivore generated in the media, Congress and general public, in the contract introduction, the DOJ poses four questions in Section ES.1 as the technical review objectives:

1. Assuming proper usage, will the Carnivore system provide investigators with all the information, and only the information, that is designed and set to provide in accordance with a given court order?

2. Assuming proper usage, will use of the Carnivore system introduce new, material risks of operational security impairment of an ISP's network?

3. Does use of the Carnivore system introduce new, material risks of the unauthorized acquisition, whether intentional or unintentional, of electronic communication information by (i) FBI personnel or (ii) persons other than FBI personnel?

4. Are the protections built into the Carnivore system, including both audit functions and operational procedures or practices, commensurate with the level of the risks, if any, identified in response to (3) above?

140. See ILL. INST. OF TECH., supra note 14, at xii.

141. Id. at xiv (stating law enforcement should "[c]ontinue to use Carnivore ... because Carnivore can be configured to reflect the limitations of a court order").

142. See id. at xii. In its conclusions, the IITRI answered the DOJ's four questions, declaring:
Despite these test results, Carnivore’s critics maintain that the program is vulnerable to abuse until the FBI releases the source code to the public.\textsuperscript{143} From the moment the DOJ announced the IITRI review team, critics alleged that the DOJ assembled a biased review panel because nearly all of their team had strong federal government and law enforcement ties.\textsuperscript{144}

Moreover, because the DOJ conducted a technical, rather than legal review,\textsuperscript{145} the IITRI study addressed only a minor part of the public controversy over Carnivore. Carnivore’s technical review gave the FBI official justification for the program’s full implementation. However, the DOJ’s failure to conduct a legal review of the program prompted computer privacy advocates to use the Fourth Amendment to criticize Carnivore.

---

1. When Carnivore is used in accordance with a Title III order, it provides investigators with no more information than is permitted by a given court order. When Carnivore is used under pen trap authorization it collects TO and FROM information, and also indicates the length of messages and the length of individual field within those messages possibly exceeding court-permitted collection.

2. Operating Carnivore introduces no operational or security risks to the ISP network where it is installed unless the ISP must to [sic] make changes to its network to accommodate Carnivore. Such changes may introduce unexpected network behavior.

3. Carnivore reduces, but does not eliminate, risk of both intentional and unintentional unauthorized acquisition of electronic communication information by FBI personnel, but introduces little additional risk of acquisition by persons other than FBI personnel.

4. While operational procedures or practices appear sound, Carnivore does not provide protections, especially audit functions, commensurate with the level of the risks.

Id.

143. See FBI’s Carnivore, supra note 30 (oral statement of Barry Steinhardt, Assoc. Dir., ACLU) (criticizing the FBI’s “[T]rust us; we do not know how this black box works” explanation offered to privacy advocates concerned with Carnivore); Digital Privacy, supra note 3 (statement of James X. Dempsey, Senior Staff Counsel, Ctr. for Democracy and Tech.) (claiming that the first problem with Carnivore is “we don’t know how it works.”); Press Release, Electronic Privacy Information Center, Lawsuit Seeks Immediate Release of FBI Carnivore Documents (Aug. 2, 2000), available at http://www.epic.org/privacy/carnivore/8_02_release.html (announcing the Electronic Privacy Information Center’s Freedom of Information Act lawsuit against the FBI and DOJ to request more detailed information on Carnivore).

144. ACLU Press Release, supra note 135.

145. ILL. INST. OF TECH., supra note 14, at xiv (stating that “IITRI specifically excluded questions of constitutionality”).
IV. BALANCING PRIVACY AGAINST GOVERNMENT INTERESTS: RESTRICTING CARNIVORE TO MAXIMIZE THE INTERNET USER'S FOURTH AMENDMENT PRIVACY RIGHTS WHILE RESPECTING LAW ENFORCEMENT'S NEED FOR INTERNET SURVEILLANCE

As internet use increases, our lives and identities grow more digitized every day. Today, an internet user can literally survive without ever leaving home. The internet is a massive system of connections and digital code that transmits personal information ranging from business transactions and online consumer purchases to simple recreational digital conversation.

Transmitting personal information on the internet leaves the user vulnerable to those who might exploit that content. ISPs encourage people to participate in online transactions by implementing security measures to raise expectations regarding internet privacy. The FBI claims that installing Carnivore onto an ISP enhances internet security because it helps them catch cyber criminals. Unfortunately, critics find it difficult to believe this reassurance because Carnivore expands the FBI's ability to monitor people's lives by gathering information that traditional telephone surveillance would never reveal.

The DOJ's review of Carnivore leaves constitutional objections unresolved. Because the FBI and DOJ rely on the analogy that the internet is like a telephone, federal law enforcement will stand by their.

