

---

---

# IS CARNIVORE DEVOURING YOUR PRIVACY?

MARICELA SEGURA\*

## I. INTRODUCTION

When the Federal Bureau of Investigation (“FBI”) wants to pursue criminals in cyberspace it uses Carnivore to do its bidding.<sup>1</sup> The Carnivore system is an internet search tool designed to collect electronic communications based on e-mail addresses, key words, or internet protocol addresses.<sup>2</sup> Operating in real-time, Carnivore searches through the binary code—the millions of 1’s and 0’s that comprise our internet communication.<sup>3</sup> By detecting a suspect’s identifying information, Carnivore isolates the suspect’s electronic communication, such as e-mail, from that of other users for further FBI examination.<sup>4</sup> Carnivore is an electronic wiretap that can collect a target’s electronic communications in real-time.

The Carnivore program encompasses a much broader scope than a traditional telephone wiretap: The electronic wiretap monitors the communications of all customers who pass through the internet service provider’s (“ISP”) system. By analogy, Carnivore does not tap into a

---

\* Class of 2002, University of Southern California Law School; B.A. 1992, University of California, Los Angeles. I would like to thank Professor Erwin Chemerinsky for providing expert guidance, support and inspiration to tackle constitutional questions. Thanks also to my parents, David and Maria Elena Segura, and all of my dear family for their tremendous love and support.

1. The Federal Bureau of Investigation has renamed Carnivore to the less menacing DCS1000. See Robert MacMillan, *Open-Carnivore Idea Sparks Lagging Conference*, NEWSBYTES NEWS NETWORK, at 2001 WL 2816314 (March 8, 2001). This Note will use the name Carnivore.

2. See Illinois Institute of Technology Research Center, Independent Review of the Carnivore System: Draft Report 1-1 (Nov. 17, 2000), at <http://www.cdt.org/security/carnivore/001117draftreport.pdf> [hereinafter IITRI Report].

3. See *Electronic Surveillance and Privacy: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (prepared statement of Donald M. Kerr, Assistant Director, Federal Bureau of Investigation), available at 2000 WL 1268432 [hereinafter *Kerr Senate Statement*].

4. See *id.*

particular line, but conducts a general “wiretap” of a segment of Pacific Bell’s customer base.<sup>5</sup> In this way, the system can conduct a far-reaching, general search of people who are not subject to a court order. For this reason, privacy advocates worry that the Carnivore system will facilitate a “fishing expedition” in search of any evidence of crime.<sup>6</sup>

To determine whether the current legal framework is appropriate for a system like Carnivore, this Note will examine which types of wiretap searches are legally sanctioned and how the program operates within these parameters. Here, the focus will be on the law and its application to the federal government, excluding equivalent state constitutional and statutory protections. Further, this Note will focus on analyzing the law as applied to domestic criminal investigations, and will consider foreign surveillance only briefly.<sup>7</sup>

Part II examines the controversy surrounding Carnivore’s use, analyzing how the system works and the findings of an independent review committee hired by the Justice Department. This Part looks at the recommendations of the committee as possible guidance for improving the system. Part III examines the current legal doctrine applying to federal actors and criminal investigations. This framework shows the tension between upholding a citizen’s right to privacy and promoting technologies that assist law enforcement efforts. Under the Electronic Communication Privacy Act (“ECPA”), the privacy protections granted to wire communications are not applied to electronic communications—a key issue—that lies at the center of the current Carnivore controversy. This Part also examines the scope of the law guiding “pen registers” or “trap and trace” searches—a function that law enforcement officers have tried to apply to the electronic context.

Part IV examines the results of the deficiencies in the current legal framework’s protection of electronic communication. This Part suggests that formalistic distinctions between wire and electronic communication and between “new” and “old” e-mail has created a legal framework that is meaningless with respect to the public’s expectation of privacy. Part V

---

5. See *Fourth Amendment Issues Raised by the FBI’s “Carnivore” Program: Hearing Before the House Subcomm. on the Constitution, House Comm. on the Judiciary*, 106th Cong. 71 (2000) (statement of Tom Perrine, Pacific Institute for Computer Security) [hereinafter *House Carnivore Hearings*].

6. Ted Bridis, *Congressional Panel Debates Carnivore as FBI Moves to Mollify Privacy Worries*, WALL ST. J., July 25, 2000, at A24.

7. The Foreign Intelligence Surveillance Act allows federal agents to conduct electronic surveillance for the purpose for foreign intelligence purposes. See 50 U.S.C. §§ 1801–1811 (1994).

examines the desirability of Carnivore as a search tool. What is most problematic about Carnivore's search capabilities is its ability to collect more data than a traditional wiretap would gather. Part VI makes specific recommendations for amending the statutory framework to properly protect electronic communication and to fashion a meaningful standard for using Carnivore as an internet search tool.

## II. WHAT IS THE CARNIVORE SYSTEM?

On July 11, 2000, the Wall Street Journal broke the news about an internet surveillance program the FBI called, "Carnivore." The story prompted a wave of news coverage expressing concern that the program "engage[s] in the widespread invasion of privacy of Americans who are not under investigation for any crimes."<sup>8</sup> In response to the news storm, the Committee on the Judiciary for the House of Representatives held hearings to examine the Fourth Amendment implications of the Carnivore program.<sup>9</sup> In addition, the Justice Department ordered an independent review of the system by the Illinois Institute of Technology Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law ("IITRI").<sup>10</sup> This Part will first discuss the mechanics of the program as outlined in the IITRI report, and then examine the team's specific recommendations.

### A. HOW DOES CARNIVORE WORK?

Even after independent review of Carnivore, questions linger about the program's actual capabilities.<sup>11</sup> Carnivore is a computer-based search

---

8. *Civil Liberties Groups Blast 'Carnivore,' Seek Privacy Protections*, ANDREWS EMPLOYMENT LITIGATION REPORTER, Oct. 3, 2000, at 10. See also Stephanie R. Geraci, *Electronic Privacy Information Center Confronts FBI Over Internet Surveillance System*, 17 No. 4 ECOMMERCE 10 (Aug. 2000); Ted Bridis & Neil King Jr., *Carnivore E-mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000, at A28.

9. See *House Carnivore Hearings*, *supra* note 5.

10. The Illinois Institute of Technology Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law, under contract with the Department of Justice, evaluated the Carnivore system and released its report on November 17, 2000. See *IITRI Report*, *supra* note 2. See also Barry Steinhardt & Christopher Chiu, *ACLU Comments Regarding Carnivore Review Team Draft Report*, at [http://www.aclu.org/news/2000/carnivore\\_comments.html](http://www.aclu.org/news/2000/carnivore_comments.html) (last visited Jan. 18, 2001) [hereinafter *Steinhardt Review*] (criticizing the review as not being objective or sufficiently addressing the essential Constitutional concerns of the program).

11. See, e.g., Steven M. Bellovin, Matt Blaze, David Farber, Peter Neumann & Eugene Spafford, *Comments on the Carnivore System Technical Review*, at [http://www.cdt.org/security/carnivore/001203\\_comments.html](http://www.cdt.org/security/carnivore/001203_comments.html) (last visited Jan. 18, 2001) [hereinafter *Comments on IITRI Review*]; *Steinhardt Review*, *supra* note 10 (asserting that due to time and financial restrictions the review team did not perform a separate analysis to verify that there is not a hidden code in the system).

tool, created to read and record all of the internet traffic that it is programmed to search.<sup>12</sup> The program enables the FBI to conduct a one-way tap into an Ethernet stream—the flow of electronic impulses carrying communications through an internet connection.<sup>13</sup> This method allows investigators to search out keywords, e-mail addresses or internet protocol (“IP”) addresses—a series of numbers and letters that correlate to websites.<sup>14</sup> Carnivore can conduct at least two types of searches. First, installed on an ISP’s network, Carnivore can monitor and record the full content of messages that a targeted user has sent in real-time.<sup>15</sup> This real-time, full-content search is conducted under the same basic legal structure that is employed for telephone wiretaps.<sup>16</sup> Second, Carnivore is reportedly able to acquire the address information for the origin and the destination of all communications to and from a particular ISP customer.<sup>17</sup> This function provides the TO and FROM addresses on an e-mail and is viewed as the electronic equivalent of a telephone pen-register or trap and trace search.<sup>18</sup>

The Carnivore hardware is comprised of computers at both ISP and FBI locations.<sup>19</sup> A “collection computer” is placed at an ISP and connected to an internet network, such as America Online (“AOL”).<sup>20</sup> This computer is loaded with the Carnivore software that can filter for target

---

12. Press Release, John E. Collingwood, Federal Bureau of Investigation Office of Public and Congressional Affairs, *The Carnivore Debate* (Aug. 18, 2000). *But see* Letter from David L. Sobel, General Counsel, Electronic Privacy Information Center, to Carnivore Review Panel (Dec. 1, 2000), [http://www.epic.org/privacy/carnivore/review\\_comments.html](http://www.epic.org/privacy/carnivore/review_comments.html) (last visited Jan. 18, 2001) [hereinafter Sobel Letter]. The Electronic Privacy Information Center (EPIC) has expressed concern that little is known about Carnivore’s capacity to search all unfiltered messages that pass through the ISP. The organization has pointed to a heavily redacted FBI document, which appears to claim that the personal computer on which a Carnivore test was run could “reliably capture and archive all unfiltered traffic.” *See id.* *See also* Electronic Privacy Information Center, Federal Bureau of Investigation Test Documents (June 5, 2000), [http://www.epic.org/privacy/carnivore/test\\_6\\_00.html](http://www.epic.org/privacy/carnivore/test_6_00.html) (acknowledging that the Carnivore program could retrieve all unfiltered information and save it onto the hard drive of the computer through which it is operating).

