

# **The Carnivore Internet Monitoring Device: Capabilities, Statutory Framework, and Constitutional Considerations**

By Casey Holland\*

\*The author is a senior at the University of Kentucky, majoring in political science. A much shorter version of this paper was originally written in the spring of 2002 for Dr. Bradley Canon's seminar in Privacy Law. It has been substantially rewritten to fulfill the University Honors Program's Independent Project requirement. The author would like to thank Dr. Canon for his assistance as a faculty advisor throughout the project, his father for providing some much-needed understanding on the reality of current networking technology, and Gregory Nojeim of the American Civil Liberties Union for his assistance in finding certain sources.

## Table of Contents

Table of Contents.....	2
Introduction: What is Carnivore?.....	4
Part I: Carnivore Capabilities.....	6
<i>A. Content Interception</i> .....	7
<i>B. Noncontent Addressing Interception</i> .....	7
<i>C. Text String Filtering</i> .....	9
<i>D. Full Mode Collection</i> .....	11
Part II: Technical Problems and IITRI Report Failings.....	12
<i>A. Encryption</i> .....	12
<i>B. IITRI Shortcomings</i> .....	15
<i>C. Packet Switching Problems and System Compatibility</i> .....	17
<i>D. Carnivore Device Security</i> .....	20
<i>E. Auditing and Accountability</i> .....	22
<i>F. Open Source Solution</i> .....	23
Part II: Statutory Framework.....	24
<i>A. Federal Communications Act of 1934</i> .....	24
<i>B. Omnibus Crime Control and Safe Streets Act of 1968</i> .....	25
<i>C. Foreign Intelligence Surveillance Act of 1978</i> .....	26
<i>D. Cable Communications Policy Act of 1984</i> .....	27
<i>E. Electronic Communications Privacy Act of 1986</i> .....	28
<i>F. Communications Assistance to Law Enforcement Act of 1994</i> .....	31
<i>G. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001</i> .....	33

Part IV: Constitutional Considerations.....	35
<i>A. Carnivore, Pen Registers, and the Fourth Amendment.....</i>	<i>35</i>
<i>B. Carnivore and the Exclusionary Rule.....</i>	<i>39</i>
<i>C. Law Enforcement vs. National Security.....</i>	<i>40</i>
Summary.....	42
Works Cited.....	45

## Introduction: What is Carnivore?

As America has rapidly become aware, the Internet is a powerful tool for research, shopping, and entertainment. However, it has also become a tool for criminals and terrorists. Child pornographers, con men, and financial hackers have found refuge in the anonymity of the World Wide Web.<sup>1</sup> It was also rapidly revealed that the horrific terrorist attacks on September 11 were planned and implemented in large part through e-mail and the Internet.<sup>2</sup> This boom in online criminal activity has thus far not coincided with an effective response from the law enforcement and intelligence communities. One possible solution is the device known by the name “Carnivore,”<sup>3</sup> developed by the Federal Bureau of Investigation (FBI) sometime prior to October of 1999 (the exact date of development has not yet been made public).<sup>4</sup> To date Carnivore usage has been made public only sparingly, with only a few deployments revealed during 1999 and none since then.<sup>5</sup> However, given recent terrorist activity it is safe to assume that Carnivore will take on a more active role in investigations.

“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

---

<sup>1</sup> *Hearings on the Carnivore Diagnostic Tool Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106<sup>th</sup> Cong. (2000) (statement of Donald Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation).

<sup>2</sup> Jay Lyman, *How Terrorists Use the Internet*, NEWS FACTOR NETWORK, available at <http://www.newsfactor.com/perl/story/7731.html> (Sept. 12, 2001) (on file with author).

<sup>3</sup> In 2001, the FBI changed the name of Carnivore to “DCS1000” due to the name’s somewhat sinister implications. Thomas McCarthy, *Don’t Fear Carnivore: It Won’t Devour Individual Privacy*, 66 MO. L. REV. 827, 849 (2001). In addition, Carnivore makes use of two post-processing programs, Packeteer and CoolMiner, that when used in conjunction with Carnivore are known as the DragonWare suite ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM FINAL REPORT at viii (2000) (hereinafter cited as IITRI Report). This paper will continue to use the original name of Carnivore to refer to both the actual device and the DragonWare suite, as it is significantly less cumbersome.

<sup>4</sup> The Wall Street Journal initially broke the story about the existence of Carnivore. Neil King, Jr., *FBI’s Wiretaps to Scan E-mail Spark Concern*, WALL STREET JOURNAL, July 11, 2000, at A3.

<sup>5</sup> *1999 Deployments*, available at <http://www.epic.org/privacy/carnivore/deployments.html> (last visited Dec. 5, 2002) (on file with author).

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... Carnivore can collect any digitally transmitted information such as the suspect’s e-mail, instant messaging, chat-room discussions, financial transactions and websites visited.’<sup>6</sup>

When Carnivore was revealed to the media, it caused an instant controversy. Law enforcement heralded the device as essential to its capability to stay on top of changing technologies, while privacy advocates were immediately concerned with the sweeping nature of Carnivore and its threat to individual rights.<sup>7</sup> Even the independent technical reviews of Carnivore have been forced to recognize the significant threat that the device can pose to individual freedom and privacy.<sup>8</sup> However, despite or perhaps because of the rhetoric often used both for and against Carnivore, the basic facts of the government’s capability to conduct electronic surveillance via the Internet have become somewhat obscured in the public eye.

This paper will examine the true capabilities of Carnivore as it relates to electronic communications in Part I. Part II will examine the technical problems with and failings of Carnivore, as well as the efficacy of the Illinois Institute of Technology Research Institute (IITRI) review. In Part III, the statutory framework allowing for the implementation of Carnivore will be covered, specifically focusing on the recent antiterrorism legislation. This section will also address the evolution of said framework as it relates to Internet communications. Part IV of this paper will address concerns over Carnivore’s constitutionality under the Fourth Amendment, especially in light of how terrorism has changed law enforcement and intelligence gathering forever. Finally, Part

---

<sup>6</sup> Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement’s Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L.J. 481, 492 (2001) (citations omitted).

<sup>7</sup> *supra* n. 1.

<sup>8</sup> IITRI Report, at 1-3 to 1-5.

V will examine how Internet surveillance is approached in the international community, and how invasive Carnivore is when compared to some of these other efforts.

### Part I: Carnivore Capabilities

There has been significant disagreement over what Carnivore can and cannot accomplish. The FBI contends that Carnivore is “both surgical and specific as to a particular criminal subject’s traffic and which is based upon the specific authority set forth in a court’s order.”<sup>9</sup> At the opposite end of the spectrum are concerns such as those voiced by the American Civil Liberties Union (ACLU):

“Carnivore is an unprecedented system. Never before has law enforcement installed a device, which accesses all the communications of a service provider’s customers, rather than only the communications of the target. Never before has a law enforcement agency claimed that it should be granted access to all communications passing through a service provider’s network based on an unsupervised promise that it will not stray beyond the confines of its authority.”<sup>10</sup>

These conflicting views of Carnivore’s capability were at last given full testing in 2000, when IITRI, acting under government contract, conducted a comprehensive technical review of the Carnivore system.<sup>11</sup> Those findings have been released to the public by the Department of Justice (DOJ), via its website.<sup>12</sup> This section will examine the report in three aspects: content interception, noncontent addressing (also known as “pen mode”) interception, text string filtering, and “full mode” collection.

---

<sup>9</sup> Letter from Donald Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, to Patrick Leahy, Ranking Member, Comm. of the Judiciary, United States Senate (Jan. 23, 2001) (on file with author).

<sup>10</sup> *Hearings on the Carnivore Diagnostic Tool Before the Subcomm. on the Constitution of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong. (2000) (statement of Barry Steinhardt, Associate Director, American Civil Liberties Union).

<sup>11</sup> IITRI Report.

<sup>12</sup> *see* <http://www.usdoj.gov/jmd/publications/publications.htm>.

### *A. Content Interception*

IITRI tested Carnivore to determine its capability to reliably intercept the content of Internet communications, including: “web browsing contents, FTP login session, commands and data, and e-mail contents.”<sup>13</sup> IITRI found that collecting content information from the target, either limited to the target’s e-mail or including all information from a specific IP address (denoting a particular computer), is fully within Carnivore’s capabilities.<sup>14</sup> In both cases, Carnivore passed with proverbial flying colors, intercepting all desired communications accurately without intercepting any undesired information from non-targets.<sup>15</sup> In layman’s terms, this conclusively demonstrates that Carnivore is capable of intercepting the subject and text blocks of e-mail, all information contained on the target’s visited web pages, and all files transferred to or from the target. Though the report does not specifically state this, presumably full content interception on a fixed IP address would also intercept the content of increasingly popular “instant messaging” programs, such as America Online Instant Messenger and Yahoo Communicator. This suspicion was partially confirmed in a presentation by FBI agent Marcus Thomas, one of Carnivore’s developers.<sup>16</sup>

### *B. Noncontent Addressing Interception*

IITRI conducted several tests to determine Carnivore’s capability to reliably intercept and catalog noncontent addressing information. Tests specifically targeted

---

<sup>13</sup> IITRI Report, at 3-25.

<sup>14</sup> *see id.*

<sup>15</sup> *see id.*, at C-9 to C-12.

<sup>16</sup> Declan McCullagh, *fyi: FC: FBI agent reportedly gives public demo of Carnivore*, available at <http://jis.mit.edu/pipermail/saag/2000q4/000107.html> (Oct. 25, 2000) (on file with author).

noncontent e-mail collection, noncontent web browsing collection, and noncontent file transfer activity collection.<sup>17</sup>

In the tests for noncontent web browsing and file transfer activity collection, Carnivore performed precisely as intended, collecting “activity source and destination IP address[es]” but not the content of the transfers taking place between the target and others.<sup>18</sup> However, “the amount of data transferred is captured” as well, which could conceivably be used to show the nature of the content of the unintercepted transmissions.<sup>19</sup> For example, if the FBI had information that a target was sending pornographic images of children, it would be simple to check the sizes of the target’s file transfers against the typical length of common image files.

In noncontent e-mail collection, however, Carnivore ran into some difficulties. The expected result was that “Carnivore will collect only the FROM and TO addresses of the e-mail that was sent from and to a target,” but not the subject or text portions of the e-mail, but in some cases, Carnivore “failed to collect FROM and TO information.”<sup>20</sup> Since the version of Carnivore tested by IITRI was not the most recent (IITRI tested version 1.3.4, while version 2.0 was and is the most current<sup>21</sup>), it is possible that this error has been corrected.