146. See Adler, supra note 29, at 1095 (explaining some of the increasing advantages of the internet).
148. Paul Swart, Chip Equipment Firms Bullish at Semicon West, ELECTRONIC TIMES, July 24, 2000, at 16 (stating that "the Internet is playing an ever greater role in business and personal lives, the massive network will generate and drive demand for many types of devices that will hook up to the Net—from smart home appliances such as microwave ovens that are remotely controlled by specialised [sic] websites, to Web-capable cellphones to TV set-top boxes and palm-type information appliances").
149. Id.
150. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).
151. See discussion infra Part IV.A.1.
152. See ILL. INST. OF TECH., supra note 14, at xiv (acknowledging that although IIRTI specifically excluded constitutional questions from its review, it warned that "the presence of Carnivore and its successors without safeguards . . . 1) fuels the concerns of responsible privacy advocates and reduces the expectations of privacy by citizens at large and 2) increases public concern about the potential unauthorized activity of law enforcement agents").
claims that Carnivore is constitutional under current surveillance regulations and prior U.S. Supreme Court decisions.\textsuperscript{153}

On the other hand, privacy advocates promise not to back down from their criticism that Carnivore, while possibly technologically sound, is unconstitutional.\textsuperscript{154} Legal precedent, the FBI's wiretapping protocol and the inherent technological differences between the internet and the telephone suggest that even a perfectly functional Carnivore compromises privacy rights under the Fourth Amendment.\textsuperscript{155}

\textbf{A. Raising the Judicial Standard: Using Legal Precedent To Protect Pen Register Source Information Surveillance Under the Fourth Amendment}

1. Carnivore's Source Information Collection on the Internet Substantially Differs from Pen Register Searches on a Telephone

Assuming Carnivore operates exactly as the FBI claims,\textsuperscript{156} law enforcement's collection of source information via current ECPA pen register regulations violates the Fourth Amendment despite the FBI's meticulous efforts to tailor Carnivore to ECPA standards.

\textit{Katz v. United States}\textsuperscript{157} is the foundation for today's Fourth Amendment surveillance regulations.\textsuperscript{158} In \textit{Katz}, the Supreme Court focused on the individual's privacy expectations when determining whether the individual deserves Fourth Amendment protection from government surveillance.\textsuperscript{159} The Court ruled the Fourth Amendment prevents the government from probing information that the individual "seeks to preserve as private, even in an area accessible to the public,"\textsuperscript{160} without a warrant based on probable cause.\textsuperscript{161} Furthermore, the Court pointed out that the Fourth Amendment does not protect information the individual "knowingly exposes to the public, even in his own home or office."\textsuperscript{162}

\textsuperscript{153} See discussion supra Parts II–III.
\textsuperscript{154} See FBI's Carnivore, supra note 30 (oral statement of Barry Steinhardt, Assoc. Dir., ACLU); Digital Privacy, supra note 3 (oral statement of Michael O'Neill, Assistant Professor, George Mason Univ. Law Sch.; Comm'r U.S. Sentencing Comm'n); Digital Privacy, supra note 3 (oral statement of James X. Dempsey, Senior Staff Counsel, Ctr. for Democracy and Tech.).
\textsuperscript{155} See discussion infra Parts IV.A–D.
\textsuperscript{156} See discussion infra Part III.B.
\textsuperscript{157} 389 U.S. 347 (1967).
\textsuperscript{158} See Cody, supra note 22, at 1194.
\textsuperscript{159} Katz, 389 U.S. at 351–52.
\textsuperscript{160} Id. at 351.
\textsuperscript{161} See id. at 358–59.
\textsuperscript{162} Id. at 351.
In *Smith v. Maryland*, the Supreme Court summarized the privacy expectation test by adopting Justice Harlan's concurrence in *Katz* and posing two questions: 1) does the individual's conduct show they subjectively expected privacy, and, if so, 2) does society recognize that expectation as reasonable? The Fourth Amendment will protect that individual's information only if the court finds an affirmative answer to both questions.

To decide whether pen register surveillance requires Fourth Amendment probable cause, the *Smith* Court adopted the holding in *United States v. New York Telephone Co.* The Court held that a pen register only discloses the telephone numbers a suspect dials, while preventing the disclosure of "any communication between the caller and the recipient of the call, their identities . . . [and] whether the call was even completed." Based on this definition, the *Smith* Court concluded that a pen register has "limited capabilities."

Applying the *Katz* test to the pen register's limited capabilities, the Court found that because phone companies employ pen registers and telephone subscribers receive an itemized phone bill, "it is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret." Additionally, the Court emphasized that because the automated switchboard is "the modern counterpart" of the human operator switchboard, the Constitution will not grant special protection for individuals just because of subsequent automation.

Ultimately, the *Smith* Court concluded that the petitioner failed the *Katz* test because he did not subjectively expect privacy in the numbers he dialed, and "even if he did, his expectation was not 'legitimate.'" Additionally, the *Smith* Court held that because a reasonable person cannot justifiably expect the numbers they dial to be confidential, pen register

---

164. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *Smith*, 442 U.S. at 740.
165. See *Smith*, 442 U.S. at 740.
169. *Id.* at 743.
170. *Id.* at 744.
171. *Id.* at 744-45.
172. *Id.* at 745.
surveillance, even without probable cause, does not violate the Fourth Amendment.\textsuperscript{173}

Today's ECPA surveillance regulations reflect the federal government's statutory restrictions on the \textit{Smith} Court's decision that a pen register search does not require a warrant. The ECPA requires that the FBI obtain approval based on a minimal level of suspicion that the source information sought by a pen register must relate to a criminal investigation before conducting surveillance.\textsuperscript{174} While Carnivore is not a pen register device per se,\textsuperscript{175} the FBI clearly programmed Carnivore to emulate a pen register.\textsuperscript{176} Thus, federal law enforcement's primary justification for Carnivore rests on a broad assumption that Carnivore's implementation is analogous to current telephone surveillance practices.\textsuperscript{177} However, when comparing Carnivore's wide range of capabilities with those of a pen register,\textsuperscript{178} it is clear that Carnivore is not a tool of the same "limited capabilities."\textsuperscript{179}