13. IITRI Report, *supra* note 2, at viii. *See also* Interview with Samuel Choi, Manager of Computer Information Systems, Los Angeles Philharmonic, in Los Angeles, Cal. (Mar. 4, 2001) (defining components of internet data transmission).

14. Interview with Samuel Choi, *supra* note 13.

15. *See* IITRI Report, *supra* note 2, at 3-12.

16. *See id.* at 4-2. *See also id.* at C-10 to -16 (showing test results for full content searches focused on IP addresses, e-mail addresses, and text strings).

17. *See id.* at 3-25.

18. *See House Carnivore Hearings, supra* note 5, at 61-62 (statement of Alan Davidson). In the telephone context pen registers are devices that capture the phone numbers dialed on outgoing telephone calls, while trap and trace units capture numbers identifying incoming calls. *See* 18 U.S.C. § 3127(3)-(4).

19. *See* IITRI Report, *supra* note 2, at ix.

20. *See id.*

information.<sup>21</sup> Via the collection computer, the Carnivore program conducts a one-way “tap” into the ISP data stream and can filter and collect all of the data passing through the segment to which it is attached.<sup>22</sup> Law enforcement agents can set Carnivore filters to search for specific electronic addresses—such as e-mail—or particular strings of text or data.<sup>23</sup> An FBI agent uses a telephone link and a computer to remotely access the collection computer and program filter settings, which indicate the information that the computer is supposed to retrieve.<sup>24</sup> Because the collection computer is typically installed without a keyboard or monitor, this task cannot be completed at the ISP site. As such, the collection computer at the ISP is merely a box that cannot be manipulated.<sup>25</sup>

Once the program has started collecting data that matches the search criteria, the collection computer sends the gathered data via telephone link to “control” computers at FBI sites.<sup>26</sup> The control computers process the raw data with software that translates it into a readable form for FBI agents.<sup>27</sup>

A basic understanding of how information is sent within computer networks reveals how Carnivore intercepts messages over the internet. ISP network computers communicate with each other by transmitting an electronic communication, such as an e-mail message, in smaller bundles called packets.<sup>28</sup> An e-mail is transmitted from one computer to another in several of these packets.<sup>29</sup> This fragmentation of the e-mail is problematic because the packets often mix up the content of the message with the address information. Thus, when a government agent uses the Carnivore program to conduct a pen register search—limited to the addresses in the TO and FROM lines—the program may also retrieve the body of the message.<sup>30</sup> The IITRI committee found that when Carnivore isolates an e-mail’s TO and FROM address information from a packet containing content, a series of X’s will replace that content, making it indiscernible to

---

21. *See id.* at ix–xi.

22. *Id.* at ix.

23. *See id.* at 3-12.

24. *See id.* at viii–ix.

25. *See id.*

26. *Id.* at ix.

27. *See id.* at xii. Packeteer and CoolMiner are programs that display data provided by Carnivore in a meaningful fashion. *Id.* All computers are equipped with Jaz disk drives to allow the stored data to be removed. *Id.* at ix.

28. *See* HENRY H. PERRITT, JR., *LAW AND THE INFORMATION SUPERHIGHWAY 5* (2d ed. 2001).

29. *See id.*

30. *See* IITRI Report, *supra* note 2, at 4-3 (discussing how content in fields other than the TO/FROM fields are replaced with X’s, thus providing information on the length of the message sent).

FBI agents.<sup>31</sup> The X's, however, reveal the length of the message conveyed.<sup>32</sup>

Alternatively, the program can be placed on full-collection mode, in which it will collect the full content of a user's electronic communications.<sup>33</sup> In this mode, Carnivore may collect an entire e-mail message sent between the target and another person. Donald Kerr, Assistant Director for the FBI Laboratory Division, stated that "during all the filtering/processing . . . no FBI personnel are seeing any information—all information filtering/processing, [is] purely in a machine-readable format . . . occurring exclusively 'within the box.'"<sup>34</sup>

In full-collection mode, the operator may also view the content of e-mail or instant messages sent, the sites browsed, and the files downloaded.<sup>35</sup> Full-collection mode, according to the government, is the approximate equivalent of a wiretap on a telephone line, although the risk of collecting nonpertinent information differs between the systems.<sup>36</sup> In a telephone wiretap, the agent is supposed to turn off the telephone intercept to avoid capturing irrelevant conversations.<sup>37</sup> With Carnivore, however, an agent must discard the nonpertinent information *after* the system has already gathered it.<sup>38</sup> Thus, the information is not discarded until after law enforcement agents have already viewed it, while with wire surveillance, the bulk of the irrelevant information may not be heard in the first place. This difference in the minimization efforts has led critics to call the two processes less than perfectly analogous.<sup>39</sup> With such broad capabilities, the IITRI concluded that "[i]ncorrectly configured, Carnivore can record any traffic it monitors."<sup>40</sup>

---

31. *See id.*

32. *See id.* Figure C-2 shows the result of a pen register search that is programmed to collect only the TO and FROM packets of an e-mail message. The content information is replaced with X's in this mode. *See id.* at C-3. The applicability of Carnivore pen register searches to the legal framework will be discussed in Part IV, *infra*.

33. *Id.* at 3-22 to -23.

34. *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987, and H.R. 4908 Before the House Comm. on the Judiciary, 106th Cong. 38* (prepared statement of Donald M. Kerr) [hereinafter *ECPA 2000 Hearings*].

35. *See* IITRI Report, *supra* note 2, at ix.

36. *See id.* at 4-2.

37. *See id.*

38. *See id.*

39. *See id.*

40. *Id.* at 4-3.

## B. WHAT DOES INDEPENDENT REVIEW OF CARNIVORE TELL US?

The scope of the IITRI report, released on November 17, 2000, was limited to the different types of searches the program conducts, the way the program acquires data and minimizes the collection of irrelevant data, and the “handling and post-processing” of the data. The IITRI did not consider the constitutionality of Carnivore or the “trustworthiness of law enforcement agents.”<sup>41</sup> The team concluded that in most cases, when properly configured, Carnivore provides investigators with no more information than is authorized by court order.<sup>42</sup> The IITRI emphasized that the program isolated the TO and FROM address information while in pen-mode.<sup>43</sup> In addition, the team found that Carnivore could successfully isolate the contents of communications both to and from a target with a fixed IP address.<sup>44</sup>

Despite the successful test results, the IITRI did not completely rubber stamp the program.<sup>45</sup> The committee suggested ways to improve the system to better ensure the security of electronic surveillance.<sup>46</sup> For example, the IITRI concluded that Carnivore collects excess data during pen register searches, in which only the TO and FROM fields of an e-mail are targeted.<sup>47</sup> The IITRI team called this practice “undesirable” because it reveals the length of the e-mail, which is more information than allowed under a pen register or trap and trace search that only gathers telephone numbers dialed.<sup>48</sup> Therefore, the report recommended that the software be rewritten to capture only the packets containing the TO and FROM data.<sup>49</sup> This, however, may be impossible since packets often contain both the header information and content.<sup>50</sup>

Another significant flaw noted by the IITRI is that the system contains no mechanism for auditing its use.<sup>51</sup> Agents logging onto the system do so under the term “Administrator” and are not required to enter individual passwords to conduct a search.<sup>52</sup> Instead, the password needed to program

---

41. *Id.*

42. IITRI Report, *supra* note 2, at xii.

43. *See id.* at ix.

44. *See id.* at 3-22 to -23.

45. *See* Sobel Letter, *supra* note 12.

46. IITRI Report, *supra* note 2, at A-1 to -4.

47. *Id.* at A-1.

48. *See id.* at xii.

49. *Id.* at A-1.

50. *See* discussion, *supra* Part II.A.

51. *See* IITRI Report, *supra* note 2, at A-2.

52. *See id.* at 4-4.

the filters is assigned to each search rather than to individual agents.<sup>53</sup> The IITRI report suggests that the program be reconfigured so that each programming task on Carnivore requires an individual password tied to an agent, making it possible to trace the particular search activity to a specific agent.<sup>54</sup> Without an auditing trail to facilitate individual accountability, the Carnivore system is not secure, and monitoring abuses remains virtually impossible.<sup>55</sup>

A related issue is that the same Carnivore software can be used to conduct both full-content searches and pen register searches.<sup>56</sup> Since these different types of searches require different legal thresholds, separate versions of the program should be designed to insure that the electronic wiretap is not accidentally or improperly configured.<sup>57</sup> Additionally, the report suggests that Carnivore should stamp the filter setting on the data collected in a tamper-free form. This stamp would be attached to the top of the collected data and would indicate, for example, that the information was gathered in pen register mode, and would also list the particular e-mail or information that was the target of the search. Creating this type of stamp will add an extra level of confidence that the search parameters have not been changed in the process of the electronic tap.<sup>58</sup> Most importantly, the report recommends publicly releasing the Carnivore source code in order to quell concerns about individual privacy. The team recognized that, in order to gain wide public acceptance of electronic surveillance, the technology must be demystified and understood in the same manner that telephone wiretap techniques are today.<sup>59</sup>

After the review was complete, critics charged that the IITRI team was biased.<sup>60</sup> A conflict of interest became apparent: Many members of the team had strong ties to the government, with one member having donated the maximum amount of money allowable to Vice President Al

---

53. *See id.*

54. *Id.* at A-2.