In addition, “IITRI observed that in pen mode Carnivore replaces e-mail header information with Xs. When the data are viewed... it is easy to determine the length of each field in the header and the length of the entire message.”<sup>22</sup> As is the problem with

---

<sup>17</sup> IITRI Report, at 3-24 to 3-25.

<sup>18</sup> *see id.*, at C-9 to C-12.

<sup>19</sup> *see id.*, at 3-25.

<sup>20</sup> *see id.*, at 3-24.

<sup>21</sup> *see id.*, at viii.

<sup>22</sup> *see id.*, at 3-25.

Carnivore's noncontent web browsing and file transfer activity collection procedures that collect the size of all transferred files, this information could conceivably be used to determine the contents of intercepted addressing information. Since Carnivore is restricted to intercepting strictly noncontent information when operating in pen mode, these capabilities create a risk that Carnivore exceeds its statutory authority.<sup>23</sup>

### *C. Text String Filtering*

In addition to the ability to function as a pen register or full-fledged wiretapping device,<sup>24</sup> Carnivore has the capability to text string filtering, essentially a keyword search of intercepted packets.<sup>25</sup> This filtering can be performed in four distinct manners: filtering text string on web activity collection, filtering on text string for e-mail collection, filtering on text string and e-mail addresses or e-mail user ID for e-mail collection, and filtering on text string for FTP collection.<sup>26</sup>

Text string filtering is in essence a way to limit the amount of data collected by Carnivore—the IITRI report uses an example wherein a court order only authorizes the collection of “e-mail sent from and to a target that contains the key word ‘Planning.’”<sup>27</sup> By using text string filtering, Carnivore is designed to be able to limit the data intercepted and thereby protect the privacy of the target's communications that are unrelated to an

---

<sup>23</sup> *see infra* pp. 24-35 for a full discussion of this authority.

<sup>24</sup> *infra* pp. 4-6.

<sup>25</sup> *see id.*, at 3-26 to 3-28.

<sup>26</sup> *see id.*, at 3-26 to 3-28. Note that the second and third text string filters appear similar, but are in fact wildly different. The second scenario will collect *all* e-mail containing the text string that passes through Carnivore, while the third scenario will only collect the e-mail that both matches the text string and is being sent or received by a specific target.

<sup>27</sup> *see id.*, at C-26.

investigation. However, with the exception of text string filtering on web activity,<sup>28</sup> Carnivore does not function properly when attempting to filter text strings.<sup>29</sup>

When performing text string filtering for e-mail collection, searching for certain words or phrases within an e-mail packet, “Carnivore collects SMTP (sending) e-mail that matches the key word correctly, but does not collect POP3 (receiving) e-mail correctly.”<sup>30</sup> This appears to be caused by a “performance trade off” within Carnivore’s programming, since SMTP e-mail is processed differently from POP3 e-mail,<sup>31</sup> but is also caused by certain packet switching problems that will be discussed below.<sup>32</sup>

The undercollection that occurs when Carnivore filters text strings for e-mail collection is contradicted by the overcollection that occurs when Carnivore filters on text strings and e-mail addresses or user IDs for e-mail collection, even though both errors are caused by the same limitations in Carnivore’s programming.<sup>33</sup> The error in this case is that “[w]hen given both a specific e-mail address and a text string, Carnivore collects all the target’s e-mail whether or not the e-mail matches the given text string.”<sup>34</sup>

Conversely, Carnivore is unable to collect all FTP (file transfer protocol) activities containing a given text string, resulting in an undercollection caused by previously mentioned packet switching problems that will be discussed fully below.<sup>35</sup> In short, Carnivore’s ability to function while utilizing text string filtering is severely limited, in part by the very nature of packet-switched networks and in part due to

---

<sup>28</sup> *see id.*, at 3-26.

<sup>29</sup> *see id.*, at 3-27 to 3-28.

<sup>30</sup> *see id.*, at C-26.

<sup>31</sup> *see id.*, at C-26.

<sup>32</sup> *infra* pp. 17-20.

<sup>33</sup> IITRI Report, at C-28.

<sup>34</sup> *see id.*, at C-28.

<sup>35</sup> *infra* pp. 17-20.

programming limitations designed as performance trade offs. Text string filtering can be a powerful tool, both for limiting the amount of raw data that law enforcement officials must read through and for protecting the privacy of electronic communications unrelated to a certain investigation, but unless Carnivore can be designed to function properly in these circumstances the tool is useless.

#### *D. Full Mode Collection*

By minimizing the filters that are used to determine how much information is intercepted, Carnivore is capable of intercepting “all TCP traffic from every device that is attached to the sniffing segment.”<sup>36</sup> Again in layman’s terms, this means that Carnivore has the capability to intercept and catalog every packet of data coming through whatever Internet service provider (ISP) the device is attached to. Remarkably enough, this is Carnivore’s *default* setting: unless intentionally altered, Carnivore will proceed to collect *all* information traveling through a given ISP.<sup>37</sup> In its report, IITRI recommends that the FBI provide “separate versions of Carnivore for pen register and full content collection.”<sup>38</sup>

However, while this capability sounds quite insidious at first, in practical terms Carnivore can almost never be utilized in such a manner. The first consideration is to processing speed: “Carnivore filters...forty million mega-bits per second or faster.”<sup>39</sup> Only very small ISPs have a traffic rate below Carnivore’s maximum processing speed.<sup>40</sup> An additional factor is storage capacity: Carnivore, like all digital processing devices, has

---

<sup>36</sup> IITRI Report, at 3-26

<sup>37</sup> “When turning on TCP full mode collection and not selecting any port, the default is to collect traffic from all TCP ports.” *See id.*, at C-20.

<sup>38</sup> *see id.*, at xiv.

<sup>39</sup> Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement’s Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L.J. 481, 493 (2001).

only a limited ability to store data. Since Carnivore “employs a generic Pentium-class PC,” this storage capacity is miniscule when compared to the amount of data that would be intercepted utilizing full mode collection.<sup>41</sup> While Carnivore is also equipped with a Jaz drive, a high-capacity storage device using interchangeable disks, in order for Carnivore to reliably save all unfiltered traffic the disks would need to be physically switched out every few hours, and every few minutes on an ISP of any significant size,<sup>42</sup> creating both time and monetary constraints that make the full mode collection setting highly unlikely.

In summary, Carnivore has a wide range of abilities to collect and monitor Internet traffic, ranging from noncontent e-mail interception all the way up to total interception over an ISP. However, there are a number of problems with Carnivore’s technical functionality, as well as with the IITRI review through which those errors became public knowledge.

## Part II: Technical Problems and IITRI Report Failings

Understanding what Carnivore can do is essential to understanding how the device fits into the statutory and constitutional framework. However, just as important to this understanding is the knowledge of how Carnivore is flawed, in some cases critically so. The underlying assumptions behind Carnivore’s utilization are that it performs as intended, was properly designed, and is immune from abuse or technological defeat. As this section will illustrate, every one of those assumptions is patently false.

### *A. Encryption*

---

<sup>40</sup> IITRI Report, at 1-3 to 1-5.

<sup>41</sup> IITRI Report, at 3-11.

<sup>42</sup> Telephone Interview with Archie Holland, Senior Network Administrator, Bluegrass Networks LLC (Feb. 26, 2002).

Data encryption has increasingly become necessary in the digital world of the Twenty-First Century. Businesses, banks and investment houses, government entities, and even individuals have begun utilizing encryption technology to protect their data and communications at an explosive rate.<sup>43</sup> This presents a rather serious problem for Carnivore, which “has been useless against suspects clever enough to encrypt their files.”<sup>44</sup> Indeed as even a general rule the only defense against packet sniffing devices “is to encrypt your data, so that while they can sniff it, they cannot read it.”<sup>45</sup>

The threat that encryption poses to Carnivore’s effectiveness is more than an abstract one. At the North American Network Operators Group conference in 2000, FBI agent Marcus Thomas publicly announced that in one tenth of the cases in which Carnivore is utilized, the intercepted files are encrypted and the investigation is thereby thwarted.<sup>46</sup> Agent Thomas did note that it is “more common to find encryption when we seize static data, such as on hard drives.”<sup>47</sup>

A distinction is important here: packet sniffers like Carnivore are fully capable of intercepting the encrypted packets, but without some means of breaking through the encryption (such as knowing the subject’s personal password) the intercepted data is very nearly useless.<sup>48</sup> It would still be possible to subject the data to traffic analysis, a study of which parties are communicating with each other and when, and such analysis may be as

---

<sup>43</sup> ETZIONI, AMITAI, *THE LIMITS OF PRIVACY*, at 75-76 (1999).

<sup>44</sup> Bob Sullivan, *FBI software crack encryption wall: “Magic Lantern” part of new “Enhanced Carnivore Project,”* MSNBC, available at <http://msnbc.com/news/660096.asp?cp11=1> (Nov. 20, 2002) (on file with author).

<sup>45</sup> Robert Graham, *Sniffing (network wiretap, sniffer) FAQ*, at 2.1, available at <http://www.robertgraham.com/pubs/sniffing-faq.html> (Sept. 14, 2000) (on file with author).

<sup>46</sup> *supra* n. 16

<sup>47</sup> *see id.*

<sup>48</sup> E-mail Interview with Matt Blaze, Research Scientist, AT&T Laboratories (Mar. 26, 2002).

important to an investigation as the content of the interceptions.<sup>49</sup> In addition, header and addressing information (which Carnivore collects when it is acting in pen mode<sup>50</sup>) must by necessity be sent unencrypted in almost every conceivable circumstance, therefore allowing Carnivore to remain unaffected by encryption efforts so long as it is operating as a non-content interception device.<sup>51</sup>

While there are several freely available forms of encryption that could be used to thwart Carnivore,<sup>52</sup> the FBI may have come up with a solution to the problem. Software known as “Magic Lantern” is now being used in conjunction with Carnivore to decrypt data that a subject has attempted to hide using any number of popular encryption programs.<sup>53</sup> Magic Lantern is a software-based keylogging program that must be installed on a subject’s computer, either through physical installation or by using a type of computer virus known as a Trojan Horse.<sup>54</sup> Magic Lantern then records everything that the subject inputs into the subject’s computer using the keyboard, including the passwords or passphrases used to encrypt electronic communications, and transmits this data back to the FBI.<sup>55</sup> Armed with the subject’s own passwords, decrypting the data that Carnivore subsequently intercepts is a simple exercise.