Carnivore, unlike the pen register, is technologically capable of disclosing "any communication between the caller and the recipient of the call, their identities . . . [and] whether the call was even completed."\textsuperscript{180} Therefore, the \textit{Smith} Court would likely disagree with the FBI's conclusion that Carnivore is technologically analogous to a pen register. Even though the FBI can try to emulate pen register surveillance by programming Carnivore to expel content and retain only source information,\textsuperscript{181} internet source information reveals significantly more detailed information about the user than a mere telephone number could ever demonstrate.\textsuperscript{182}

\begin{thebibliography}{99}
\bibitem{173} Id. at 745–46.
\bibitem{175} \textit{See FBI's Carnivore, supra} note 30 (prepared statement of Tom Perrine, Principal Investigator, Pacific Inst. for Computer Security) (describing the capabilities of Carnivore and the differences between the internet and telephones).
\bibitem{176} \textit{See Digital Privacy, supra} note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI) (discussing how Carnivore operates and complies with EPCA regulations).
\bibitem{177} President's Working Group, \textit{supra} note 4, at 12 (emphasizing "the use of computers and modern telecommunication facilities (analogous to the use of telephones as tools) to commit an offense"); David McGuire, \textit{FBI Defends 'Carnivore' Cyber-Snoop Device, NEWSBYTES, at http://www.newsbytes.com/news/00/15943.html} (July 11, 2000) (citing an FBI contention that Carnivore is merely an extension of the FBI's wiretapping practices to e-mail).
\bibitem{178} \textit{Smith}, 442 U.S. at 741–42.
\bibitem{179} \textit{Id.} at 742.
\bibitem{180} \textit{Id.} at 741 (citing \textit{N.Y. Tel. Co.}, 434 U.S. at 167).
\bibitem{181} \textit{Carnivore Diagnostic, supra} note 50.
\bibitem{182} \textit{FBI's Carnivore, supra} note 30 (oral statement of Alan B. Davidson, Staff Counsel, Ctr. for Democracy and Tech.).
\end{thebibliography}
For instance, if Carnivore were to search e-mail in a manner analogous to a pen register, it would isolate and store only the sender and recipient e-mail addresses.183 Unlike a pen register, however, Carnivore downloads and reads all of the digital code that passes through the ISP for the court order’s duration.184 This means that Carnivore will not only read all of a suspect’s e-mail, but it will also read all other e-mail on the server.185 Additionally, it determines what websites they visit, monitors their chat-room discussions and combs through all of their file transfers.186 Because Carnivore temporarily acquires all of the digital code on the ISP’s network, an overwhelming amount of the code originates from the ISP’s non-criminal clients.187 Furthermore, because e-mails necessarily pass directly through the ISP’s network, Carnivore collects all sender and recipient addresses, instantly recording the exact times senders complete the communication.188

In contrast to Carnivore’s rapid processing speed, wide surveillance ability and technological sophistication, a pen register only produces telephone numbers.189 In United States v. New York Telephone Co., the Court described the pen register as a machine of limited capabilities190 because its surveillance fails to disclose the identities of the callers, does not indicate whether the suspect completed the call and is incapable of the “aural acquisition”191 of anything, it just produces telephone numbers.192 Carnivore, even when programmed by the FBI to operate like a pen register, fails to produce such limited results because it reveals the sender’s and recipient’s identities by collecting e-mail addresses. It also intercepts a

183. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).
184. FBI’s Carnivore, supra note 30 (oral statement of Tom Perrine, Principal Investigator, Pacific Inst. for Computer Security).
185. See id. (oral statement of Alan B. Davidson, Staff Counsel, Ctr. for Democracy and Tech.).
186. See id.
187. See generally id. (oral statement of Stewart Baker, Att’y, Steptoe & Johnson) (discussing how innocent users may be unfairly monitored).
188. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI). Dr. Kerr stated that, because Carnivore operates so quickly, an agent could never review the information passing through it in real-time. Id. However, as long as Carnivore reads transmissions in real-time, it is capable of determining the exact time a user sends an e-mail because it will receive it the moment the user transmits it through Carnivore. Furthermore, Carnivore’s auditing capabilities may include a time stamp if transmission time is important for establishing the evidentiary chain. See id.
190. Id.
suspect's e-mail the instant the sender completes correspondence and temporarily acquires all digital code, the vast majority of which originates from non-suspect internet users.  

In addition, the internet source information Carnivore collects encompasses a diverse array of electronic signatures that attach to all information on the internet. Because the internet provides broad communication abilities through services such as e-mail, web sites, chat rooms and video streaming, source information can include everything from sender and recipient e-mail addresses to an author's identification macro embedded in a transferred file.  

Even when the source does not provide a specific name or e-mail address, source information, like a website's Uniform Resource Locator ("URL"), often reveals the content of the particular website. In fact, even when the URL fails to reveal the content of a website, the FBI is free to access that site to determine whether the suspect employed it for criminal purposes. Carnivore is a "maximization tool," giving the FBI access to all communication sources passing through ISP networks.