55. *See id.*

56. *See id.* at A-1.

57. *See id.* The placement of the pen-mode button next to the full-mode button leaves open the risk that with the slip of a finger the tap will collect more information than is authorized. *See id.*

58. *Id.* at A-3. The IITRI recognized that this capability is being added to Carnivore 2.0. *See also ECPA 2000 Hearings, supra* note 34, at 38 (prepared statement of Donald M. Kerr, Assistant Director of the Federal Bureau of Investigation, asserting that Carnivore does indeed provide an audit history, attached to each file collected during the operation of the program).

59. IITRI Report, *supra* note 2, at A-4.

60. *See* Letter from Dick Arney, House Majority Leader, to Janet Reno, Attorney General (Oct. 19, 2000), at <http://www.cdt.org/security/carnivore/001019armey.shtml> (last visited Nov. 12, 2000).

Gore's presidential campaign.<sup>61</sup> In addition, the Justice Department's refusal to identify the contractor who created Carnivore raised concerns that a conflict of interest between the IITRI and the developer could go undiscovered.<sup>62</sup> Some doubted that a review of this magnitude was even possible in fewer than six weeks with a budget of less than \$175,000.<sup>63</sup> While others, such as Barry Steinhardt, Associate Director of the American Civil Liberties Union, were concerned with the relevance of the report, given that the FBI was set to employ a new version of the system in the near future.<sup>64</sup>

The report is clear that there are serious concerns with the Carnivore system, even if it could successfully isolate target communications as intended. Given the fact that the report was highly redacted,<sup>65</sup> reliance on the IITRI's conclusions may be unwise. Carnivore has the capability to capture and record electronic communications while in transit.<sup>66</sup> In a worst-case scenario, the system could be scanning and recording all electronic communications that pass before it, without limiting the search to a particular individual subject to probable cause. The government could use general keyword searches to "fish" for crimes, or target individuals and groups it deems unsavory. A general search of public communication would be unconstitutional and in violation of the current statutory scheme. Many privacy advocates claim that the report confirms that individual privacy is at the mercy of federal agents who could configure a search to monitor all internet traffic.<sup>67</sup> Given the rise in racial profiling<sup>68</sup> and the call

---

61. *See id.*

62. *See id.*

63. *Institute's Report on Carnivore Causes Uproar Among Critics*, 4 No. 8 ANDREWS TELECOMMUNICATIONS INDUSTRY REPORTER, Dec. 21, 2000, at 12.

64. *Id.* *See also* Robert Lemos, *Experts: Carnivore Review Had No Teeth*, ZDNET NEWS FROM ZDWIRE, Dec. 4, 2000, available at 2000 WL 4022374 (finding that prominent academic security researchers have criticized the government review of Carnivore).

65. *See* IITRI Report, *supra* note 2, at D-1 to -9. The last several pages of the document have been left redacted. *Id.*

66. *See id.* at C-1 to -16 (showing testing results from Carnivore system checks).

67. *See generally* *Comments on IITRI Review*, *supra* note 11 (conducting a section by section critique of Carnivore's broad search capabilities).

68. *See generally*, Steven Rosenberg, *Backlash Stings Local Arabs Isolation Marks Crowning Community*, BOSTON GLOBE, Nov. 4, 2001, at North Weekly 1 (reporting on the rise of racial profiling in the North Shore community since the terrorist attacks on September, 11, 2001), Jodi Wilgoren, *A Nation Challenged: Arab Americans; Struggling to Be Both Arab and American*, N.Y. TIMES, Nov. 4, 2001, at IB (discussing the impact of the terrorist attacks and ethnic profiling on the cultural expression of Arab Americans).

for tightened security since the terrorist attacks on September 11, 2001,<sup>69</sup> governmental abuse of the system seems quite likely.

### III. THE LEGAL FRAMEWORK

#### A. CONSTITUTIONAL PROTECTIONS

Although the right to privacy is not expressly stated in the United States Constitution, the Supreme Court has found it to be a fundamental right subject to strict scrutiny.<sup>70</sup> The Court has found the right to privacy implicitly protected under the due process clauses of the Fifth and Fourteenth Amendments.<sup>71</sup> In addition to a general constitutional right to privacy, the Fourth Amendment explicitly provides that individuals' right to "be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."<sup>72</sup> Federal courts have defined the parameters of this right as what constitutes a search under the Fourth Amendment.<sup>73</sup> In this arena, technological surveillance poses a significant threat to individual privacy; however, the government has been "slow to respond to this unique type of 'search and seizure.'"<sup>74</sup> The constitutional standard for searches involving electronic surveillance developed in the context of government wiretapping of criminal suspects.<sup>75</sup>

The first case to challenge government wiretapping was *Olmstead v. United States*.<sup>76</sup> In *Olmstead*, federal officers fashioned wiretaps—without warrants—on the telephone lines in the street outside the suspects'

---

69. See *U.S. Attorney General John Ashcroft's Address at the U.S. Conference of Mayors*, available at [http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/ashcrofttext\\_1025](http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/ashcrofttext_1025) (last visited Oct. 29, 2001).

70. See ERWIN CHEMERINSKY, *CONSTITUTIONAL LAW PRINCIPLES AND POLICIES* 659 (1997) (discussing *Griswold v. Connecticut*, 381 U.S. 479 (1965), and Justice Douglas' finding that the right to privacy is implicit in provisions in the Bill of Rights).

71. See *id.* at 664 (discussing the due process clause of the Fourteenth Amendment as the basis for the right to privacy in *Roe v. Wade*, 410 U.S. 113 (1973)).

72. U.S. CONST. amend. IV.

73. CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, *CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS* 110–12 (4th ed. 2000).

74. *Id.* at 326.

75. See generally PERRITT, *supra* note 28, at 892–98 (discussing the common law development of Fourth Amendment privacy protection to government wiretaps).

76. 277 U.S. 438 (1928).

homes.<sup>77</sup> The Court held that the eavesdropping did not constitute a search or seizure because the taps were not a “trespass” on the suspect’s property, and the officers did not seize “tangible” items.<sup>78</sup> Justice Brandeis, in his now-famous dissent, cautioned that the interpretation of constitutional protections must keep pace with technology in order to prevent invasions of individual liberty.<sup>79</sup> Brandeis analogized wiretapping to the government opening one’s mail, but he cautioned that wiretapping threatened a greater invasion of privacy because it implicated “the privacy of the persons at both ends of the line.”<sup>80</sup>

The Court overturned *Olmstead* in *Katz v. United States*, holding that a warrant issued upon probable cause is a prerequisite to authorizing a wiretap.<sup>81</sup> The Court rejected the “trespass doctrine” from *Olmstead*, finding instead that the wiretap infringed Charles Katz’s reasonable expectation of privacy while using a public telephone booth.<sup>82</sup> The Court explained that the Fourth Amendment offers Constitutional protection of information that an individual seeks to keep private even when in a public area.<sup>83</sup>

Justice Harlan, in his concurrence, used an individual’s reasonable expectation of privacy as the standard for determining whether an intrusion caused a Fourth Amendment violation.<sup>84</sup> Harlan stated that the reasonableness test has two components: “[F]irst 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>85</sup> Thus, in order for a government search to be constitutional, it must not invade an area that an individual reasonably believes should remain private.

---

77. *Id.* at 456–57.

78. *See id.* at 464.

79. *See id.* at 474 (Brandeis, J., dissenting). *See also* PERRITT, *supra* note 28, at 892 n.243.

80. *Olmstead*, 277 U.S. at 476. *See also* Hillary Victor, Comment, *Big Brother Is at Your Back Door: An Examination of the Effect of Encryption Regulation on Privacy and Crime*, 18 J. MARSHALL J. COMPUTER & INFO. L. 825, 838 (2000).

81. *See Katz v. United States*, 389 U.S. 347 (1967). *See also* WHITEBREAD & SLOBOGIN, *supra* note 73, at 329; Victor, *supra* note 80, at 838.

82. *Katz*, 389 U.S. at 353, 359.

83. *Id.* at 351.

84. *Id.* at 360–61. In fact, analyzing whether an individual has a reasonable expectation of privacy is the contemporary theoretical foundation of Fourth Amendment privacy analysis. *See* WHITEBREAD & SLOBOGIN, *supra* note 73, at 329.

85. *Katz*, 389 U.S. at 361. For further discussion of the reasonableness test, see Victor, *supra* note 80, at 838–39 n.98 (discussing the application of Justice Harlan’s reasonableness test in subsequent court decisions).

Just prior to *Katz*, in *Berger v. New York*, the Court held that state statutes regulating court-ordered wiretaps must comply with traditional Fourth Amendment search warrant requirements.<sup>86</sup> In *Berger*, the New York wiretap statute was deficient in the following ways: (1) It did not require probable cause that a particular crime had been or was to be committed; (2) it lacked a requirement for a particularized description of the place to be searched and what was to be seized; (3) it failed to provide a termination date for the wiretap once the conversation sought was seized; (4) it failed to provide a provision for notice, instead allowing for uncontested entry without a showing of special circumstances; and (5) it did not require the officer to return a report to the court explaining how the warrant was executed and what was seized, giving the officer full discretion without judicial supervision.<sup>87</sup> Today, many of the principal concerns in *Berger* are codified as statutory requirements for wiretaps under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).