In short, encryption presents something of a conundrum for Carnivore: subjects must have a certain level of sophistication to use electronic communications (and hence be subject to packet sniffing), yet lack the level of sophistication needed to encrypt said communications, in order for Carnivore to be effective as a content intercept. While

---

<sup>49</sup> *see id.*

<sup>50</sup> *infra* pp. 7-9.

<sup>51</sup> *supra* n. 48

<sup>52</sup> *supra* n. 45

<sup>53</sup> *supra* n. 44

<sup>54</sup> *supra* n. 45

Magic Lantern has been useful in at least one case (against mob boss Nicodemo Scarfo<sup>56</sup>), it is highly doubtful that most subjects with the savvy to use encryption software would be so lax as to allow keylogging software to be installed without their knowledge. From this it can therefore be generally concluded that encryption is an easy and effective way to defeat Carnivore.

### *B. IITRI Shortcomings*

“In several press releases the FBI specified that the technical review [of Carnivore] was to be conducted by a “major university.” However, the FBI solicitation included several important restrictions on the information it would make available, the furnishing of full source code, the issues that could be raised in the study, and the right to release the report to the public. These restrictions led several respected institutions to decline to submit proposals, which further inflamed public opinion regarding the integrity and credibility of the project. On September 26, 2000, the FBI announced that it had awarded the technical review project to [IITRI], one of eleven groups that had made submissions. The reaction to the selection by the information technology community was immediate and vociferous.”<sup>57</sup>

In particular, the ACLU strongly criticized the IITRI review team for its connection with “government insiders, including... team members [with] backgrounds in the National Security Agency (NSA), the Department of Defense, and the Department of the Treasury.”<sup>58</sup> The ACLU also implicitly suggested that IITRI was in collusion with the FBI and the DOJ by accepting conditions on what it was not allowed to review, by confining the report to the older Carnivore version 1.3.4, and by performing the immense and complicated evaluation in less than six weeks and with a budget of only \$175,000.<sup>59</sup>

---

<sup>55</sup> *supra* n. 44

<sup>56</sup> *supra* n. 44

<sup>57</sup> E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J. L. & TECH. 10, 43 (2001) (internal citations omitted).

<sup>58</sup> Barry Steinhardt & Christopher Chiu, *ACLU Comments regarding Carnivore review team draft report*, available at [http://www.aclu.org/news/2000/carnivore\\_comments.html](http://www.aclu.org/news/2000/carnivore_comments.html) (Dec. 1, 2000) (on file with author).

<sup>59</sup> *see id.*

Considering that the FBI's 2002 budget request included more than \$13 million towards Internet surveillance (the FBI claims that requests for such surveillance increased 1,850% from 1997 to 1999),<sup>60</sup> such a small budget seems quite inadequate.

Of course, the ACLU officials were not the only people concerned with possible privacy abuses using Carnivore. House Majority Leader Dick Armey, a Texas Republican and strong conservative, strongly criticized the IITRI review, calling its findings "questionable" and agreeing with the ACLU that "the choice of reviewers dictated the tone of the report."<sup>61</sup>

Perhaps even more damning than the above perspectives on the IITRI review is that presented by a team of highly respected telecommunications researchers asked by the DOJ to initially identify what issues the review team should address.<sup>62</sup> After studying the IITRI report, the same team concluded that it "simply cannot support a conclusion that Carnivore is correct, safe, or always consistent with legal limitations."<sup>63</sup> The team's post-IITRI comments concluded that the report contained "a lack of analysis of operational and 'systems' issues" that could reveal "[many] potential security flaws and collection errors;" that "the exclusion from analysis or testing of RADIUS[, a programming language,] is a very serious omission;" and that "serious technical questions remain about the ability of Carnivore to satisfy its requirements for security, safety, and soundness."<sup>64</sup>

---

<sup>60</sup> *Extent of FBI's Web surveillance disclosed*, U.S.A. TODAY, May 4, 2001, available at <http://www.usatoday.com/life/cyber/tech/2001-05-04-carnivore.htm> (on file with author).

<sup>61</sup> *Report: Carnivore Could Be Abused*, U.S.A. TODAY, available at <http://www.usatoday.com/life/cyber/tech/cti834.htm> (Nov. 22, 2000) (on file with author).

<sup>62</sup> Steven Bellovin, et al., *Comments on the Carnivore System Technical Review*, available at [http://www.crypto.com/papers/carnivore\\_report\\_comments.html](http://www.crypto.com/papers/carnivore_report_comments.html) (Dec. 3, 2000) (on file with author).

<sup>63</sup> *see id.*

<sup>64</sup> *see id.*

In short, some of the most highly regarded specialists in the field concluded that the IITRI report was woefully inadequate in its analysis of Carnivore's technical capabilities.

It is impossible to determine if a more thorough or well-funded analysis of Carnivore would have yielded any substantially different results from those of the IITRI report, and there are no serious suggestions that IITRI failed to make a good-faith effort to study Carnivore. However, considering the number of limitations placed on the supposedly independent review from the beginning, it should not be surprising that the IITRI report did little if anything to sway public opinion regarding Carnivore.

### *C. Packet Switching Problems and System Compatibility*

To understand Carnivore's inability to deal with certain problems intrinsic to the nature of Internet surveillance and the consequences thereof, it is first necessary to have an overview of how the Internet actually functions.

The Internet began as an effort to protect America's communications from a massive nuclear assault in the 1960's.<sup>65</sup> This effort led to the initial research into packet-switching theory, wherein "a decentralized computer network first splits a message into small chunks, called packets, and then routes messages from one computer location to another at a remote site."<sup>66</sup> These data packets each take "the most efficient route at the time of transmittal,"<sup>67</sup> leading to the all-too-common analogy of the Internet as a web. Because of this "least cost path" principle of communication, it is necessary for the individual packets to be fairly small in nature, containing in many cases less than 100

---

<sup>65</sup> Barry Leiner et al., *A Brief History of the Internet*, E-ONTHEINTERNET, available online at <http://www.isoc.org/oti/articles/0597/leiner.html> (last visited Dec. 5, 2002) (on file with author).

<sup>66</sup> Frank Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment?*, 80 N. C. L. REV. 315, 321 (2001).

<sup>67</sup> Joseph Goodman et al., *Cybercrime: Carnivore: Will it Devour Your Privacy?*, 2001 DUKE L. & TECH. REV. 28, 32 (2001).

bytes of data.<sup>68</sup> Considering that even incredibly short and unencrypted e-mail runs to several thousand bytes, no single packet contains more than a glimpse at the overall communication.

This packet switched nature of Internet communications creates a serious problem for packet sniffers<sup>69</sup> such as Carnivore. If a single packet is missed, repeated, or even just miscategorized, the intercepted data could easily be misinterpreted. In practice, these are all common occurrences for packet sniffers.<sup>70</sup> In addition, “it is frequently possible for a third party to alter, forge, or misroute packets,” in which cases Carnivore is incapable of properly intercepting the desired data.<sup>71</sup>

Two prime examples of Carnivore’s difficulty to accurately intercept packet-based data can be found by examining its failures to properly perform text string filtering.<sup>72</sup> The best possible example occurs when Carnivore is attempting to perform text string filtering for FTP collection: Carnivore “only collects the packets containing the text string or... collects from the first packet containing the text string to the end of the session.”<sup>73</sup> When performing text string filtering for e-mail collection, Carnivore fails to process the packets correctly at all. “The specified text strings have to be included in the packet” in order to be intercepted, but due to a “performance trade off” designed “to save processing time,” Carnivore improperly filters the intercepted data so that it is not

---

<sup>68</sup> *supra* n. 45.

<sup>69</sup> “A packet sniffer is a wire-tap devices [sic] that plugs into computer networks and eavesdrops on the network traffic.” *See id.*

<sup>70</sup> Matt Blaze & Steven Bellovin, *Tapping, Tapping On My Network Door*, CACM, Oct. 2000, at 124.

<sup>71</sup> *see id.*

<sup>72</sup> *infra* pp. 9-11.

<sup>73</sup> IITRI Report, at C-30.

screened for the desired text string.<sup>74</sup> Therefore, no e-mail is collected at all, even e-mail from or to the subject containing the text string.

Another possibly major flaw in Carnivore is its compatibility with the diverse range of ISPs. IITRI concluded that “[o]perating Carnivore introduces no operational or security risks to the ISP network where it is installed,”<sup>75</sup> but factually speaking this is incorrect. In early 2000, Earthlink, Inc., installed Carnivore on several of its servers, which subsequently crashed and disrupted Internet access for Earthlink customers.<sup>76</sup> Carnivore was so incompatible with the ISPs servers that Earthlink was forced to install an older version of its operating system.<sup>77</sup> While the ISP later reached an agreement with the FBI whereby Carnivore will no longer be used on its servers,<sup>78</sup> the damage had already been done and Carnivore had already been proven incompatible with some systems.

The true dangers of Carnivore’s above failures were made readily apparent in 2002. The FBI released a bombshell memo under the Freedom of Information Act (FOIA) that detailed Carnivore’s failure to properly function in a 2000 investigation performed under the Foreign Intelligence Surveillance Act, possibly of persons connected to terrorist Usama bin Laden.<sup>79</sup> The memo begins by saying that “[t]o state that [redacted, an official with the DOJ Office of Intelligence Policy and Review] is

---

<sup>74</sup> *see id.*, at C-26.

<sup>75</sup> *see id.*, at xii.

<sup>76</sup> Thomas McCarthy, *Don’t Fear Carnivore: It Won’t Devour Individual Privacy*, 66 MO. L. REV. 827, 830 (2001).

<sup>77</sup> Peter Young, *The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy*, 35 IND. L. REV. 303, 322 (2001).

<sup>78</sup> *supra* n. 76.