Unlike a pen register, Carnivore allows the FBI to probe deeply into a specific person's internet use, exposing more information about that

193. See FBI's *Carnivore*, supra note 30 (oral statement of Stewart Baker, Att'y, Steptoe & Johnson) (discussing how innocent users can be unfairly monitored).

194. See *Digital Privacy*, supra note 3 (oral statement of Dr. Vinton G. Cerf, Member, Bd. of Dirs., Internet Soc'y) (explaining how Carnivore views flowing source information on the internet).

195. See FBI's *Carnivore*, supra note 30 (oral statement of Alan B. Davidson, Staff Counsel, Ctr. for Democracy and Tech.).


197. A URL is a web address where a person can find a website on the internet.

198. URL's such as http://www.eactivist.org, http://www.carprice.com and http://www.porn.com illustrate the pages' general subject matter. A URL may also reveal the terms for which the internet user searches. For example, on the popular search engine, Yahoo! (http://www.yahoo.com), if a user wants to find information on fertilizer, a substance often used to make explosives, the search term "fertilizer" becomes a part of the URL: http://search.yahoo.com/bin/search?p=fertilizer. If the FBI were permitted to monitor URLs under the pen register laws, presumably the FBI could use Carnivore's source information surveillance to investigate similar internet searches without even establishing probable cause so long as their source information collection is relevant to investigating criminal conduct. See 18 U.S.C. § 3122 (1994).


200. Id.
person's identity, private habits and daily personal contacts than a mere telephone number ever reveals.\textsuperscript{201}

2. Carnivore's Source Information Collection Is an Unconstitutional Search Because It Fails the \textit{Katz} Reasonable Expectation of Privacy Test

While the FBI claims it can program Carnivore to emulate a pen register,\textsuperscript{202} clearly Carnivore is not the same surveillance device of limited capabilities upon which the \textit{Smith} Court relied.\textsuperscript{203} Even under the unlikely assumption that the \textit{Smith} Court intended its ruling to apply to a device of such widespread capabilities, Carnivore would still fail the privacy expectation test originating from Harlan's concurrence in \textit{Katz}.\textsuperscript{204}

The \textit{Smith} Court applied the \textit{Katz} two-prong test and found that pen register surveillance does not offend a reasonable expectation of privacy.\textsuperscript{205} In its inquiry, the Court posed two questions: 1) whether the individual's conduct shows a subjective expectation of privacy, and if so, 2) whether society recognizes that expectation as reasonable?\textsuperscript{206} The answer to the first question rests on the individual's subjective intent, but the second question provides the more objective and relevant standard for this test.\textsuperscript{207}

Does society recognize a reasonable expectation of privacy for source information on the internet? Once again, the distinct technological advantages of Carnivore contrasted with the very limited capabilities of a pen register lead to a different answer than the one the \textit{Smith} Court addressed.

\textit{Smith} analyzed the relationship between the telephone user and the telephone company by focusing on the company's business practices to determine whether the customer's expectation of privacy in the phone numbers dialed is reasonable.\textsuperscript{208} The Court ultimately concluded that a reasonable person would not legitimately expect privacy in the phone numbers dialed.\textsuperscript{209} The Court based its decision on three findings. First, the Court found that customers convey their phone numbers to the

\begin{itemize}
\item\textsuperscript{201} See id.
\item\textsuperscript{202} See Carnivore Diagnostic, supra note 50.
\item\textsuperscript{203} See Smith, 442 U.S. at 745–46.
\item\textsuperscript{204} Katz, 389 U.S. at 361 (Harlan, J., concurring).
\item\textsuperscript{205} Smith, 442 U.S. at 745–46.
\item\textsuperscript{206} Id. at 740.
\item\textsuperscript{207} Id. at 741–46. The \textit{Smith} Court primarily focused its analysis on the second question.
\item\textsuperscript{208} Id. at 735.
\item\textsuperscript{209} Id. at 745.
\end{itemize}
telephone company’s switchboard.\textsuperscript{210} Second, the customer knows that the phone company records phone numbers dialed because it sends a list of phone numbers in its long-distance bill.\textsuperscript{211} Finally, even if the user remains “oblivious to a pen register’s esoteric functions,”\textsuperscript{212} the Court presumed that everyone knows that phone companies use pen registers to track calls.\textsuperscript{213} The Court based this finding on the fact that most phone books have a customer information page that states that the phone company can acquire an obscene caller’s phone number for the authorities.\textsuperscript{214} Clearly, these findings do not describe a user’s expectations when communicating on the internet.

The \textit{Smith} Court’s rationale does not apply to internet users for three reasons. First, the internet user does not knowingly convey source information to the ISP in the same way the telephone customer conveys phone numbers to the telephone company. Unlike the telephone switchboard, an ISP’s network has always been a fully computerized system without human operators to physically input websites or e-mail addresses for people.\textsuperscript{215} Although telephone companies continue to employ human operators for certain services despite significant automation,\textsuperscript{216} the internet user is the only human to type in a URL, log onto a chat site or send an e-mail.