## B. STATUTORY PROTECTIONS

### 1. The Omnibus Crime Control and Safe Streets Act of 1968

In response to the issues the *Katz* and *Berger* decisions raised, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) to address federal government searches.<sup>88</sup> In passing Title III, Congress sought to balance the privacy concerns raised by the intrusiveness of eavesdropping against the need for surveillance tools to fight organized crime.<sup>89</sup> Title III limits the use of wiretaps to enumerated offenses<sup>90</sup> and requires a senior Justice Department official to approve the

---

86. 388 U.S. 41 (1967).

87. See *Berger*, 388 U.S. at 55–60.

88. Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2513, 2515–2520 (West 1994). See also WHITEBREAD & SLOBOGIN, *supra* note 73, at 330–31.

89. See James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 71 (1997) (citing *Controlling Crime Through More Effective Law Enforcement: Hearings on S. 300, S. 552, S. 580, S. 674, S. 675, S. 678, S. 798, S. 824, S. 916, S. 917, S. 992, S. 1007, S. 1094, S. 1194, S. 1333, and S. 2050 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 90th Cong. (1967)).

90. 18 U.S.C. § 2516(1)–(3). A partial list of the offenses for which wiretapping is allowed include: kidnapping, robbery, bribery of public officials, offenses involving counterfeiting, narcotics production, distribution, or purchase. 18 U.S.C. §§ 2516(1)(b)–(e).

wiretap order.<sup>91</sup> Further, the application requires government officials to provide a “full and complete statement of the facts and circumstances relied upon . . . to justify [their] belief that an order should be issued.”<sup>92</sup> For a warrant to be issued, the suspect must be alleged to have committed, or be expected to commit, an offense.<sup>93</sup>

Title III enhanced judicial oversight of wiretaps by providing specific guidelines to both applicants and courts issuing wiretap warrants. In a wiretap application, the law enforcement officer must include the following information: (1) the identity of the officers making and approving the application;<sup>94</sup> (2) the facts relied upon to justify the order—including details of the particular offense that has been, or is expected to be, committed, a particular description of the location of the interception, the type of communication to be intercepted, and the identity of the person targeted;<sup>95</sup> (3) whether other investigative procedures have been tried and have failed;<sup>96</sup> (4) the period of time for which the interception is required, including additional information, if probable cause exists to believe that communications of the same type will continue after the first relevant communication has been obtained;<sup>97</sup> and (5) information about all previous wiretap applications involving the same persons or facilities.<sup>98</sup> Where the order is an extension of an original wiretap warrant, the applicant must make a statement as to “the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.”<sup>99</sup> Additionally, Title III provides a minimization requirement—providing that the government officer must conduct the search in such a manner so as to reduce the interception of conversations outside the scope of the order.<sup>100</sup>

To approve the wiretap order, a judge must make four findings: First, probable cause that an enumerated offense is being—or will be—

---

91. See 18 U.S.C. § 2516(1). The list of officials authorized to approve an application includes: “[t]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General.” 18 U.S.C. § 2516(1).

92. 18 U.S.C. § 2518(1)(b).

93. *Id.*

94. 18 U.S.C. § 2518(1)(a).

95. 18 U.S.C. § 2518(1)(b).

96. 18 U.S.C. § 2518(1)(c). While lower courts differ on the interpretation of the exhaustion requirement, the Supreme Court has determined that it generally insures that eavesdropping is not the initial tool utilized in an investigation. See *WHITEBREAD & SLOBOGIN*, *supra* note 73, at 338.

97. 18 U.S.C. § 2518(1)(d).

98. 18 U.S.C. § 2518(1)(e).

99. 18 U.S.C. § 2518(1)(f).

100. 18 U.S.C. § 2518(5).

committed;<sup>101</sup> next, probable cause that a wiretap will obtain particular communications concerning that offense;<sup>102</sup> third, a belief that law enforcement officials have exhausted all reasonable and “normal investigative procedures;”<sup>103</sup> and finally, a determination that the facilities to be intercepted are—or will be—used in commission of the offense or that they “are leased to, listed in the name of, or commonly used by [the person subject to the order].”<sup>104</sup>

Title III includes privacy protections in addition to the standards outlined in *Berger*. Pursuant to the statute, the issuing judge has the discretion to require periodic surveillance reports.<sup>105</sup> Once the wiretap is completed, law enforcement officers must give notice of the surveillance to the person subject to the order.<sup>106</sup> Title III also provides a statutory suppression remedy requiring the exclusion of wire or oral evidence when: (1) the information was unlawfully intercepted; (2) the order authorizing approval is facially insufficient; or (3) the interception was not in compliance with the authorization order.<sup>107</sup>

## 2. The Electronic Communications Privacy Act of 1986

In 1986, Congress significantly amended Title III with the Electronic Communications Privacy Act (“ECPA”).<sup>108</sup> Recognizing that legal protections had not kept pace with technology, Congress noted that Title III protections did not cover e-mail, cellular phones, pagers, and transmitters for radio surveillance.<sup>109</sup> The ECPA therefore extended some Title III

---

101. 18 U.S.C. § 2518(3)(a).

102. 18 U.S.C. § 2518(3)(b).

103. 18 U.S.C. § 2518(3)(c).

104. 18 U.S.C. § 2518(3)(d).

105. 18 U.S.C. § 2518(6). The issuing judge may review the reports to determine whether the progress is being made toward achievement of the authorized objective. The purpose of this section is to insure that extension of the order is not automatically granted without justification. *See* S. REP. NO. 90-1097, at 103-04 (1968).

106. *See* 18 U.S.C. § 2518(8)(d). The section provides in part, that the judge shall serve: persons named in the order . . . and such other parties to intercepted communications as the judge may determine in his discretion . . . an inventory which shall include notice of—(1) the fact of the entry of the order or the application; (2) the date of the entry and the period of the authorized, approved or disapproved interception, or the denial of the application; and (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

*Id.* Coverage for electronic communications was added in the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 1367, 2521, 2701-2711, 3117, 3121-3127.

107. 18 U.S.C. § 2518(10)(a). *See also* WHITEBREAD & SLOBOGIN, *supra* note 73, at 344 (noting that Title III exclusionary rules have are independent of the constitutional suppression remedy).

108. The ECPA is codified in various sections of 18 U.S.C. including §§ 1367, 2521, 2701-2711, 3121-3127. *See* Dempsey, *supra* note 89, at 73.

109. *See* H.R. REP. NO. 99-647, at 18 (1986).

protections to “wireless voice communications and electronic communications of a non-voice nature, such as e-mail or other computer-to-computer transmissions.”<sup>110</sup> Congress hoped to encourage the use of new technologies by protecting their use while creating procedures to support the legitimate needs of law enforcement.<sup>111</sup>

Currently, the ECPA requires a court order for the real-time interception of electronic messages<sup>112</sup> and a warrant for files stored by a service provider for fewer than 180 days.<sup>113</sup> Congress provided protection for e-mail stored fewer than six months because it recognized that the service provider often copies and retains e-mail messages for a short period of time in order to maintain its system.<sup>114</sup> To the extent that the ISP possesses this information, the amendments to Title III provide protection that the Fourth Amendment does not because, generally, there is no expectation of privacy in information surrendered to a third party.<sup>115</sup> In the legislative history of the ECPA, however, Congress recognized that e-mail content differs from telephone records, which compile numbers dialed from a telephone line, or bank account records because the ISP itself does not prepare or compile the content of an e-mail message. Thus, customers’ e-mail messages should be afforded greater protection because they are analogous to “items stored under [their] control, in a safety deposit box.”<sup>116</sup>

Despite the recognition that e-mail suggests an expectation of privacy, Congress drafted the ECPA so that the warrant required to acquire

---

110. Dempsey, *supra* note 89, at 73 (citing provision in the Electronic Communications Privacy Act, 18 U.S.C. § 2516(3) (1996)).

111. See H.R. REP. NO. 99-647, at 19 (1986).

112. See 18 U.S.C. § 2516(1).

113. See 18 U.S.C. § 2703(a).

114. See H.R. REP. NO. 99-647, at 22 (1986). Service providers copy e-mail messages in the case of system failure, but these messages are electronically generated and are not “normally accessed” by the provider. *Id.* at 22 n.34. There is no expectation of privacy in records kept by a third party, such as copies of checks and transactional records compiled by a bank. The rationale for this is that those who surrender information to a third party take a risk that the information will be provided to government officials. See Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III’s Statutory Exclusionary Rule and Expressly Reject a “Good Faith” Exception*, 34 HARV. J. ON LEGIS. 393, 404 (1997).

115. See WHITEBREAD & SLOBOGIN, *supra* note 73, at 331. See also *United States v. Miller*, 425 U.S. 435, 443 (1976). The Court in *Miller* held that the defendant had no Fourth Amendment privacy interest in banking records maintained by the bank because they are the property of the institution. Part of the rationale is that the person assumes the risk that information will be given to government authorities when they communicate information to third parties. See *id.* at 443 (citing *United States v. White*, 401 U.S. 745, 751–52 (1970)). Congress subsequently reversed the effect of the *Miller* decision by enacting the Right to Financial Privacy Act, 12 U.S.C. §§ 3401, et. seq. See H.R. REP. NO. 99-647, at 23 n.40 (1986). See also Leib, *supra* note 117, at 404.