<sup>79</sup> *FBI Memo on “FISA Mistakes,” available at <http://www.epic.org/privacy/carnivore/fisa.html> (last visited Dec. 5, 2002) (on file with author).*

unhappy... would be an understatement of incredible proportions.”<sup>80</sup> It goes on to state that “[Carnivore} was turned on and did not work correctly. The FBI software no only picked up the E-Mails under the electronic surveillance of the FBI’s target, [redacted] but also picked up E-Mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [redacted].”<sup>81</sup> An FBI spokesman later announced that the overcollection was a “rare mistake” that was caused by the ISP.<sup>82</sup> In other words, Carnivore’s incompatibility with an ISP caused possibly priceless electronic surveillance intelligence to be destroyed.<sup>83</sup> But whatever the cause of the error, Carnivore has demonstrated in at least two separate instances that it cannot be counted on to perform properly when it is needed.

#### *D. Carnivore Device Security*

The IITRI review puts it quite simply: “[t]he lack of physical control of the Carnivore computer could be a problem.”<sup>84</sup> While a portion of IITRI’s concern in this area is due to complications with the chain of custody of the evidence Carnivore obtains,<sup>85</sup> a much more important reason for better physical security of Carnivore is the “risk of compromise by untrustworthy ISP personnel.”<sup>86</sup> Since the computer that runs Carnivore is “typically installed without a keyboard or monitor”<sup>87</sup> the FBI presumed that

---

<sup>80</sup> *see id.*

<sup>81</sup> *see id.* (emphasis in original).

<sup>82</sup> George Leopold, *Flaws seen in FBI Net surveillance system*, ELECTRONIC ENGINEERING TIMES, June 13, 2002, at 22.

<sup>83</sup> The FBI technician’s destruction of all the Carnivore intercepts is not standard FBI procedure, and was apparently performed without supervisory knowledge. *Carnivore Puts Terror Investigation at Risk, Fox News Network*, available at [http://www.foxnews.com/printer\\_friendly\\_story/0,3566,53883,00.html](http://www.foxnews.com/printer_friendly_story/0,3566,53883,00.html) (May 29, 2002) (on file with author). Nonetheless, a Carnivore malfunction directly caused a potentially catastrophic loss of intelligence.

<sup>84</sup> IITRI Report, at 5-3.

<sup>85</sup> *see id.*, at 5-3.

<sup>86</sup> *see id.*, at 4-5.

<sup>87</sup> *see id.*, at viii-ix.

ISP personnel or other unauthorized persons would be unable to alter the performance of the device. However, this is not necessarily the case. To begin with, simply installing a monitor and input device on the computer is an effortless task, thereby opening Carnivore up to interference. The IITRI review states that “[t]he work area at the ISP is secured, and substantial precautions are taken to ensure that no ISP staff members have access” to Carnivore, but does not go into detail regarding exactly what steps have been taken. Considering that the U.S. has a history of poor physical security in and around areas of national security (spies in many cases have simply walked off with reams of information)<sup>88</sup>, establishing some simple security around the Carnivore computer should be a priority.

However, physically altering Carnivore’s settings is not the only way in which the device can be meddled with. Since Carnivore is normally controlled remotely via a telephone link,<sup>89</sup> it is conceivable that that link could be hacked into and exploited. While there are a number of password-oriented security devices to prevent unauthorized use of Carnivore over this telephone link,<sup>90</sup> the simplest and most effective security device on the telephone link, an automatic callback device that requires the person wishing to alter Carnivore’s settings to be calling from a predetermined and FBI-controlled telephone, is for some reason not included.

Assuming for a moment that Carnivore can be accessed, either physically or via the telephone link, there should be some way to ensure that Carnivore’s setting cannot be tampered with. In order to change the actual filter settings, the person must access the

---

<sup>88</sup> Frederick Wattering, *Counterintelligence: The Broken Triad*, 13 INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE 3, at 2-3 (2000).

<sup>89</sup> IITRI Report, at 3-12.

<sup>90</sup> *see id.*, at 3-12.

advanced setup features, which require a password.<sup>91</sup> However, this password is for some reason compiled into the Carnivore source code, making it readable (and even changeable) to anyone with both access to the computer and sufficient technical knowledge.<sup>92</sup> This is not standard practice in the programming industry, and a major security hole.<sup>93</sup> In short, in order for Carnivore to be even moderately trusted, its security infrastructure must be substantially improved to protect against unauthorized access.

#### *E. Auditing and Accountability*

Despite repeated FBI assertions that Carnivore contains auditing and accountability procedures,<sup>94</sup> in fact there are “no effective auditing functions that would expose and prevent abuse.”<sup>95</sup> IITRI acknowledges that “[a]uditing is crucial in security... [as] the means by which users are held accountable for their actions,” and that Carnivore had no auditing procedures.<sup>96</sup> The lack of auditing is due in part to the fact that any FBI agent using Carnivore is simply logged in under the same “Administrator” user ID, giving “every user of the system... full control over the resources of the system.”<sup>97</sup> The review continues to state that “[e]ven if auditing were enabled, there is nothing to prevent someone from editing or deleting those audit logs.”<sup>98</sup> According to

---

<sup>91</sup> *see id.*, at 3-13.

<sup>92</sup> *see id.*, at 3-13.

<sup>93</sup> *supra* n. 62.

<sup>94</sup> “Auditing refers to the ability of the FBI to retrace the steps of its agents after the collection has occurred,” thus providing accountability. Frank Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment?*, 80 N. C. L. REV. 315, 330 (2001).

<sup>95</sup> *supra* n. 58

<sup>96</sup> IITRI Report, at 4-5.

<sup>97</sup> *see id.*

<sup>98</sup> *see id.*

some, the lack of adequate auditing and accountability functions are still more indications of Carnivore's ill suitedness as a law enforcement tool.<sup>99</sup>

The lack of auditing procedures is made even worse when the FBI agent or agents using Carnivore access the device via the telephone link. Carnivore uses a type of remote access software known as pcAnywhere, which “does not provide audit on an individual basis” even though the agents use unique login IDs.<sup>100</sup> It has been noted that “PCAnywhere is *far* too powerful” for us with the telephone link,<sup>101</sup> as anyone logged in under the software could easily erase any trace that any changes had been made to Carnivore's settings.<sup>102</sup>

In the end, the lack of auditing and accountability functions gives rise to serious reservations about Carnivore. “Ultimately, it comes down to trust—of those who operate and control the system and of the software itself. Trusting a law enforcement agent to be honest and faithful to duty in a free society is one thing. Trusting complex, black-box software to be correct and operationally faithful to specifications, however, is quite another.”<sup>103</sup>

#### *F. Open Source Solution*

One suggestion that could go a long way towards eliminating the above listed problems has been suggested by several sources: making the Carnivore source code, the most basic details of its programming, publicly available for review.<sup>104</sup> IITRI suggested that the FBI should not release the source code until “technical limitations that could be

---

<sup>99</sup> David Sobel, *EPIC Comments on Carnivore Technical Review (12/1/00)*, available at [http://www.epic.org/privacy/carnivore/review\\_comments.html](http://www.epic.org/privacy/carnivore/review_comments.html) (Dec. 1, 2000) (on file with author).

<sup>100</sup> *supra* n. 96.

<sup>101</sup> *supra* n. 62 (emphasis in original).

<sup>102</sup> *supra* n. 96.

<sup>103</sup> *supra* n. 70.

exploited to defeat surveillance” are all fixed.<sup>105</sup> “The security benefits of making software open-source are well understood by the security community; open source could be expected to do much to strengthen a system as complex and security-critical as Carnivore.”<sup>106</sup> One might reasonably assume that allowing would-be targets of Carnivore to examine its source code would leave the system vulnerable, but this assumption is only partially correct. A number of technical professionals take the time to examine open source software and then inform the software’s designer (in this case, the FBI) of any possible bugs and security holes.<sup>107</sup> But in addition to providing an extra layer of analysis for Carnivore, releasing the Carnivore source code to public scrutiny is perhaps the only way to verify to the public that the device actually functions as the FBI and IITRI claim it does.<sup>108</sup>

### Part III: Statutory Framework

Understanding Carnivore’s capabilities and weaknesses is only the first step in understanding how it is actually used within a legal structure. There are a number of federal statutes and congressional acts that all pertain to the FBI’s ability to install and use Carnivore. Rather than examining these as part of a comprehensive regulatory scheme, this paper will address the issue chronologically, demonstrating how Congress has reacted to changes in technology over the years.

---

<sup>104</sup> *see e.g., supra* n. 58.

<sup>105</sup> IITRI Report, at 4-8.

<sup>106</sup> Matt Blaze, *Carnivore and Open Source Software*, available at <http://www.crypto.com/papers/opentap.html> (July 20, 2000) (on file with author).

<sup>107</sup> *see id.*

<sup>108</sup> *see id.*

### *A. Federal Communications Act of 1934*

The United States Supreme Court first addressed the tapping of telephones in 1928, with the majority holding that without an actual physical search or seizure, listening to a defendant's telephone calls is constitutional under the Fourth Amendment.<sup>109</sup> Justice Brandeis vigorously argued in the dissent, stating the case for increasing privacy rights in the face of rapidly expanding technology: "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."<sup>110</sup> By exposing that which many consider private, Carnivore threatens to do just what Justice Brandeis predicted.

Congress responded to Justice Brandeis' warning with the Federal Communications Act of 1934, which stated in part that "no person not being authorized by the sender shall intercept any communication."<sup>111</sup> This complete prohibition on wiretapping served as the only relevant federal statute for many years.

### *B. Omnibus Crime Control and Safe Streets Act of 1968*

In 1967, the Supreme Court readdressed wiretapping with respect to the Fourth Amendment, overruling *Olmstead* and holding that the Fourth Amendment prohibited warrantless tapping of telephones.<sup>112</sup> The *Katz* decision also featured the now-famous concurrence by Justice Harlan, in which the "expectation of privacy" test was first put forth: Harlan wrote that in cases where "a person [has] exhibited an actual (subjective)

---

<sup>109</sup> *Olmstead v. United States*, 277 U.S. 438, 464 (1928).

<sup>110</sup> *see id.*, at 474.

<sup>111</sup> Federal Communications Act, 48 Stat. 1103 (1934).