Second, while ISPs use sniffers like Carnivore to maintain their systems, much like the phone company uses pen registers in its maintenance,\textsuperscript{217} ISPs do not send a monthly itemized bill.\textsuperscript{218} According to \textit{Smith}, without a billing system such as a monthly itemized statement, people may not even know their ISP employs a sniffer in the first place.\textsuperscript{219}

\textsuperscript{210} \textit{Smith}, 442 U.S. at 744. The Court further described the switchboard as the “modern counterpart” of the human operator. \textit{Id.}
\textsuperscript{211} \textit{Id.} at 742-43.
\textsuperscript{212} \textit{Id.} at 742.
\textsuperscript{213} \textit{Id.} at 743.
\textsuperscript{214} \textit{Id.} at 742-43.
\textsuperscript{215} See Chris Ayres, \textit{Putting Words in the Mouth of the Internet}, TIMES (London), Oct. 22, 1998 (discussing how computer companies are attempting to humanize their digital operators).
\textsuperscript{216} See Language Legalities Increase Personnel Officials, Immigrants Fight Drawl Debate While Speech Patterns Continue to Promote Stereotypes, AUGUSTA CHRON., Sept. 24, 2000, at A17 (discussing the firing of bilingual telephone operators hired for collect calls).
\textsuperscript{217} \textit{FBI’s Carnivore, supra} note 30 (oral statement of Tom Perrine, Principal investigator, Pacific Inst. for Computer Sec.).
\textsuperscript{218} \textit{See FBI’s Carnivore, supra} note 30 (oral statement of Stewart Baker, Att’y, Steptoe & Johnson).
\textsuperscript{219} \textit{See Smith}, 442 U.S. at 742-46.
Finally, because people now conduct more of their personal, business and commercial lives online, one of the most important services an ISP offers is a secure connection. Unlike a telephone company phone book, ISP sites do not advertise their capacity to review code that passes through their networks to track obscene e-mail. Rather, ISPs have a significantly stronger capital interest to insure that their customers' information does not get into the hands of someone who might abuse it, including the government. While the internet has established its strong presence in our economy, a computer connected to the internet would not be a common household appliance if ISPs failed to secure their networks. Thus, society recognizes a reasonable expectation of privacy for internet source information.

The inherent differences between the rich source information Carnivore collects and the simple telephone numbers a pen register collects reveal that Carnivore is not a device of the same limited capabilities as a pen register. Additionally, society places significant expectations on ISPs to keep their internet traffic private, leading to a reasonable expectation that the public or government will not see the source information it conveys to their ISPs. When ruling that pen register surveillance does not require Fourth Amendment protection, the *Smith* Court did not likely envision a relatively limitless device like Carnivore. For this reason, the Fourth Amendment should restrain Carnivore’s source information surveillance and require the FBI to establish probable cause before unleashing Carnivore’s vast capabilities to interfere with privacy.


223. PR Newswire, *Network Associates and Ingram Micro Partner to Provide Active Security Special Agent Program to Top Industry Resellers* (Dec. 8, 1999), at http://www.prnewswire.com/cgi-bin/storie...5&story=/www/story/12-08-1999/0001091481 (quoting Bob Bennett, vice president and general manager, of Enterprise Solutions Group at Ingram Micro who said, “[a]s the e-business economy grows, more businesses realize the vital importance of network security to their success and survival”) [hereinafter PR Newswire].


225. See, e.g., Benedict Carey, *Web Plays 2 Roles in Casual Sex*, L.A. TIMES, July 31, 2000, at S1 (stating that, “[b]ecause of privacy agreements, Internet service providers are reluctant to provide personal details about their customers”).

B. Condemning Carnivore’s Dragnet Tactics: Employing Additional Legal Precedent to Expose the Fourth Amendment Threat of Carnivore’s Broad Search Protocol

Because Carnivore must scan all of the digital code on an ISP’s network to extract the single suspect’s information, its broad use poses further threats to Fourth Amendment privacy. Combing through all of the digital code that runs through a network significantly differs from wiretapping a telephone line because the vast majority of the information Carnivore scans comes from innocent users.

The Supreme Court has warned that “a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope.” Even if the FBI establishes probable cause to monitor a suspect, a court may find Carnivore’s ability to intensely intercept more than forty million mega-bits of digital code per second is too intolerable an intensity, unlike a traditional low-tech wiretap on a telephone conversation. In addition, because Carnivore broadly scans each ISP customer’s digital code, a court may find that Carnivore’s searches violate the Fourth Amendment.

More specifically, Carnivore surveillance constitutes an internet dragnet. Despite the FBI’s reassurance that Carnivore is a minimalization tool because of its precise filters, scanning all of the digital code that streams over an ISP to gather incriminating information on a single suspect is an excessive tactic. By analogy, if the FBI were to conduct traditional telephone wiretaps in the same manner, it would have to divert every phone line from all users’ homes and offices through an FBI listening station just to find one person’s conversation.

Because internet privacy is so important to an ISP’s customers, the mere threat that Carnivore may be reading all of the digital code on any

227. FBI’s Carnivore, supra note 30 (oral statement of Barry Steinhardt, Assoc. Dir., ACLU).
228. Id. (prepared testimony of Stewart Baker, Att’y, Steptoe & Johnson) (suggesting that Carnivore “protects the privacy of the crooks, but not the innocent people who are investigated”).
230. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).
231. See FBI’s Carnivore, supra note 30 (oral statement of Tom Perrine, Principal investigator, Pacific Inst. for Computer Security).
232. See Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).
given network is enough to compromise a user’s trust that their information is secure. This will certainly cost the ISP its clients.