116. H.R. REP. NO. 99-647, at 23 n.41 (1986).

electronic communication in storage for fewer than 180 days should be one issued under the Federal Rules of Criminal Procedure, or an equivalent state warrant, rather than a Title III warrant.<sup>117</sup> Such warrants provide less protection to suspects. First, they do not include a reporting requirement—allowing the judge to mandate that government agents report back information about their search.<sup>118</sup> This system of judicial oversight is an important method for monitoring government eavesdropping efforts.<sup>119</sup> Also, unlike Title III, the ECPA does not require that government agents compile annual reports of intercepted electronic communication. Title III yearly wiretap reports including the following information: the average length of the wiretaps; the number of persons and conversations intercepted per tap; and the number of arrests, trials, and convictions that have resulted from wiretaps.<sup>120</sup> Without similar reports on the acquisition of stored electronic data, it is impossible for the government and the public to monitor seizures of this kind.<sup>121</sup> Further, unlike Title III, the statute does not require the agent to conduct the search so as to minimize the acquisition of irrelevant data,<sup>122</sup> nor is there an exhaustion requirement.<sup>123</sup>

The standard for retrieving electronic communications in storage for longer than 180 days (older e-mail) is much more lenient than for e-mails acquired while in transit or during the statutory period. The older e-mail may be acquired in one of three ways: (1) through a federal or state warrant, which does not require prior notice to the suspect;<sup>124</sup> (2) through administrative or grand jury subpoena authorized by state or federal law—provided the suspect obtains advance notice;<sup>125</sup> or (3) through a court order, assuming specific facts are articulated to show reasonable grounds

---

117. See 18 U.S.C. § 2703(a).

118. See *supra* notes 94–100 and accompanying text.

119. See 18 U.S.C. § 2701(a). See also WHITEBREAD & SLOBOGIN, *supra* note 73, at 339 n.32 (discussing the importance of periodic court reports to limit the interception of irrelevant conversations).

120. See 18 U.S.C. § 2519(1), (2). In April of each year, the Director of the Administrative Office of the United States Courts releases the report to the United States Congress. 18 U.S.C. § 2519(3). See also *ECPA 2000 Hearings*, *supra* note 34, at 53 (statement of James X. Dempsey, Center for Democracy and Technology, advocating the mandate of government reporting on the seizure of stored electronic mail).

121. See *ECPA 2000 Hearings*, *supra* note 34, at 53 (statement of James X. Dempsey, Center for Democracy and Technology).

122. See 18 U.S.C. § 2518(5).

123. See 18 U.S.C. § 2518(1)(c). See also *supra* note 96 and accompanying text.

124. See 18 U.S.C. § 2703(a)–(b)(1)(A); PERRITT, *supra* note 28, at 905.

125. See 18 U.S.C. § 2703(b)(1)(B)(i), H.R. REP. NO. 99-647 at 71. See also PERRITT, *supra* note 28, at 905 (discussing the standard for acquiring e-mail in storage for over 180 days).

exist to believe the records are relevant to an ongoing investigation.<sup>126</sup> With a court order, notice to the subscriber may be delayed for up to ninety days if the court has reason to believe that notice will jeopardize the investigation or produce adverse consequences.<sup>127</sup> These exigencies include endangering the physical safety of individuals, flight from prosecution, tampering with evidence, intimidation of witnesses, or “jeopardizing an investigation or unduly delaying trial.”<sup>128</sup>

### 3. Pen Register or Trap and Trace Searches Under the ECPA

Even more relevant to Carnivore is the law guiding pen register or trap and trace searches because the system is currently being used as a pen register or trap and trace device (pen register search).<sup>129</sup> Pen registers and trap and trace devices record the telephone number dialed or received by a particular line.<sup>130</sup> In *Smith v. Maryland*, the Supreme Court held that there is no constitutionally protected privacy interest in the telephone numbers one dials, and thus, the use of pen registers to generate such records does not constitute a Fourth Amendment search.<sup>131</sup> Applying the *Katz* standard, the *Smith* Court held that no reasonable expectation of privacy in such information exists because telephone users know that the telephone company generates records for billing and troubleshooting.<sup>132</sup>

Interpreting Title III, the Court in *United States v. New York Telephone* emphasized that the low expectation of privacy partly depends on the fact that the information collected is limited only to the numbers dialed on a particular telephone.<sup>133</sup> Pen registers do not intercept communications because “[n]either the purport of any communication

---

126. See *id.*, 18 U.S.C. §§ 2703(b)(2)(C)(ii), 2703(d). See also PERRITT, *supra* note 28, at 609.

127. See 18 U.S.C. § 2705(a)(1)(A). See also PERRITT, *supra* note 28, at 609.

128. 18 U.S.C. § 2705(a)(B)(2). See also PERRITT, *supra* note 28, at 609–10.

129. See *ECPA 2000 Hearings*, *supra* note 34, at 37 (statement of Donald M. Kerr, Assistant Director, Federal Bureau of Investigations). Currently, there is no way to properly monitor the use of pen register and trap and trace devices as there is no national reporting requirement. Besides Justice Department reports, there are no statistics for numerous federal, state law enforcement applications. See *House Carnivore Hearings*, *supra* note 5, at 63 (statement of Alan Davidson, Staff Counsel, Center for Democracy and Technology).

130. See *supra* notes 17–18 and accompanying text. See also Center for Democracy and Technology, *CDT's Analysis of S. 2029: Amending Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections*, at <http://wzww.cdt.org/security/000404amending.html> (last visited Feb. 15, 2001) [hereinafter *CDT*].

131. *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

132. See *id.*

133. See 434 U.S. 159, 167 (1977). See also *CDT*, *supra* note 130, at 2 (discussing the information appropriate for a pen register and trap and trace search).

between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed.”<sup>134</sup>

Under the ECPA, an attorney for the government, a law enforcement officer, or an investigative officer may file an order for a pen register search.<sup>135</sup> The showing required for the government to conduct a pen register search—similar to obtaining an e-mail fewer than six months old—requires only that the information sought is relevant to an ongoing investigation.<sup>136</sup> The pen register order should contain the name of the person to whom the telephone line is leased, the identity of the person subject to the investigation, and the physical location to which the device will be attached.<sup>137</sup> The applicant should also submit a statement indicating the probable offense to which the information likely relates.<sup>138</sup>

Unlike wiretaps, the ECPA does not require national reporting on the use of pen register searches.<sup>139</sup> In addition, the standard of proof for obtaining a pen register search is similar to a subpoena, and thus, is significantly less stringent than probable cause.<sup>140</sup> The statutory language providing that “the court *shall* enter an *ex parte* order” for pen register searches upon a showing of relevance, illustrates that the court need not make any factual determination prior to granting the request.<sup>141</sup> In fact, in testimony before the House Subcommittee on the Constitution, Alan B. Davidson, Staff Counsel for the Center for Democracy and Technology, stated that judges have little discretion in granting these orders; meanwhile, investigators have broad leeway to seek orders without providing “any indication that the targets have been involved in criminal wrongdoing themselves.”<sup>142</sup> Many privacy advocates have likened the standard for pen register or trap and trace orders to a “rubber stamp.”<sup>143</sup>

---

134. *New York Tel. Co.*, 434 U.S. at 167. The Ninth Circuit Court of Appeals found that pen registers are not within the scope of Title III “[b]ecause pen registers do not intercept the contents of communications.” *United States v. Kail*, 612 F.2d 443, 448 (9th Cir. 1979).

135. *See* 18 U.S.C. § 3123(a).

136. *Id.*

137. 18 U.S.C. § 3123(b)(1)(A)–(C).

138. 18 U.S.C. § 3123(b)(1)(D).

139. *See House Carnivore Hearings*, *supra* note 5, at 63 (statement of Alan B. Davidson).

140. *See id.*

141. 18 U.S.C. § 3123(a) (emphasis added).

142. *House Carnivore Hearings*, *supra* note 5, at 63 (statement of Alan B. Davidson).

143. *CDT*, *supra* note 130, at 4; *Electronic Surveillance: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (prepared statement of Senator Patrick Leahy), available at 2000 WL 1268432 [hereinafter, *Leahy Senate Statement*].

#### IV. ELECTRONIC COMMUNICATION REQUIRES GREATER PROTECTION

##### A. WIRE AND ORAL COMMUNICATION ARE GRANTED GREATER PROTECTION

A significant problem with Carnivore is that electronic communication—the target of its search—is granted less protection than wire communication under the ECPA. This disparity is puzzling given that, in 1968, Congress sought to protect the privacy of wire and oral communications by creating elaborate rules covering government surveillance through wiretaps.<sup>144</sup> Some of the protections afforded Title III wiretaps include requiring high level Justice Department authorization, limiting wiretaps to enumerated offenses, requiring a warrant for wire communication both in storage and in transit, and providing the remedy of statutory suppression for illegal searches.<sup>145</sup> Recall that Title III mandates the exclusion of evidence gained through gross violations of the statutory scheme.<sup>146</sup> The ECPA does not, however, grant such protections for stored electronic communication. Many believe that Justice Department opposition to granting equivalent protections to new technologies influenced the final version of the bill.<sup>147</sup> During the Reagan administration, only bills supported by the Justice Department had a chance of being approved.<sup>148</sup> Testifying on the ECPA, James Knapp, Deputy Assistant Attorney General, stated that “interception of electronic mail should include some but not all of the procedural requirements of Title III.”<sup>149</sup> Part of the rationale for this position is that electronic mail should be treated the same as a first class mail, and thus, the contents should be obtainable upon a traditional search warrant that a magistrate judge can issue.<sup>150</sup> This reasoning, however, does not explain why the committee ultimately assigned different levels of protection to e-mail based on how

---

144. S. REP. NO. 90-1097, at 22 (1968).

145. See discussion *supra* Part III.B.1.

146. See 18 U.S.C. § 1218(10)(a).

147. See Leib, *supra* note 117, at 409. The legislative history of the ECPA offers no rationale for the differential treatment between electronic and wire communications, “merely stating that the position was adopted as a result of discussions with the Justice Department.” WHITEBREAD & SLOBOGIN, *supra* note 73, at 345 (internal quotes omitted).