<sup>112</sup> *Katz v. United States*, 389 U.S. 347 (1967).

expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable,’” the police must acquire a warrant in order to conduct a search.<sup>113</sup> Partially in response to this decision, which they felt significantly hampered law enforcement, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968,<sup>114</sup> Title III of which dealt specifically with the procedures for obtaining a warrant to intercept communications.<sup>115</sup>

### *C. Foreign Intelligence Surveillance Act of 1978*

The Foreign Intelligence Surveillance Act (FISA) of 1978<sup>116</sup> was passed due to the need for secrecy in investigations of suspected foreign intelligence agents.<sup>117</sup> The act specifies that FISA procedures may be utilized only in investigations of non-“United States person[s],” a term of art that excludes both U.S. citizens and permanent resident aliens.<sup>118</sup> Applications for search warrants under FISA, which can and almost certainly have authorized the use of Carnivore,<sup>119</sup> are submitted to a special panel of judges who are selected by the Chief Justice of the United States Supreme Court.<sup>120</sup> The FISA court meets in a sealed room at the Department of Justice.<sup>121</sup> In short, FISA presents an

---

<sup>113</sup> *see id.*, at 361.

<sup>114</sup> Omnibus Crime Control and Safe Streets Act, *codified as amended in* 18 U.S.C.A. §§ 2510-2520 (1968).

<sup>115</sup> RICHARD TURKINGTON & ANITA ALLEN, *PRIVACY LAW*, at 229 (1999).

<sup>116</sup> Foreign Intelligence Surveillance Act, Pub. L. 95-511, 92 Stat. 1783 (1978), *codified at* 50 U.S.C. 1801-1829 (2001)

<sup>117</sup> John Lewis, *Carnivore—The FBI’s Internet Surveillance System: Is it a Rampaging Emailasaurus Rex Devouring Your Constitutional Rights?*, 23 WHITTIER L. REV. 317, 341 (2001).

<sup>118</sup> 50 U.S.C. 1801(i)

<sup>119</sup> “80% of Carnivore’s cases have involved national security,” strongly implying that it was the FISA court that issued the orders for its use. Declan McCullagh, *fyi: FC: FBI agent reportedly gives public demo of Carnivore*, available at <http://jis.mit.edu/pipermail/saag/2000q4/000107.html> (Oct. 25, 2000) (on file with author).

<sup>120</sup> John Lewis, *Carnivore—The FBI’s Internet Surveillance System: Is it a Rampaging Emailasaurus Rex Devouring Your Constitutional Rights?*, 23 WHITTIER L. REV. 317, 341 (2001).

<sup>121</sup> *see id.*

alternative to the ordinary Title III method of gaining judicial permission to utilize Carnivore, but that alternative can be dangerous to privacy.

While the need for FISA to “serve as the government’s primary means of collecting information on suspected terrorist collaborators”<sup>122</sup> is surely valid, a brief overview of the FISA court shows that it could easily be used for malicious investigations. The FISA court has been little more than a rubber-stamping procedure for secret search warrants over the last several years, as evidenced by the fact that during calendar years 1996-1999, the court failed to grant only *seven* out of well over three thousand applications.<sup>123</sup> In addition, during those years “[n]o orders were entered which modified or denied the requested authority.”<sup>124</sup>

Convincing evidence of the FBI’s and the DOJ’s abuse of the FISA court is found in the words of the court itself. The FISA court recently issued its first ever published ruling, denying some new DOJ proposals for intelligence sharing procedures.<sup>125</sup> The court strongly criticized the FBI’s “misstatements and omissions of material facts”<sup>126</sup> in its presentations of evidence, ample proof that FISA warrants can be misused just as easily, if not more so, than Title III warrants.

#### *D. Cable Communications Policy Act of 1984*

---

<sup>122</sup> Anthony Orr, *Marking Carnivore’s Territory: Rethinking Pen Registers on the Internet*, 8 MICH. TELECOMM. TECH. L. REV. 219, 246 (2001).

<sup>123</sup> *Annual Foreign Intelligence Surveillance Act Reports to Congress, 1996-1999*, available at [http://www.usdoj.gov/ag/readingroom/ag\\_foia1.htm](http://www.usdoj.gov/ag/readingroom/ag_foia1.htm) (last visited Dec. 5, 2002) (on file with author).

<sup>124</sup> *see id.* There is an apparent problem with the fact that the FISA court failed to grant seven applications, yet also never modified or denied any applications. This is due to the fact that the reports are filed yearly, and some applications submitted towards the end of the year are not heard until the following year.

<sup>125</sup> Dan Eggen & Susan Smith, *Secret Court Rebuffs Ashcroft, Justice Dept. Chided on Misinformation*, WASHINGTON POST, August 23, 2002, at A1.

<sup>126</sup> *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, Docket Numbers: Multiple (F.I.S.C. 2002). Note that while the FISA court’s holding pertaining to intelligence sharing procedures was overturned via the internal appeals procedure of FISA, the assertions of the court regarding FBI and DOJ abuse were left standing.

While the typical user accesses the Internet via a traditional telephone line or a high-speed Ethernet line, technology has enabled much faster access via coaxial cables of the type used to broadcast cable television, by routing the cable through a cable modem.<sup>127</sup> This sort of setup raises two difficulties for Carnivore: to begin with, due to the much faster access speed of cable modems, attempting to intercept packets on a cable modem network (such as the one being used at the University of Kentucky by the author of this paper) “would be like drinking from a firehose—you would miss lots of the data.”<sup>128</sup> In addition, due to the technological nature of cable modem communications, Carnivore-type interceptions may be simply “out of the question.”<sup>129</sup>

However, simple because Carnivore may not be technologically capable of intercepting cable modem traffic does not mean that it is impossible. However, from a legal standpoint it may be much more difficult to do. Under current case law and subsequent federal statutes, using Carnivore as a pen register to intercept electronic communications is constitutional with only a court order, as opposed to a judicial warrant.<sup>130</sup> However, long before cable television technology began being utilized for Internet access, Congress passed the Cable Communications Policy Act (CCPA) of 1984<sup>131</sup> to limit the government’s capability “to snoop on what people were watching on their televisions.”<sup>132</sup> Under the CCPA, “e-mail sent by cable modem actually has a greater protection under the law of surveillance than that sent by modem or Ethernet wire,”<sup>133</sup>

---

<sup>127</sup> *supra* n. 45.

<sup>128</sup> *see id.*

<sup>129</sup> *see id.*

<sup>130</sup> *infra* pp. 28-31.

<sup>131</sup> Cable Communications Policy Act, Pub. L. 98-549, 98 Stat. 2780 (1984).

<sup>132</sup> Aaron Kendal, *Carnivore: Does the Sweeping Sniff Violate the Fourth Amendment?*, 18 T. M. COOLEY L. REV. 183, 188 (2001).

<sup>133</sup> *see id.*

simply by virtue of traveling along a coaxial cable. However, to date no court has thus applies the CCPA to limit electronic surveillance such as Carnivore.<sup>134</sup>

#### *E. Electronic Communications Privacy Act of 1986*

Once again, the Supreme Court played a role in the statutory evolution of communications interception. In 1977, the Court ruled that pen registers, devices used to “record the date, time, and numbers that were dialed on a telephone,”<sup>135</sup> did not fall under the scope of Title III.<sup>136</sup> The Court again ruled on the use of pen registers as a law enforcement tool in 1979 in *Smith v. Maryland*, holding that warrantless use of pen registers falls outside the scope of the Fourth Amendment.<sup>137</sup> In the space of two years, the Court had ruled that pen registers are not only permissible under then-current statutes, but under the federal Constitution as well. Congress responded to these decisions, and to other technological advances in communication, with the Electronic Communications Privacy Act (ECPA) of 1986,<sup>138</sup> which substantially amended Title III.<sup>139</sup>

ECPA divided Title III into three separate provisions: Title I, which deals with the interception of the contents of communications, Title II, regulating the acquisition of stored communications and communications records, and Title III, regulating the use of pen registers and trap and trace devices.<sup>140</sup> Titles I and III of ECPA will be discussed below.

---

<sup>134</sup> *see id.* In addition, to the author’s knowledge no court has ever been asked to apply the CCPA to limit electronic surveillance.

<sup>135</sup> *see id.*, at 254.

<sup>136</sup> *United States v. New York Telephone Company*, 434 U.S. 159 (1977).

<sup>137</sup> *Smith v. Maryland*, 442 U.S. 735 (1979).

<sup>138</sup> *Electronic Communications Privacy Act*, Pub. L. 99-508, 100 Stat. 1848 (1986).

<sup>139</sup> RICHARD TURKINGTON & ANITA ALLEN, *PRIVACY LAW*, at 230 (1999).

<sup>140</sup> *see id.* All subsequent references to Title III should be taken to mean Title III of the ECPA, as opposed to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which in essence became Title I of the ECPA, *see id.*, at 231.

Section 2518 of Title I provided “procedure for interception of wire, oral, or electronic communications.”<sup>141</sup> Subsection 3 provides the basic framework for the now-common “probable cause” terminology, stating that upon application by a law enforcement or investigative office:

“(3) ... the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications... if the judge determines on the basis of the facts submitted by the applicant that—

- (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense...;
- (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, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.”<sup>142</sup>

As applied to *Carnivore*, this section of ECPA meant that in order for the FBI to implement the device in its content collection mode, it would be required to go before a federal judge and submit evidence that must hold up to the “substantial” burden of probable cause.<sup>143</sup> In addition, subsection 6 of § 2518 requires periodic progress reports to the judge issuing the warrant, to be made whenever the judge requests.<sup>144</sup> This high burden of proof has found praise in the legal community: “requiring the government to

---

<sup>141</sup> *see id.*, at 810. The ECPA has been amended by the USA-PATRIOT Act of 2001, *infra* pp. 33-35, and therefore all quotations from and citations to the ECPA are taken from a reprinting of the act prior to its amendment, *see id.*, 795-839.

<sup>142</sup> *see id.*, at 811.

<sup>143</sup> JOHNNY KILLIAN & GEORGE COSTELLO, ANALYSIS AND INTERPRETATION: ANNOTATIONS OF CASES DECIDED BY THE SUPREME COURT OF THE UNITED STATES (1998).

meet a ‘probable cause’ standard whenever it seeks to intercept electronic mail, header information, or contents, would provide the level of privacy protection to Internet communications contemplated by the Fourth Amendment.”<sup>145</sup>

By contrast, when used as a pen register or trap and trace device under its more filtered settings, Carnivore requires a much lower burden of proof for judicial approval.

“While Carnivore is not a pen register device per se, the FBI clearly programmed Carnivore to emulate a pen register. 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.”<sup>146</sup>

The procedures for acquiring said approval to use Carnivore as a pen register device are found in § 3123 of Title III.