Additionally, Carnivore’s infinitely broad dragnet exceeds the scope of the Fourth Amendment because Carnivore wades through material that even the most lenient ECPA court order would prohibit in the telephone communications context. Tailored to limit the scope of FBI searches, the ECPA requires, if known, the identity of the person subject to criminal investigation for a source collection, and the identity of the person whose communications are to be intercepted for content surveillance. Because Carnivore will be intercepting and combing through all digital communications on an ISP, the FBI could just produce a list of all the ISP’s customers to identify the subjects of its search, satisfying the ECPA identity requirement. Even without such a literal reading of the statute, the ECPA does not invite such a broad search. As the Supreme Court stated, the Fourth Amendment “was meant to prevent wholesale intrusions upon the personal security of our citizenry.” Yet, Carnivore’s rapid processing and broad dragnet capabilities compromise this constitutionally guarded privacy.

C. Following the Telephone Wiretap Precedent: Letting ISPs Produce the Surveillance Results Themselves to Protect Their Customers’ Fourth Amendment Right to Privacy

Carnivore creates constitutional problems. However, the internet will become a safe-haven for criminal conduct. In fact, the FBI may not be the best entity to effectively regulate the internet because of its slow response to internet security concerns, lack of adequate resources to monitor criminal conduct on the internet, and bureaucratic hurdles hampering its surveillance. On the other hand, because of high consumer demand for internet security, ISPs already have similar sniffers devoted solely to network maintenance. Given their commercial access to internet security resources, ISPs have had great success over the last decade securing their

234. Id. § 3123(b)(1)(B).
235. Id. § 2518(4)(a).
236. FBI’s Carnivore, supra note 30 (oral statement of Barry Steinhardt, Assoc. Dir., ACLU).
237. Davis v. Mississippi, 394 U.S. 721, 726 (1969). While this case discussed arrests and investigatory detentions, the Court’s statement offers a relevant definition of the Fourth Amendment’s broad role in society. See id.
238. See President’s Working Group, supra note 4, at 26.
own systems from criminal conduct by using commercial sniffers that operate like Carnivore, but without the cumbersome Fourth Amendment information filters.240

Promoting ISP regulation over the internet may not be a perfect solution reducing internet crime while securing user privacy.241 Because federal law gives ISPs broad control over their networks' content, the ISP may never have an incentive to monitor criminal conduct.242 However, the FBI should be willing to cooperate with an ISP to develop commercial sniffers. This would certainly be more productive than compelling ISPs to consent to the invasive installation of Carnivore's software and hardware onto its systems and the covert operation of Carnivore from a remote location.243

In fact, critics attribute many of Carnivore's problems to this very hostile and adversarial role that the FBI envisions as its future on the internet.244 To protect telephone companies from excessive government intrusion on its systems, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA").245 Fearing that a telephone company would become the government's newest law enforcement branch, CALEA prohibits the FBI from exploiting telephone services.246 It effectively entrusts a phone company to conduct surveillance and produce the results, leaving the FBI out of the physical process of wiretapping.247

240. See Jeffrey Benner, Nailing the Company Spies, WIRED, March 1, 2001, at http://www.wired.com/news/print/0,1294,41968,00.html (last visited March 20, 2001) (describing "Silent Runner," a commercial network surveillance device that Benner describes as "a sophisticated information gathering and analysis tool that makes traditional keyword 'sniffers' obsolete"); see also PR Newswire, supra note 223 (describing the availability of effective, private internet security resources).

241. See generally Cody, supra note 22.


243. See FBI's Carnivore, supra note 30 (oral statement of Robert Corn-Revere, Att'y, Hogan & Hartson) (discussing the successful cooperation between an ISP and law enforcement in an e-mail surveillance project).

244. See Ann Harrison, Don't Like Carnivore? How About Altivore?, COMPUTERWORLD, Sept. 25, 2000, at 12. In her article, Harrison discusses Earthlink's lawsuit against the FBI. Id. Earthlink, an ISP, feared that Carnivore's installation would affect network stability, and the judge ruled that Earthlink could create and use its own sniffer for surveillance. Id.


246. Id. § 1004; Digital Privacy, supra note 3 (oral statement of James X. Dempsey, Senior Staff Counsel, Ctr. for Democracy and Tech.) (stating that "[a] telecommunication service provider shall design its system so that a wiretap is activated within the switching premises and controlled by telephone company personnel, not by the law enforcement personnel—precisely because this committee was concerned about the problem of remote FBI access to the actual guts of the network of the service provider").

247. See Digital Privacy, supra note 3 (oral statement of James X. Dempsey, Senior Staff Counsel, Ctr. for Democracy and Tech.).
CALEA does not govern the internet.\textsuperscript{248} However, considering that the FBI relies so heavily on an analogy between the telephone and internet when arguing for surveillance, it is hard to understand why it refuses to follow its own precedent protocol by allowing ISPs to produce the searches for it.