148. See Robert W. Kastenmeier, Deborah Levy & David Beier, *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 733–34 (1989).

149. *The Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. On Courts, Civil Liberties, and the Administration of Justice, House Comm. on the Judiciary*, 99th Cong. 230 (1989).

150. See *id.* at 234.

long it is stored. Further, the legislative history of the ECPA does not provide an alternate, coherent rationale for the differential treatment of wire and electronic information; it “merely stat[es] that the position was adopted as a result of discussion with the Justice Department.”<sup>151</sup>

#### B. STORED ELECTRONIC COMMUNICATION IS EASILY OBTAINABLE

Currently, “any attorney for the Government” can authorize an application to intercept electronic communications when the evidence sought relates to “any Federal felony.”<sup>152</sup> In addition, it is far easier to obtain stored electronic communication than to obtain stored wire communication, such as voicemail. Voicemail falls within the definition of “wire communication” and thus is only obtainable upon a Title III intercept order.<sup>153</sup> The retrieval of stored electronic communication, such as e-mail, is regulated by the ECPA.<sup>154</sup> In order to obtain e-mail stored with an ISP for 180 days or fewer, the officer need not obtain a Title III warrant. Rather, law enforcement must only obtain a less restrictive warrant issued under the Federal Rules of Criminal Procedure or equivalent State law.<sup>155</sup>

Electronic communication that has been stored with an ISP for more than 180 days (older e-mail) can be obtained by warrant, subpoena, or a court order based on “specific and articulable facts showing . . . reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation.”<sup>156</sup> This relevance standard is far less stringent than a warrant based on probable cause, and thus creates a dichotomy of protection for e-mail based on the length of time it has been stored with a service provider.<sup>157</sup> In the legislative history of the ECPA, Congress noted that almost every service provider creates backup files of all e-mail messages on its network for system maintenance and integrity purposes—even if the customer erased or deleted the original message. The report states that “[a] person who subscribes to an electronic mail

---

151. See WHITEBREAD & SLOBOGIN, *supra* note 73, at 345.

152. 18 U.S.C. § 2516(3). See also *House Carnivore Hearings*, *supra* note 5, at 52 (prepared statement of Barry Steinhardt, Associate Director, American Civil Liberties Union).

153. See 18 U.S.C. §§ 2510(1), 2518. See also Leib, *supra* note 117, at 407 n.101 (discussing the need to bring electronic communication within the Title III framework to afford sufficient privacy protection). Under Title III, Section 2703(a) provides that the definition of wire communication includes “any electronic storage of such communication,” thus the retrieval of voicemail is not subject to the provisions dealing with the storage of electronic communication. See 18 U.S.C. § 2703(a).

154. See 18 U.S.C. §§ 2701–2711.

155. See 18 U.S.C. § 2703(a). See also discussion *supra* Part III.

156. See 18 U.S.C. § 2703(d).

157. See *House Carnivore Hearings*, *supra* note 5, at 52 (prepared statement of Barry Steinhardt, Associate Director, American Civil Liberties Union).

service may not realize it, but that service likely maintains a record of all system transactions for a period of time, usually six months.”<sup>158</sup> Thus, Congress set the warrant requirement for this amount of time.<sup>159</sup>

The ECPA house report states that Congress intended to provide greater statutory privacy protection to stored e-mail than that afforded records maintained by a third party, which have no constitutional privacy protection.<sup>160</sup> The report suggests that a customer should be afforded more protection for the backup files that the ISP automatically saves and that are potentially retrievable. It seemed important to the committee that the protected customer files include those that are “maintained on [customers’] behalf for the purpose of providing remote computing services.”<sup>161</sup> Files that are saved by the customer for longer than six months are more easily retrieved by the government. The committee viewed records stored with a remote server beyond 180 days as “closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.”<sup>162</sup> Congress made this distinction between older and newer e-mail because—at least with many of the newer messages—the ISP chose to make a duplicate copy. In terms of older e-mail, the report suggests that the customer assumed the risk that it would be discovered when they choose to save the message remotely. Therefore, a lower level of protection is granted.<sup>163</sup>

The underlying assumption is that older e-mail is analogous to transactional records held by a third party. The report discusses *United States v. Miller*, which held that individuals do not have an expectation of privacy with respect to bank records maintained by a third party.<sup>164</sup> *Miller*, decided in 1976, involved government access to checks, deposit slips, and other banking records that were deemed public “negotiable instruments” used in commercial transactions.<sup>165</sup> The broad implication of this decision was that there was no expectation of privacy in paper records held by a third party.<sup>166</sup> Thus, three years later, the Supreme Court held in *Smith v. Maryland* that using a pen register search to collect a record of the numbers dialed on a suspect’s telephone did not implicate that individual’s privacy

---

158. H.R. REP NO. 99-647, at 72 (1986).

159. *Id.*

160. *Id.*

161. *Id.* at 73.

162. *Id.* at 68.

163. *See id.*

164. 425 U.S. 435 (1976).

165. *Id.* at 442.

166. *See PERRITT, supra* note 28, at 895.

rights.<sup>167</sup> The ECPA responded to *Smith* by outlining the requirements to obtain a court order for a pen register or trap and trace search.<sup>168</sup> As stated previously, however, this standard is basically a “rubber stamp” relevance standard that does not require the issuing judge to make independent factual findings on the contents of the order.<sup>169</sup> Currently, electronic communications—such as the research projects or personal communications stored on a university server, or employees’ records stored on an employer’s server—can be acquired under the relevance standard if they are stored for longer than six months.<sup>170</sup>

This standard, however, is improper because electronic communications, such as e-mail, research projects, or business records, are distinguishable from mere transactional records held by a third party. Electronic mail files stored on a remote server, unlike banking records, are neither compiled by a third party, nor are they public information. Communications such as e-mail or instant messages—used to communicate with family and friends—are distinguishable based on the expectation of privacy that the public holds towards this type of information.<sup>171</sup> *United States v. New York Telephone Company* is instructive, as it emphasized that no expectation of privacy in pen register searches exists because they reveal neither the individuals making the call, nor the content of the communications.<sup>172</sup> This rationale does not apply to the electronic context, however, because e-mail addresses often do reveal the individuals involved in the communication, whether the address is a derivation of the individual’s name, or the full name appears in parenthesis after the address. Further, as the ITRI tests have shown, pen register searches reveal the length of the message by replacing the context of a message with X’s.<sup>173</sup> The legal standard should recognize that electronic files that convey content or the identity of those in communication with one another should implicate an expectation of privacy—regardless of the file’s age.

---

167. 442 U.S. 735 (1979). See also *ECPA 2000 Hearings*, *supra* note 34, at 87 (testimony of James X. Dempsey, Center for Democracy and Technology).

168. See H.R. REP. NO. 99-647, at 25, 72.

169. See discussion *supra* Part III.B.3.

170. See generally, Leib, *supra* note 117, at 405–06 (contrasting the relevance standard for seizing e-mail in storage for over 180 days with the standard for obtaining mail delivered by the United States Postal Service).

171. See generally *United States v. Miller*, 425 U.S.435, 435 (1976) (holding that the disclosure of public instruments such as bank records does not violate the Fourth Amendment).

172. 434 U.S. 159, 167 (1977).

173. See *supra* notes 30–32 and accompanying text.

Perhaps another rationale for why e-mail stored on a remote server is afforded less protection than voicemail is the assumption that no expectation of privacy exists in a message that can be retrieved and read at will by ISP employees. It should be noted, however, that ISP employees are not supposed to engage in such activities. In fact, employees at AOL must sign a confidentiality agreement that they will not read customer communications such as e-mail, even if they may manipulate it to maintain the server.<sup>174</sup> Additionally, Title III recognizes that it is not unlawful for service providers to intercept or disclose the contents of wire or electronic communication in the normal course of employment while engaging in activities that are necessary to render service to the customer.<sup>175</sup> The statute does not provide that these employees have the right to read customer messages at will. In fact, there is a recognition that the exception to service providers is solely for the purpose of providing computer processing service.<sup>176</sup> What this suggests is that customers should have an expectation of privacy in their electronic communication, even if saved on a remote server. Additionally, the agreement to save files with an ISP does not equate to an agreement that the provider may surrender the files to the government without meeting probable cause. Information that individuals are willing to release to private parties often differs from that which they are willing to share with the government.

The privacy concerns surrounding “new” e-mails should not change just because the message is stored for a longer period of time. In fact, it is intuitive that e-mails stored for a long period of time are those which people consider most important, and perhaps, the most private. E-mail is more analogous to voice communication than it is to postal mail and should be recoverable under the same standard. In e-mail, people tend to communicate in a spontaneous fashion, as in telephone conversations;<sup>177</sup> messages are sent back and forth with instantaneous turnaround. Most individuals that use the telephone probably do not expect that their conversations are being monitored, and the same feeling is likely to apply to personal e-mail accounts.<sup>178</sup> E-mail likely replaces as much oral

---

174. Telephone Interview with B. Jingle, AOL Customer Care Consultant (Mar. 12, 2001).

175. 18 U.S.C. § 2511(2)(a)(i).

176. See 18 U.S.C. § 2703(b)(2)(A)–(B).

177. See *House Carnivore Hearings*, *supra* note 5, at 52 (prepared statement of Barry Steinhardt, Associate Director, American Civil Liberties Union).