Title III provides fewer procedural protections for the individual to be monitored than Title I, under the doctrine enumerated by the Supreme Court in *Smith v. Maryland* that pen registers do not constitute an invasion of privacy.<sup>147</sup> Perhaps most importantly, § 3123 states that upon application for a court order authorizing a pen register, a judge “shall enter an ex parte order authorizing the installation,” as opposed to the word “may” used in Title I.<sup>148</sup> In addition, rather than adhering to the strict “probable cause” standard, Title III orders for pen registers must only determine “that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”<sup>149</sup>

---

<sup>144</sup> RICHARD TURKINGTON & ANITA ALLEN, *PRIVACY LAW*, at 813 (1999).

<sup>145</sup> Peter Young, *The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy*, 35 *IND. L. REV.* 303, 320 (2001).

<sup>146</sup> Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement’s Newest Electronic Surveillance Strategy*, 21 *LOY. L.A. ENT. L.J.* 481, 501 (2001) (citations omitted). It should be noted that this article was written prior to the USA-PATRIOT Act of 2001, discussed below. At the time it was written, statutes did not explicitly authorize devices such as Carnivore, necessitating the analogy to telephone surveillance.

<sup>147</sup> RICHARD TURKINGTON & ANITA ALLEN, *PRIVACY LAW*, at 255 (1999).

<sup>148</sup> *see id.*, at 835 (emphasis added).

<sup>149</sup> *see id.*

Furthermore, Title III contains none of the judicial supervision procedures found in Title I. Lastly, while Title I contains an exclusionary provision for evidence obtained outside of its standards,<sup>150</sup> Title III contains no such protection. It is under these limited burdens that the FBI has been implementing Carnivore, when used in pen mode.

*F. Communications Assistance for Law Enforcement Act of 1994*

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 was one of the first federal acts that targeted the boom in technology surrounding the Internet, but was strongly opposed by both telecommunications carriers and civil liberties organizations.<sup>151</sup> CALEA requires that telecommunications carriers (such as ISPs) “cooperate in the interception of communications for law enforcement purposes, and for other purposes.”<sup>152</sup> In other words, CALEA would require an ISP to assist the FBI in intercepting the communications that would be intercepted by Carnivore. This premise was thoroughly adopted by the U.S. Court of Appeals for the D.C. Circuit in *U.S. Telecom Association v. FCC*, holding that CALEA requires telecommunications carriers (including ISPs) to install technology that would allow for the interception of digital packet-switched data.<sup>153</sup>

“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 own systems from criminal conduct by using commercial sniffers that operate like Carnivore, but without the cumbersome Fourth Amendment information filters.”<sup>154</sup>

---

<sup>150</sup> *see id.*, at 806.

<sup>151</sup> PHILIPPA STRUM, *PRIVACY: THE DEBATE IN THE UNITED STATES SINCE 1945*, at 161(1999).

<sup>152</sup> Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994).

<sup>153</sup> *United States Telecom Assoc. v. Federal Communications Commission*, 227 F.3d 450, 464-465 (D.C.Cir. 2000)

<sup>154</sup> Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L.J. 481, 509-510 (2001).

In fact, many ISPs regularly conduct the type of surveillance that Carnivore is capable of for nothing more insidious than routine system maintenance, and in some circumstances have refused FBI requests to place Carnivore devices on their servers, stating that the ISP itself can do a better job of monitoring.<sup>155</sup> Network administrators know their own systems better than even highly technically proficient FBI agents, thus making it much easier for the ISP to monitor itself.<sup>156</sup> It is because of this that “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.”<sup>157</sup> Due to the CALEA, ISPs no longer have an option to refuse to cooperate with FBI surveillance, and even large ISPs with the resources and capabilities to perform the necessary interception can now be legally required to allow Carnivore to be placed on their servers.

*G. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*

September 11, 2001, is a date that Americans will never forget. The terrorist attacks in New York and Washington, D.C. have stamped themselves into the national consciousness, and many aspects of life after September 11 have been permanently altered. One of these aspects is surely the monitoring of Internet communications. “Just hours” after the attacks, “FBI agents began to visit Web-based, e-mail firms and network providers,” demanding that Carnivore devices be placed on their servers.<sup>158</sup> Less than two months after the attacks, Congress had passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

---

<sup>155</sup> *supra* n. 42

<sup>156</sup> *see id.*

<sup>157</sup> Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement’s Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L.J. 481, 509-510 (2001).

Act (USA-PATRIOT) of 2001,<sup>159</sup> substantially revising a number of federal law enforcement statutes, Title III among them.

“The FBI and the DOJ have claimed that existing statutory provisions, the pen register and trap and trace portion of the Electronic Communications Privacy Act and Title III of the Omnibus Crime Control and Safe Streets act of 1968, authorize surveillance conducted via Carnivore’s pen and full modes, respectively. Some commentators have questioned this claimed authority; however, such questions about authorization have been rendered moot by legislation enacted in the wake of the September 11, 2001 terrorist attacks on the United States.”<sup>160</sup>

USA-PATRIOT amended ECPA specifically so as to include Internet monitoring devices such as Carnivore. As amended, the relevant portion of Title III now reads:

“A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.”<sup>161</sup>

While Carnivore was certainly used prior to USA-PATRIOT, this is the specific authorization needed to provide full statutory coverage. However, it remains to be seen how the Supreme Court will interpret the addition of “routing and addressing” information under the concept of pen registers.<sup>162</sup>

In addition, the USA-PATRIOT Act amended the FISA so that it became applicable not just to counterintelligence and espionage investigations, but to “any investigation to obtain foreign intelligence information... or to protect against

---

<sup>158</sup> Declan McCullagh, *Anti-Attack Feds Push Carnivore*, WIRED NEWS, available at <http://www.wired.com/news/print/0,1294,46746,00.html> (Sept. 12, 2001) (on file with author).

<sup>159</sup> Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub.L. 107-56, 115 Stat. 272 (2001).

<sup>160</sup> Thomas McCarthy, *Don’t Fear Carnivore: It Won’t Devour Individual Privacy*, 66 MO. L. REV. 827, 842 (2001) (citations omitted).

<sup>161</sup> 18 U.S.C. § 3121 (c)

international terrorism.”<sup>163</sup> This new language carries with it “a broad mandate”<sup>164</sup> in the wake of September 11 to conduct electronic surveillance on any number of people. “Where criminal charges are not pending or even contemplated, FISA will serve as the government’s primary means of collecting information on suspected terrorist collaborators within the United States.”<sup>165</sup>

#### Part IV: Constitutional Considerations

Above, the more mundane aspects of Carnivore’s existence are examined: what it is, how it works, what its technical drawbacks are, and how it is used in a statutory framework. However, the most essential aspect of understanding Carnivore in a contemporary context is the constitutional perspective. The law must constantly adapt to changing technologies, and must do so with Carnivore as well. This section will demonstrate that Carnivore is far from a simple tool of the law enforcement community. At a very fundamental level, Carnivore is an affront to some of the most core values of constitutional jurisprudence.

##### *A. Carnivore, Pen Registers, and the Fourth Amendment*

The modern era of Fourth Amendment law can be understood as beginning with *Katz v. United States*.<sup>166</sup> *Katz* overruled the Supreme Court’s holding in *Olmstead v. United States*,<sup>167</sup> finding that “the Fourth Amendment protects people, not places.”<sup>168</sup> However, it is Justice Harlan’s now-famous concurrence in *Katz* that expounded the

---

<sup>162</sup> see discussion *infra* pp. 35-39.

<sup>163</sup> 50 U.S.C. § 1842(a)(1)

<sup>164</sup> Anthony Orr, *Marking Carnivore’s Territory: Rethinking Pen Registers on the Internet*, 8 MICH. TELECOMM. TECH. L. REV. 219, 245 (2001).

<sup>165</sup> Anthony Orr, *Marking Carnivore’s Territory: Rethinking Pen Registers on the Internet*, 8 MICH. TELECOMM. TECH. L. REV. 219, 246 (2001).

<sup>166</sup> 389 U.S. 347 (1967)

<sup>167</sup> 277 U.S. 438 (1928)

principle with which the Court has since examined Fourth Amendment searches. Harlan wrote that the Fourth Amendment creates “a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”<sup>169</sup> The standard has been adopted by the Court in most Fourth Amendment questions.<sup>170</sup>

As stated above,<sup>171</sup> the Court has ruled on the acceptability of pen registers several times. The Court found that pen registers were not covered by the requirements of Title III in *US v. New York Tel. Co.*,<sup>172</sup> and that pen registers fell outside the scope of the Fourth Amendment itself because a person cannot have a reasonable expectation of privacy in information voluntarily given over to a third party.<sup>173</sup> The theory that information conveyed to a third party loses its constitutional privacy protection was by no means a revolutionary one in *Smith*, as the Court had consistently held that such information could be legally seized without a warrant in a variety of situations.<sup>174</sup>

However, not all courts agree that the Supreme Court’s reasoning in excluding pen registers from Fourth Amendment protections was valid. Courts in Texas and New Jersey, among other states, have held that state constitutional provisions nearly identical to the Fourth Amendment do in fact provide protection against warrantless pen register usage.<sup>175</sup> The court in the Texas case put it best: “The mere fact that a telephone caller has disclosed the number called to the telephone company for the limited purpose of

---

<sup>168</sup> *Katz v. United States*, 389 U.S. 347, 351 (1967).

<sup>169</sup> *see id.*, at 361

<sup>170</sup> *see e.g.*, *California v. Greenwood*, 486 U.S. 35 (1988).

<sup>171</sup> *infra* pp. 28-31.

<sup>172</sup> 434 US 159 (1977)

<sup>173</sup> *Smith v. Maryland*, 442 U.S. 735 (1979).