Because the Fourth Amendment explicitly regulates the government and not private businesses,\textsuperscript{249} a communication providers have the power to regulate their systems without the same Fourth Amendment encumbrances that hinder the government.\textsuperscript{250} Not only do ISPs already use their own commercial sniffers to maintain their systems,\textsuperscript{251} they also have a fundamental business interest in securing their customers’ personal information from illegitimate third parties, including the government.\textsuperscript{252} Effectively, if ISPs were to conduct surveillance for the FBI in the same manner as the telephone companies, the ISPs could restrict the FBI’s broad access while limiting the FBI’s attempts to make ISPs its newest law enforcement facilities.

The FBI, however, does not share this idealistic vision of harmony between law enforcement and ISPs.\textsuperscript{253} The FBI urges that smaller ISPs do not have the technical capacity to monitor their systems.\textsuperscript{254} Clearly, this rationale does not address why the FBI wants to compel larger ISPs to implement Carnivore, even though they are more than capable of conducting the surveillance on their own. Nevertheless, the FBI asserts that it designed Carnivore with the “mom and pop” ISPs in mind because they do not have the financial resources for meeting the FBI’s surveillance needs.\textsuperscript{255} Because the FBI needs access to all ISPs, it presents itself as “willing to bear the technical and cost burden” of installing Carnivore onto any network.\textsuperscript{256}

The FBI has failed to provide a compelling reason why large ISPs should open their systems to Carnivore. Despite its resources and lack of

\begin{itemize}
\item \textsuperscript{248} 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A).
\item \textsuperscript{249} U.S. CONST. amend. IV. The Fourth Amendment secures privacy from unreasonable government searches and seizures. \textit{Id.}
\item \textsuperscript{250} See \textit{id.}
\item \textsuperscript{251} \textit{See FBI’s Carnivore, supra} note 30 (oral statement of Tom Perrine, Principal investigator, Pacific Inst. for Computer Sec.).
\item \textsuperscript{252} King, \textit{supra} note 221, at 89.
\item \textsuperscript{253} Fourth Amendment Issues, \textit{supra} note 93 (prepared statement of Donald M. Kerr, Assistant Dir., FBI) (indicating that the FBI intends to limit the ISP’s assistance with Carnivore to the initial installation).
\item \textsuperscript{254} \textit{Id.}
\item \textsuperscript{255} \textit{Id.}
\item \textsuperscript{256} \textit{Id.}
\end{itemize}
Fourth Amendment restraints, the FBI overlooks the fact that even the smaller ISPs have the resources and technical skills to monitor their own systems. Even if the smaller ISPs lack sniffer software, the FBI has two alternatives to hijacking systems. First, the FBI can release Carnivore's source code. This is unlikely, as the FBI fears that public disclosure of Carnivore's intricacies will make it more vulnerable to hackers. However, releasing the source code to the ISPs ensures that the smaller ISPs will be capable of searching their own networks. Additionally, releasing the program's code gives the ISPs a chance to build their own sniffer systems based on Carnivore but tailored to maintain the security of their own systems. Even the DOJ technical review team suggested that the FBI release Carnivore's source code to allow the ISPs to test and use the program and free themselves from FBI entanglement.

While the FBI adamantly refuses to release Carnivore's code, it has the option of providing the ISP with the Carnivore black box for the duration of the court order, so the ISPs can conduct the searches themselves. If ISPs use Carnivore to conduct the surveillance themselves, it is justifiable because ISPs have a business interest in protecting the privacy of their innocent clients. Additionally, this option requires the FBI to cooperate with the ISPs and respect their desire to maintain the integrity of their services and systems.

As a check on the FBI's attempt to watch the whole internet with one program, it is the ISPs that should conduct internet surveillance at the request of the FBI, just like the telephone companies conduct the FBI's

257. See id.

258. FBI's Carnivore, supra note 30 (oral statement of Peter William Sachs, President, ICONN, LLC). Sachs characterized his own ISP as one the FBI claims is too small to conduct the searches it needs. Id. He rebutted, "[w]e do have the capability—in fact, any ISP has the capability of supplying the FBI with exactly what it wants in a more accurate, more efficient and more private manner, because we have absolutely no need to look at anybody's information, except for the actual target."

259. Digital Privacy, supra note 3 (prepared statement of Donald M. Kerr, Assistant Dir., FBI).

260. FBI's Carnivore, supra note 30 (oral statement of Tom Perrine, Principal Investigator, Pacific Inst. for Computer Sec.) (indicating that "if the equivalent of Carnivore were available in open source, that... would lower the barriers to entry for the smaller and less technically capable ISPs to provide this information").

261. ILL. INST. OF TECH., supra note 14, at xv. IITRI's review recommends that the FBI "work toward public release of Carnivore source code." Id.

262. Fourth Amendment Issues, supra note 93 (prepared statement of Donald M. Kerr, Assistant Dir., FBI) (stating that the FBI "would have a problem with full open disclosure, because that, in fact, would allow anyone who chose to develop techniques to spoof what we do an easy opportunity to figure out how to do that").
wiretaps.\textsuperscript{263} While this solution imposes significant burdens on ISPs,\textsuperscript{264} it is infinitely less intrusive than Carnivore’s current network-hijacking protocol. Given the choice, it is a safe assumption that most ISPs would prefer control of their own systems rather than suffer a takeover by law enforcement.