178. With the existence of workplace surveillance, however, the expectation of privacy over an employer’s server is probably lower than that which applies to a home computer. See generally Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1481–82 (2000) (discussing the availability of relatively inexpensive workplace monitoring devices).

communication as postal mail because of its ease and the casualness by which it is sent.<sup>179</sup> The internet is often preferred when communicating with others across long distances because it is a relatively inexpensive alternative to the telephone. Given these considerations, the distinction between electronic mail and voice communications appears to collapse.

Additionally, if the foundation of the Fourth Amendment is a reasonable expectation of privacy, then electronic communication should be protected. In the current regime, there is a disconnection between what communication the government believes should carry a reasonable expectation of privacy and what the public actually believes is reasonable.<sup>180</sup> For example, individuals using an ISP's services may not understand that the e-mail they are saving is actually saved on the server—not their personal computer.<sup>181</sup> Based on this misunderstanding, the public probably has a high expectation of privacy regarding this type of information. Congress, therefore, should be cautious in developing legal distinctions based on knowledge that the majority of the public does not share. In *Smith v. Maryland*, Justices Marshall's and Brennan's dissent argued that a reasonable expectation of privacy should not be based on the assumption that the public understands the "esoteric functions" of corporate billing or recordkeeping.<sup>182</sup> To make the Fourth Amendment workable in reality, a reasonable expectation of privacy cannot depend on technical distinctions that the average person cannot make.<sup>183</sup> For example, users of e-mail are unlikely to believe that an unread message deserves more protection than one that has been read and saved.<sup>184</sup>

The ECPA report is puzzling because it is difficult to reconcile its ultimate conclusion that "older" electronic communications may be acquired on a low relevance standard with its recognition of a privacy expectation in transactional records held by third parties. The report noted that Congress effectively overruled *Miller* by passing the Right to Financial Privacy Act in 1978, which required "federal government agencies to use legal process to obtain bank records and allow the bank customer to seek to

---

179. See Megan Connor Bertron, *Home is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 184–85 (1996).

180. See *ECPA 2000 Hearings*, *supra* note 34, at 82 (testimony of Jerrold Nadler).

181. See *id.* at 82 (testimony of Robert Corn-Revere, Attorney, Hogan & Hatson). Many ISP's have a system that allows users to save messages on their own computers. *Id.*

182. 442 U.S. 735, 749 n.1 (1979) (Marshall, J. and Brennan, J., dissenting).

183. See *ECPA 2000 Hearings*, *supra* note 34, at 45 (prepared statement of Representative Jerrold Nadler, New York).

184. See *id.*

quash such process.”<sup>185</sup> Thus, the committee reasonably could have concluded that a standard greater than relevance should apply to older e-mail. At the very least, the committee should have provided a means by which the aggrieved individual could exclude illegally obtained electronic information. Perhaps as suggested earlier, however, the committee caved under pressure from the Justice Department.<sup>186</sup>

### C. STATUTORY SUPPRESSION DOES NOT APPLY TO ELECTRONIC COMMUNICATION

Currently if government agents were to acquire electronic communication in violation of Title III or the ECPA, the statutory suppression remedy available to wire communications would not apply. In drafting the ECPA, Congress did not amend the exclusionary rule in Title III to cover electronic communication.<sup>187</sup> This exclusionary rule provides for the suppression of oral wiretap evidence where the interception violates any “central” provision in Title III—even if the suppression is not required on Fourth Amendment grounds.<sup>188</sup> In amendments to the ECPA in 1986, Congress made it clear that electronic communications are afforded only “judicial remedies and sanctions for nonconstitutional violations of this chapter.”<sup>189</sup> Again, the Justice Department appears to have influenced the direction of statutory protection.<sup>190</sup>

The suppression remedy is necessary because it provides a clear incentive for law enforcement to comply with the provisions of Title III.<sup>191</sup>

---

185. H.R. REP. NO. 99-647, at 73 (1986). *See also* 12 U.S.C. § 3405(A)(3) (1994) (providing that customers may seek to quash subpoena for bank records).

186. *See* WHITEBREAD & SLOBOGIN, *supra* note 73, at 345.

187. 18 U.S.C. § 2515 (1994).

188. *See* 18 U.S.C. § 2515. The section provides:

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

*Id.* *See also* Leib, *supra* note 117, at 408 (discussing fact that Title III statutory suppression is purely statutory and not constitutionally required); WHITEBREAD & SLOBOGIN, *supra* note 73, at 344–45 (finding that statutory suppression surpasses constitutional protections, as it applies to private interceptions and to all hearings).

189. 18 U.S.C. § 2518(10)(c). *See also* Leib, *supra* note 117, at 408 n.104 and accompanying text (discussing the fact that Congress did not intend to provide electronic communications with the protection of Title III suppression).

190. *See* Leib, *supra* note 117, at 411.

191. *See generally* S. REP. NO. 90-1097, at 68–69 (1968) (discussing the development of the suppression of evidence as a remedy for unconstitutional government surveillance).

Congress viewed this sanction as essential to curtail unconstitutional interceptions of non-electronic communications.<sup>192</sup> Given the intrusiveness of government surveillance, the suppression remedy should apply to both real-time interceptions and the acquisition of electronic communication in storage, in order to sufficiently protect the privacy of the information.<sup>193</sup> Some from the Justice Department argue that a suppression remedy already exists for government misconduct that rises to the level of a constitutional violation.<sup>194</sup> They further argue that extending the suppression provision to stored electronic communication would interfere with the “search for truth” in criminal trials and confer an “unwarranted windfall on criminals.”<sup>195</sup> Despite these misgivings, the Justice Department has supported an amendment that would afford the suppression remedy to real-time interceptions of electronic communication in an effort to “harmoniz[e]” wiretap law for both voice and electronic communication.<sup>196</sup>

The distinction that the Justice Department makes between real-time and stored electronic communication is based on the *Miller* standard that information “held in storage with a third party is not constitutionally protected.”<sup>197</sup> Given the *Miller* precedent, the government may argue that a stored e-mail is analogous to a business record maintained by a third party, and thus, is not afforded Fourth Amendment protections.<sup>198</sup>

This argument is flawed because the public believes their e-mail is confidential and that ISP employees do not routinely read customers’ messages.<sup>199</sup> With public banking records, such as individual checking account statements, it is typically understood that bank employees must compile, and account for, all transactions. The bank thereby facilitates and participates in the transaction. With e-mail, however, ISP employees are not reading the e-mail for its content, but rather, are monitoring the format of the e-mail, to ensure that the server is operating properly.<sup>200</sup> The ISP is a carrier of the information, much like Pacific Bell is a carrier of our telephone service. In fact, electronic information saved with an ISP is

---

192. See Leib, *supra* note 117, at 418.

193. See *id.* See also CDT, *supra* note 130.

194. See *ECPA 2000 Hearings*, *supra* note 34, at 20 (testimony of Kevin DiGregory, Deputy Associate Attorney General, Department of Justice).

195. *Id.*

196. *Id.*

197. *ECPA 2000 Hearings*, *supra* note 34, at 51 (testimony of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

198. See *id.* at 54.

199. See Telephone Interview with B. Jingle, *supra* note 174.

200. *Id.*

more analogous to items stored in a safety deposit box than to checking account records stored at a bank. Most bank customers would agree that they have an expectation of privacy over their safety deposit box because bank employees should not be searching through their valuables. The same logic should apply to e-mail saved with an ISP.<sup>201</sup> Therefore, it makes little sense that the real-time interception of e-mail should be protected by the suppression remedy, while opened e-mail saved on the server (that may be just one second older) is not. The Justice Department, however, has argued just that.<sup>202</sup> Certainly the distinction does not lie in the difference between the content of such messages. It is reasonable to believe that an individual has a similar expectation of privacy for e-mails that are currently in-transit and those they have just read. When pressed to provide the policy rationale behind this distinction, Deputy Associate Attorney General Kevin DiGregory could only offer that this was “a policy determination that was made with respect to wire and oral communications by the Congress when it imposed the strict statutory exclusionary rule.”<sup>203</sup>

The suppression remedy provided by Title III is a necessary protection against unlawful electronic surveillance because its scope exceeds Fourth Amendment protection. Title III applies to both private and government interceptions, and to all hearings—not just criminal trials as under the Fourth Amendment.<sup>204</sup> In addition, evidence may be excluded under Title III when proper procedures are not followed. Under the Fourth Amendment, the exclusionary rule applies only to situations where a search violates an individual’s reasonable expectation of privacy. For example, in *United States v. Giordano*, an ECPA case, evidence was excluded because someone without the proper legal authority approved the wiretap order: the Executive Assistant to the Attorney General signed the Attorney General’s initials.<sup>205</sup> Since there was probable cause, no Fourth Amendment violation occurred; hence, only the Title III suppression remedy provided protection for the defendant.<sup>206</sup> If this scenario occurred today with e-mail, the court could not suppress the evidence because *Giordano* involved wire

---

201. In fact, the beginning of the ECPA report, finding no case law on point, maintains that e-mail could be distinguished from bank records as they are “analogous to items stored, under customer’s control, in a safety deposit box.” See H.R. REP. NO. 99-647, at 23 n.41 (1986).

202. See *ECPA 2000 Hearings*, *supra* note 34, at 58–59 (testimony of Gregory T. Nojeim, Legislative Counsel, American Civil Liberties Union).

203. *ECPA 2000 Hearings*, *supra* note 34, at 48 (discussion between Jerrold Nadler and Kevin DiGregory on the Congressional rationale for the distinction between e-mail intercepted in real-time and e-mail in storage).