<sup>174</sup> *see e.g.*, *United States v. Miller*, 425 U.S. 435 (1976), *see also Hoffa v. US*, 385 US 293 (1966).

obtaining the services does not invariably lead to the conclusion that the caller has relinquished his expectation of privacy.”<sup>176</sup>

Applying Harlan’s test from *Katz* to pen registers, it is difficult to understand just why the Supreme Court decided to exclude them from constitutional protection. A person can expect that his or her dialing (or in the case of e-mail, addressing) information will remain private, even if the Court does not reasonably assume so. As for the premise that society must accept an expectation of privacy as “reasonable” in order for the Court to protect it against law enforcement encroachment, how exactly is this societal expectation measured? Surely with any aspect of technological surveillance, evidence can be found proving that the communication is not as secure as many people would like to believe. However, the mere fact that privacy in the communication can be threatened does not necessarily eliminate any vestige of privacy. Society can legitimately sanction some types of communication as private despite the fact that some limited disclosure must take place in order for the communication to occur. In addition, there is ample evidence that society *does* expect its e-mail to remain private. The American Bar Association has concluded that lawyer-client communication via e-mail is perfectly acceptable, “because the medium affords a reasonable expectation of privacy.”<sup>177</sup>

Specifically dealing with Carnivore, it should be understood that Carnivore is not actually a pen register, even when operating in “pen mode.” Electronic addressing information reveals much more about a person than do the numbers dialed on a

---

<sup>175</sup> Richardson v. State, 865 S.W. 2d 944 (Tex.Cr.App. 1993), *see also* State v. Hunt, 91 N.J. 338 (N.J. 1982), *see also* Mark Elmore, *Big Brother Where Art Thou, Electronic Surveillance and the Internet: Carving Away Fourth Amendment Privacy Protections*, 32 TEX. TECH. L. REV. 1053, 1063 (2001).

<sup>176</sup> Richardson v. State, 865 S.W. 2d 944, 951 (Tex.Cr.App. 1993).

<sup>177</sup> Frank Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment?*, 80 N. C. L. REV. 315, 337. (2001).

telephone—in essence, addressing and routing information reveals true content.<sup>178</sup> It is undeniable that ISP administrators can view addressing information without any problem, but it is illogical to therefore assume that no privacy exists in that information. After all, those same administrators can snoop on content as well.

While the Supreme Court possibly erred by excluding pen registers from the scope of the Fourth Amendment, a number of lower courts have exhibited great confusion over how to treat e-mail. One court has analogized e-mail to a postcard, the contents of which can be read by anyone with the desire, utterly eliminating any expectation of privacy in the communication.<sup>179</sup> Another court applied another mail analogy, comparing e-mail to an envelope, wherein the contents are private but the addressing information is not.<sup>180</sup> Yet another court held that so long as the e-mail was being stored on a computer and had not yet actually been read by the recipient, it held no constitutional protection.<sup>181</sup> Still another court expounded a rule that is nearly the polar opposite, holding that the sender's expectation of privacy is paramount while the communication is in transit, but it is virtually eliminated once the e-mail has been received.<sup>182</sup>

In short, the relatively new technology of e-mail has befuddled a number of courts in multiple jurisdictions. However, when compared to other new surveillance technology, the courts have been remarkably open to allowing governmental searches. The Fourth Circuit struck down an attempt by law enforcement to utilize a digital pager

---

<sup>178</sup> Thomas McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MO. L. REV. 827, 845-846 (2001).

<sup>179</sup> *Smyth v. Pillsbury Company*, 914 F.Supp. 97, 101 (E.D.Pa. 1996).

<sup>180</sup> *United States Telecom Association v. Federal Communications Commission*, 227 F.3d 450 (D.C.Cir. 2000).

<sup>181</sup> *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5<sup>th</sup> Cir. 1994).

clone for the highly technical reason that it was not attached to a phone line as the ECPA required.<sup>183</sup> However, the seminal case in this area is *Kyollo v. US*.<sup>184</sup> In *Kyollo*, the Supreme Court invalidated a search done using thermal imaging technology for the specific reason that the technology was not in “general public use.”<sup>185</sup>

This is the standard that should be applied to online communication surveillance. In cases like *Smith*, the Court has held that since the possibility of third party eavesdropping exists, there is no reasonable expectation of privacy.<sup>186</sup> However, a more logical standard would be that used by the Court in *Kyollo*: that while the possibility of non-law enforcement surveillance may exist in our technological society, so long as the technology used for the surveillance is not in general public use the expectation of privacy still carries its full force. Using this standard, pen registers and all forms of Internet communications would receive the full protection of the Fourth Amendment, as one would expect contemporary citizens rationally desire.

#### *B. Carnivore and the Exclusionary Rule*

Simply put, the exclusionary rule is one of the most powerful judicial implements to keep law enforcement from running ragged over constitutional freedoms. It “*can* deter illegal police searches,”<sup>187</sup> a fact that should not be overlooked.

The exclusionary rule found its origins in *Weeks v. US*,<sup>188</sup> holding that evidence gained from illegal searches was inadmissible in federal criminal trials. That rule was

---

<sup>182</sup> *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996).

<sup>183</sup> *Brown v. Waddell*, 50 F.3d 285 (4<sup>th</sup> Cir. 1995).

<sup>184</sup> *Kyollo v. United States*, 533 U.S. 27 (2001).

<sup>185</sup> *see id.*, at 30

<sup>186</sup> *supra* n. 173

<sup>187</sup> Bradley Canon, *Testing the Effectiveness of Civil Liberties Policies at the State and Local Levels: The Case of the Exclusionary Rule*, 5 AM. POL. QUARTERLY 57, reprinted in AMERICAN COURT SYSTEMS:

famously extended to apply to state trial courts as well in the famous case *Mapp v. Ohio*.<sup>189</sup> As Justice Clark stated in his opinion for the Court, “Nothing can destroy a government more quickly than its failure to observe its own laws, or worse, its disregard of the charter of its own existence.”<sup>190</sup> Without the exclusionary rule, law enforcement would have a nearly unlimited power to conduct illegal searches without consequence.

Unfortunately, that is precisely the case at hand when dealing with Carnivore in pen mode. The ECPA, as amended by the USA-PATRIOT Act, contains no exclusionary provision for evidence obtained via pen register. Since pen registers are currently not under the scope of the Fourth Amendment,<sup>191</sup> this means that any evidence that Carnivore illegally obtains while in pen mode is perfectly admissible in criminal court. This shakes the very foundations of justice upon which a free society is based. If our nation’s law enforcement entities can conduct illegal searches without even a semblance of probable cause, and later have the evidence admitted in a criminal trial, then the entire concept of due process has been undermined.

### *C. Law Enforcement vs. National Security*

To date, Carnivore has been utilized solely as a surveillance device under relevant federal statutes. However, a rather ominous argument could be made that no judicial authorization is required to use Carnivore at all, in any of its numerous collection modes. The argument could be made that in today’s world, with the heightened risk of terrorist

---

READINGS IN JUDICIAL PROCESS AND BEHAVIOR, at 610 (Sheldon Goldman & Austin Sarat eds., 1978) (emphasis added).

<sup>188</sup> *Weeks v. United States*, 232 U.S. 383 (1914).

<sup>189</sup> *Mapp v. Ohio*, 367 U.S. 643 (1961).

<sup>190</sup> *see id.*, at 659

<sup>191</sup> *supra* n. 173

attack, Carnivore can be used at will to further the promotion of national security interests.

There is a long line of Supreme Court cases detailing the ability of the government to conduct warrantless and indeed suspicionless searches so long as it furthers “legitimate governmental interests.”<sup>192</sup> Thus far national security has never been cited as one of these interests, but considering that current national climate it is no stretch of the imagination to believe that it soon will be. The cases follow two distinct lines of reasoning, both under the cover of protecting legitimate governmental interests. The first set of cases covers suspicionless and mandatory drug testing. The Supreme Court has ruled that it is constitutional under the Fourth Amendment to conduct drug tests on U.S. Customs Bureau agents,<sup>193</sup> to test train engineers,<sup>194</sup> to test high school students participating in extracurricular athletics,<sup>195</sup> and to test high school students participating in *any* extracurricular activity.<sup>196</sup> All of these drug testing cases allow for suspicionless searches that can be highly violative of individual privacy, all solely because the government has a legitimate interest in keeping schools and governmental agencies free from drug abuse.

The other line of cases follows similar reasoning, holding that public safety is a sufficient governmental interest to set up roadblocks and conduct searches. The Court has held that a permanent checkpoint to search for illegal aliens is constitutional under

---

<sup>192</sup> *Vernonia School District No. 47J v. Acton*, 515 U.S. 646 (1995) (quoting *Delaware v. Prouse*, 440 U.S. 648, 654 (1979)).

<sup>193</sup> *National Treasury Employees v. Von Raab*, 489 U.S. 656 (1989).

<sup>194</sup> *Skinner v. Railway Labor Executives Ass’n*, 489 U.S. 601 (1989).

<sup>195</sup> *Vernonia School Dist. No. 47J v. Acton*, 515 US 646 (1995).

<sup>196</sup> *Board of Ed. of Ind. School Dist. No. 92 of Pottawatomie County v. Earls*, 122 S.Ct. 2559 (2002).

the premise that such a search will improve public safety,<sup>197</sup> and the Court has held a checkpoint with the intent of catching drunk drivers constitutional.<sup>198</sup> However, the Court did draw the line at a checkpoint with the sole purpose of randomly conducting suspicionless searches of automobiles in order to find illegal narcotics.<sup>199</sup> In the case, the Court reasoned that the searches were being conducted with the clear intent of law enforcement, not to protect public safety.<sup>200</sup>

All things considered, if the FBI or some other governmental agency were to make the argument that random suspicionless Carnivore searches were being conducted not in order to prosecute criminals, but to protect the nation against another devastating terrorist attack, under current law it could quite possibly be held constitutional. Some may see no problem with this, and in fact find comfort in it, but such a precedent would fly in the face of the idea that suspicionless searches are antithetical to a free society.

### Summary

Carnivore's capabilities are a mixture of the necessary and the bewilderingly unconstitutional. For example, while some method of court-approved internet wiretapping is almost certainly within the scope of the Fourth Amendment, it is difficult at best to understand why the system's designers built in capabilities such as full mode collection, which could not conceivably be considered under constitutional current jurisprudence. The confusion surrounding Carnivore's purported uses and actual capabilities is compounded when viewed against the backdrop of the hodgepodge of legislation dealing with electronic wiretapping, much of which was passed before the

---

<sup>197</sup> United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

<sup>198</sup> Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

<sup>199</sup> Indianapolis v. Edmond, 531 U.S. 32 (2000).

<sup>200</sup> *see id.*

Internet was even a laboratory idea. This bafflement is compounded yet again when one considers the lack of direct precedent relating to government snooping of online communications, and the fact that the related precedents that do exist are often contradictory.