\textit{D. Abandoning Unacceptable Analogies and Outdated Legislation: Adopting Internet-Specific Legislation}

As both law enforcement and privacy advocates prepare to shape future internet regulation, lawmakers and the courts must balance law enforcement’s need to police the internet for crime against the public’s expectation of privacy. Current federal statutes do not adequately address sophisticated technologies. The government needs to abandon deficient analogies that fail to account for obvious discrepancies between modern and antique surveillance tools.

The DOJ asserts that criminal surveillance regulations should be technology-neutral in order to avoid using multiple standards for the same surveillance.\textsuperscript{265} However, internet surveillance vastly differs from telephone surveillance. Because of this flawed analogy, law enforcement’s ignorance of the inherent technological differences between the internet and the telephone tramples on the internet user’s constitutionally protected privacy.\textsuperscript{266}

As long as the courts characterize the internet as “‘ambient—nowhere in particular and everywhere at once,’”\textsuperscript{267} despite its great prominence in our lives, it is difficult to predict any course of action. Similar to the courts, legislators share the onerous task of either manipulating technologically outdated law or pioneering new law and risking social, economic and political accountability for unforeseeable failures.\textsuperscript{268}

While it is impossible to expect law to remain current with technology, it utterly fails when it cannot recognize technological trends

\textsuperscript{263} See 47 U.S.C. § 1004.

\textsuperscript{264} \textit{FBI’s Carnivore, supra} note 30 (oral statement of Stewart Baker, Att’y, Steptoe & Johnson) (remarking that no small ISP wants the role of intercepting content for the government).

\textsuperscript{265} \textit{Digital Privacy, supra} note 3 (oral statement of Kevin V. DiGregory, Deputy Assistant Att’y General, Criminal Div., U.S. Dep’t of Justice).

\textsuperscript{266} See discussion, \textit{supra} Part IV.A.

\textsuperscript{267} ACLU v. Reno, 217 F.3d 162, 169 (3d Cir. 2000) (citing Doe v. Roe, 955 P.2d 951, 956 (Ariz. 1998)).

and respond quickly enough to secure individuals' constitutional rights. The lack of new legislation specifically regulating internet surveillance freezes Fourth Amendment rights, crystallizing them into technologically inappropriate legislation. Currently, the possibility exists for the FBI and other law enforcement agencies to simply tweak their search protocol and adopt less threatening names for their surveillance programs like Echelon\textsuperscript{269} or Altivore.\textsuperscript{270} As long as surveillance regulations fail to specifically address the uniqueness of the internet, millions of users will log on as guinea pigs subject to law enforcement surveillance experiments, with little recourse to protect their personal privacy other than staying offline.

Lawmakers are a long way from controlling the internet with balanced legislation. At this juncture, Congress should prioritize internet legislation and continue the trial and error process integral to new lawmaking. While internet-specific legislation poses its own pitfalls,\textsuperscript{271} even the most controversial internet-specific legislation will guarantee vigorous dialogue between digital libertarians and control-hungry agencies, hashing out policies to forge a more evenhanded solution. When lawmakers insecurely clutch inadequate and outdated standards out of political timidity, they stifle public advocacy, the very heart of our democracy.

In general, reliance on outmoded statutes to govern a new electronic medium imposes constitutional threats. Carnivore's existence confirms internet users' Orwellian fears, and law enforcement agencies are permitted to exploit loopholes in current surveillance law until Congress fortifies Fourth Amendment privacy rights with internet-specific legislation. No other communications technology retains infinite personal information through such progressive communications services. Therefore, Congress needs to disregard the DOJ's plea for technology-neutral legislation and embark on new surveillance regulations for the internet.

V. CONCLUSION

Carnivore's broad search protocol, coupled with the fact that digital code over the internet discloses significantly more private information than a telephone could ever reveal, makes it a threat to Fourth Amendment


\textsuperscript{270} Harrison, supra note 244.

\textsuperscript{271} Digital Privacy, supra note 3 (prepared statement of Kevin V. DiGregory, Deputy Assistant Att'y General, Criminal Div., U.S. Dep't of Justice) (warning that creating technology-specific law in substantive and procedural criminal law creates too many standards for surveillance, raising the bar for the prosecutor).
privacy rights. Lawmakers need to either shut the program down or drastically alter its search capabilities. Ultimately, the FBI's struggle to monitor the internet within its technologically outdated federal guidelines highlights the internet's need for technology-specific legislation. Until such legislation exists, lawmakers leave innocent internet users with little protection, while law enforcement simultaneously makes stronger and less conspicuous attempts to compromise users' constitutional right to privacy.

Graham B. Smith*

* Special thanks to MaryBeth Lipp for her love, intelligence, teachings and courage that inspire me to succeed in everything I do. I would also like to thank my big brother, Stu Smith, and good friend, Samuel "Mac" Jenkins, for their impromptu research, tireless discourse and technical consulting on this Comment. Sincere thanks to the editors and staffwriters of *Loyola of Los Angeles Entertainment Law Review* for their time, particularly Shivani Rosner, Aida Darakjian, Fara Blecker, Brian Lerner, Alisa Edelson and Brigit Connelly for their talent and effort on my behalf. Thanks to Professor Linda Beres for her expert suggestions and mentorship. Finally, I would like to thank my West and East Coast families for their unconditional support and belief in me.