To obtain any type of certainty as to what the law is in this area, much more time and effort must be put into modernizing the law, by no means an easy process. Federal statutes should be crafted which address not only the interception of online communications, but a host of other legal issues involving the online industry. The courts, which have traditionally been slow to adapt to changing technologies, should become better versed with the basics of the Internet so as to render decisions that both uphold the spirit of the law and the ability of Americans to innovate and expand into new technological areas. Specifically regarding Carnivore, *much* more knowledge should be made public regarding its usage in the field and exact performance, so that the American people can have the assurance they need that it is not being used as a tool of of Big Brother government. Until all of the above conditions are met, Carnivore will remain at the very least a controversial tool of law enforcement.

The contention surrounding Carnivore, the statutory framework built up around it, and its Fourth Amendment considerations will surely continue for some time. “New technologies open new avenues of abuse, both by criminals and the government.”<sup>201</sup> It would be foolish to state with certainty that Carnivore is or is not violative of individual privacy when it functions and is used properly; is or is not an effective way to prevent terrorist attacks; is or is not an Orwellian monster. All that is certain is that Carnivore is

flawed, both technologically and jurisprudentially. Whether these flaws will prove to be fatal to Carnivore remains to be seen.

---

<sup>201</sup> Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic*

## Works Cited

*1999 Deployments*, available at <http://www.epic.org/privacy/carnivore/deployments.html> (last visited Dec. 5, 2002) (on file with author).

*Annual Foreign Intelligence Surveillance Act Reports to Congress, 1996-1999*, available at [http://www.usdoj.gov/ag/readingroom/ag\\_foia1.htm](http://www.usdoj.gov/ag/readingroom/ag_foia1.htm) (last visited Dec. 5, 2002) (on file with author).

AMERICAN COURT SYSTEMS: READINGS IN JUDICIAL PROCESS AND BEHAVIOR, (Sheldon Goldman & Austin Sarat eds., 1978).

Steven Bellovin, et al., *Comments on the Carnivore System Technical Review*, available at [http://www.crypto.com/papers/carnivore\\_report\\_comments.html](http://www.crypto.com/papers/carnivore_report_comments.html) (Dec. 3, 2000) (on file with author).

Matt Blaze & Steven Bellovin, *Tapping, Tapping On My Network Door*, CACM, Oct. 2000, at 124.

Board of Ed. of Ind. School Dist. No. 92 of Pottawatomie County v. Earls, 122 S.Ct. 2559 (2002).

Brown v. Waddell, 50 F.3d 285 (4<sup>th</sup> Cir. 1995).

Cable Communications Policy Act, Pub. L. 98-549, 98 Stat. 2780 (1984).

California v. Greenwood, 486 U.S. 35 (1988).

*Carnivore Puts Terror Investigation at Risk, Fox News Network*, available at [http://www.foxnews.com/printer\\_friendly\\_story/0,3566,53883,00.html](http://www.foxnews.com/printer_friendly_story/0,3566,53883,00.html) (May 29, 2002) (on file with author).

Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994).

Dan Eggen & Susan Smith, *Secret Court Rebuffs Ashcroft, Justice Dept. Chided on Misinformation*, WASHINGTON POST, August 23, 2002, at A1.

Frank Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment?*, 80 N. C. L. REV. 315 (2001).

Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986).

Mark Elmore, *Big Brother Where Art Thou, Electronic Surveillance and the Internet: Carving Away Fourth Amendment Privacy Protections*, 32 TEX. TECH. L. REV. 1053 (2001).

AMITAI ETZIONI, *THE LIMITS OF PRIVACY*, (1999).

E-mail interview with Matt Blaze, Research Scientist, AT&T Laboratories (Mar. 26, 2002).

*Extent of FBI's Web surveillance disclosed*, U.S.A. TODAY, May 4, 2001, available at <http://www.usatoday.com/life/cyber/tech/2001-05-04-carnivore.htm> (on file with author).

*FBI Memo on "FISA Mistakes,"* available at <http://www.epic.org/privacy/carnivore/fisa.html> (last visited Dec. 5, 2002) (on file with author).

Federal Communications Act, 48 Stat. 1103 (1934).

Foreign Intelligence Surveillance Act, Pub. L. 95-511, 92 Stat. 1783 (1978).

Joseph Goodman et al., *Cybercrime: Carnivore: Will it Devour Your Privacy?*, 2001 DUKE L. & TECH. REV. 28 (2001).

*Hearings on the Carnivore Diagnostic Tool Before the Subcomm. on the Constitution of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong. (2000) (statement of Barry Steinhardt, Associate Director, American Civil Liberties Union).

*Hearings on the Carnivore Diagnostic Tool Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106<sup>th</sup> Cong. (2000) (statement of Donald Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation).

*Hoffa v. United States*, 385 U.S. 293 (1966).

ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM FINAL REPORT* (2000).

In re All Matters Submitted to the Foreign Intelligence Surveillance Court, Docket Numbers: Multiple (F.I.S.C. 2002).

*Indianapolis v. Edmond*, 531 U.S. 32 (2000).

E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J. L. & TECH. 10 (2001).

*Katz v. United States*, 389 U.S. 347 (1967).

Aaron Kendal, *Carnivore: Does the Sweeping Sniff Violate the Fourth Amendment?*, 18 T. M. COOLEY L. REV. 183 (2001).

JOHNNY KILLIAN & GEORGE COSTELLO, ANALYSIS AND INTERPRETATION: ANNOTATIONS OF CASES DECIDED BY THE SUPREME COURT OF THE UNITED STATES (1998).

Neil King, Jr., *FBI's Wiretaps to Scan E-mail Spark Concern*, WALL STREET JOURNAL, July 11, 2000, at A3.

*Kyollo v. United States*, 533 U.S. 27 (2001).

George Leopold, *Flaws seen in FBI Net surveillance system*, ELECTRONIC ENGINEERING TIMES, June 13, 2002, at 22.

Barry Leiner et al., *A Brief History of the Internet*, E-ONTHEINTERNET, available at <http://www.isoc.org/oti/articles/0597/leiner.html> (last visited Dec. 5, 2002) (on file with author).

John Lewis, *Carnivore—The FBI's Internet Surveillance System: Is it a Rampaging Emailasaurus Rex Devouring Your Constitutional Rights?*, 23 WHITTIER L. REV. 317 (2001).

Letter from Donald Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, to Patrick Leahy, Ranking Member, Comm. of the Judiciary, United States Senate (Jan. 23, 2001) (on file with author).

Jay Lyman, *How Terrorists Use the Internet*, NEWS FACTOR NETWORK, available at <http://www.newsfactor.com/perl/story/7731.html> (Sept. 12, 2001) (on file with author).

*Mapp v. Ohio*, 367 U.S. 643 (1961).

Thomas McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MO. L. REV. 827 (2001).

Declan McCullagh, *Anti-Attack Feds Push Carnivore*, WIRED NEWS, available at <http://www.wired.com/news/print/0,1294,46746,00.html> (Sept. 12, 2001) (on file with author).

Declan McCullagh, *fyi: FC: FBI agent reportedly gives public demo of Carnivore*, available at <http://jis.mit.edu/pipermail/saag/2000q4/000107.html> (Oct. 25, 2000) (on file with author).

*Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990).

*National Treasury Employees v. Von Raab*, 489 U.S. 656 (1989).

Olmstead v. United States, 277 U.S. 438 (1928).

Omnibus Crime Control and Safe Streets Act, *codified as amended in* 18 U.S.C.A. §§ 2510-2520 (1968).

Anthony Orr, *Marking Carnivore's Territory: Rethinking Pen Registers on the Internet*, 8 MICH. TELECOMM. TECH. L. REV. 219 (2001).

*Report: Carnivore Could Be Abused*, U.S.A. TODAY, available at <http://www.usatoday.com/life/cyber/tech/cti834.htm> (Nov. 22, 2000) (on file with author).

Richardson v. State, 865 S.W. 2d 944 (Tex.Cr.App. 1993).

Robert Graham, *Sniffing (network wiretap, sniffer) FAQ*, available at <http://www.robertgraham.com/pubs/sniffing-faq.html> (Sept. 14, 2000) (on file with author).

Skinner v. Railway Labor Executives Ass'n, 489 U.S. 601 (1989).

Graham Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L.J. 481 (2001).  
Smith v. Maryland, 442 U.S. 735 (1979).

Smyth v. Pillsbury Company, 914 F.Supp. 97 (E.D.Pa. 1996).

David Sobel, *EPIC Comments on Carnivore Technical Review (12/1/00)*, available at [http://www.epic.org/privacy/carnivore/review\\_comments.html](http://www.epic.org/privacy/carnivore/review_comments.html) (Dec. 1, 2000) (on file with author).

State v. Hunt, 91 N.J. 338 (N.J. 1982).

Barry Steinhardt & Christopher Chiu, *ACLU Comments regarding Carnivore review team draft report*, available at [http://www.aclu.org/news/2000/carnivore\\_comments.html](http://www.aclu.org/news/2000/carnivore_comments.html) (Dec. 1, 2000) (on file with author).

Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5<sup>th</sup> Cir. 1994).

PHILIPPA STRUM, *PRIVACY: THE DEBATE IN THE UNITED STATES SINCE 1945* (1999).  
Telephone Interview with Archie Holland, Senior Network Administrator, Bluegrass Networks LLC (Feb. 26, 2002).

Bob Sullivan, *FBI software crack encryption wall: "Magic Lantern" part of new "Enhanced Carnivore Project"*, MSNBC, available at <http://msnbc.com/news/660096.asp?cpl1=1> (Nov. 20, 2002) (on file with author).

RICHARD TURKINGTON & ANITA ALLEN, *PRIVACY LAW* (1999).

United States Telecom Association v. Federal Communications Commission, 227 F.3d 450 (D.C.Cir. 2000)

United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

United States v. Miller, 425 U.S. 435 (1976).

United States v. New York Telephone Company, 434 U.S. 159 (1977).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub.L. 107-56, 115 Stat. 272 (2001).

Vernonia School District No. 47J v. Acton, 515 U.S. 646 (1995).

Weeks v. United States, 232 U.S. 383 (1914).

Frederick Wettering, *Counterintelligence: The Broken Triad*, 13 INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE 3 (2000).

Peter Young, *The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy*, 35 IND. L. REV. 303 (2001).