204. See *WHITEBREAD & SLOBOGIN*, *supra* note 73, at 344.

205. See 416 U.S. 505 (1974).

206. See Leib, *supra* note 117, at 416.

communication. This distinction between wire and electronic communication appears formalistic and does not properly recognize the private nature of certain electronic interactions, such as online banking, shopping, and prescription drug purchasing.<sup>207</sup>

Further, there remains a constitutional question as to whether there is an expectation of privacy in e-mail, or whether it is a transactional record in the hands of a third party. Understanding the importance of electronic communications to citizens, Congress should provide extra protection to e-mail, rather than waiting for courts to hear the issue. Many individuals and businesses utilize the internet to transact business, receive news and information, and communicate with friends and family members.<sup>208</sup> Given the pervasiveness of personal transactions over the internet, Congress should ensure that suppression of electronic communication exists as a remedy for the most serious procedural violations. Procedural safeguards provide a much-needed additional check on the government. The comprehensive procedures in Title III, for example, provide various levels of protection by limiting who may seek a warrant, for what cause, and by providing judicial oversight.<sup>209</sup> Mandating the exclusion of evidence provided in violation of these procedures creates an incentive to follow proper protocol.

Because the Supreme Court has held that the suppression remedy shall not apply to minor technical violations, expanding the suppression remedy will not significantly harm law enforcement interests.<sup>210</sup> In *Giordano*, the Supreme Court held that suppression is warranted only where law enforcement officers have violated the central statutory requirements of Title III.<sup>211</sup> Where a violation of Title III is constitutional in nature, the Fourth Amendment good faith exception applies—holding that exclusion is not necessary where police are “‘reasonably’ unaware they are violating

---

207. *See id.*

208. *See Electronic Surveillance: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (prepared statement of Senator Orin G. Hatch), available at 2000 WL 1268432 [hereinafter *Hatch Senate Statement*].

209. *See* discussion *supra* Part III.B.1.

210. *See* Center for Democracy and Technology, *Summary of H.R. 5018, the Electronic Communications Privacy Act of 2000*, at <http://www.cdt.org/security/000927hr5018.shtml> (last visited Nov. 12, 2000) [hereinafter *CDT Summary*].

211. *See Giordano*, 416 U.S. at 527. *See also CDT Summary, supra* note 210, at 5 (asserting that statutory exclusionary rule is very weak, as it applies only to a few egregious violations); WHITEBREAD & SLOBOGIN, *supra* note 73, at 345 (acknowledging that statutory exclusion applies only when a government officer violates a provision intended to play a central role in the Title III scheme).

Fourth Amendment principles.”<sup>212</sup> Additionally, the Title III good faith exception is analogous to and has supported the use of evidence in cases where probable cause was lacking<sup>213</sup> or where a judge failed to sign a wiretap order.<sup>214</sup> A leading treatise on electronic surveillance has asserted that the exclusionary rule is somewhat weak, as there are “relatively few violations which will lead to the ultimate and absolute sanction of complete suppression of all surveillance evidence.”<sup>215</sup> In fact, many instances exist where the government has failed to abide by the procedural protections of Title III without affecting the admissibility of “eavesdropping evidence.”<sup>216</sup> It seems reasonable to conclude, therefore, that the extension of the suppression remedy to electronic communication in transit and in storage will not confer a “windfall” on criminals using the internet. To the contrary, case law suggests that the exclusionary rule would apply to only the most egregious procedural failures.

#### V. IS CARNIVORE A DESIRABLE SEARCH TOOL?

The Carnivore system has broad capabilities. It can gather the contents of almost any traffic on the internet connection to which it is attached. Although its filters help to minimize unlawful interception of communications, Carnivore’s far-reaching capabilities alone make it much more intrusive than a traditional wiretap connected to a single phone line. Further, the program conducts a search by reading or filtering through all internet traffic that passes by, which is in essence an unconstitutional general search of individuals who are not subject to a court order. The FBI has asserted that this “filtering stage” is not a search, as it is the Carnivore program (a machine), and not federal agents, that is processing information of the innocent public.<sup>217</sup> The FBI asserts that, by the time agents attain a copy of the collected data, Carnivore has provided only that information authorized by the court order.<sup>218</sup> This position, however, is indefensible, as

---

212. WHITEBREAD & SLOBOGIN, *supra* note 73, at 26. See also *CDT Summary*, *supra* note 210, at 5; *United States v. Leon*, 468 U.S. 897 (1984) (establishing that a good faith belief in the validity of a search warrant creates an exception to the exclusionary rule).

213. See *United States v. Millan*, 817 F. Supp 1072, 1077–78 (S.D.N.Y. 1993). *Millan* found that wiretap evidence should only be suppressed where: (1) the issuing judge is not neutral or detached; (2) the agent was dishonest or reckless in preparing the affidavit supporting the wiretap order; or (3) the agent was not objectively reasonable in relying on the warrant. *Id.* at 1078.

214. See *United States v. Moore*, 41 F.3d 370 (8th Cir. 1994).

215. *CDT Summary*, *supra* note 210, (quoting JAMES G. CARR, *THE LAW OF ELECTRONIC SURVEILLANCE* at § 6.3 (1998)).

216. See *id.*

217. See *Kerr Senate Statement*, *supra* note 3.

218. See *id.*

the Supreme Court held in *Kyllo v. United States* that thermal imaging technology used to detect heat emanating from a suspect's home was a search within the Fourth Amendment.<sup>219</sup> There, as here, it was a machine, not government agents, that detected what was occurring within a suspect's home.<sup>220</sup> This leaves open the possibility that the operation of Carnivore may be unconstitutional regardless of its ability to potentially isolate a suspect's communication. Additionally, the Carnivore program's versatility is a troubling feature. With the push of a button, Carnivore can be configured to accommodate various searches—operating as either a full-content wiretap, or a pen register, or a trap and trace device.<sup>221</sup> To evaluate the constitutionality of both operations, this paper will examine each in turn.

#### A. CARNIVORE'S OPERATION AS A WIRETAP

When Carnivore is operated in full-collection mode—recording the content of a particular suspect's e-mail or internet browsing habits—the standard of a Title III warrant is appropriate. Currently, “[t]here is no dispute that the stringent legal requirements governing wiretaps apply to Carnivore when it is used to capture the content of e-mails or other computer transmissions.”<sup>222</sup> The definition of content for the purpose of a Title III warrant applies not only the text of e-mail messages, but also to the subject lines as well.<sup>223</sup> Under a full-content search, the high standard of probable cause and the protections of statutory suppression, judicial oversight, and yearly reporting are sufficient to protect privacy concerns.<sup>224</sup>

The significant question regarding a full-content search, however, is whether Carnivore—as asserted by the FBI—can actually zero in on the subject of the search.<sup>225</sup> This particularized targeting is essential because if Carnivore actually cannot filter for the suspect's addressing information alone, the program could conceivably collect the e-mail of innocent individuals who are not targets of the search. A traditional telephone wiretap can be limited to one telephone at a time, and usually, records help to pinpoint the household where the suspect resides. On the internet,

---

219. 121 S. Ct. 2038 (2001).

220. *See id.* at 2044–45.

221. *See Leahy Senate Statement, supra* note 143.

222. *See id.*

223. *See id.*

224. *See generally* S. REP. NO. 90-1097, at 48 (1968) (discussing Title III as the codification of the constitutional standards set out in *Katz v. United States*, 389 U.S. 347 (1967)).

225. *See Kerr Senate Statement, supra* note 3.

however, the tap is not limited to a single subscriber line, as Carnivore is installed on the ISP's data network and searches the data of all subscribers.<sup>226</sup> If Carnivore cannot adequately target the subject of its search, the program cannot meet the minimization requirement of Title III, which states that wiretaps must be conducted to limit the interception of communications not subject to the order.<sup>227</sup> According to the IITRI tests, the program does have this capability, and it effectively excludes all other traffic.<sup>228</sup> Assuming IITRI's conclusion is accurate, a Title III warrant is the appropriate standard because it requires the court to make a probable cause determination on the following: (1) whether the offense has been, or will be, committed; (2) whether the communications to be intercepted are relevant to the crime; (3) whether normal investigative procedures have been tried and have failed; and (4) whether the facilities subject to the search are connected with the offense or the person named.<sup>229</sup>

Even if Title III is the appropriate standard for a full-content search, the FBI should cease using Carnivore until the system's security issues are rectified.<sup>230</sup> Further, without amending the ECPA to provide appropriate statutory protection for electronic communications—such as statutory suppression and a warrant requirement for the acquisition of stored e-mail—Carnivore will consistently intrude upon areas where the public has a reasonable expectation of privacy.

#### B. CARNIVORE DOES NOT OPERATE AS A PEN REGISTER OR TRAP AND TRACE DEVICE

Carnivore should not be recognized as a pen register or trap and trace device because the program gathers far more data than is authorized under a pen register court order. The Supreme Court has held that the information compiled by pen registers or trap and trace devices is not protected by the Fourth Amendment because the public does not have a reasonable expectation of privacy in the telephone numbers they dial.<sup>231</sup> In another case, the Court emphasized that telephone records do not reveal the identities of the callers, whether the call was completed, or the content or

---

226. See *House Carnivore Hearings*, *supra* note 5, at 84 (statement of Robert Corn-Revere, Attorney, Hogan & Hartson).

227. See 18 U.S.C. § 2518(5).

228. See IITRI Report, *supra* note 2, at xii. However, the report acknowledges that the program does not eliminate all risks of unauthorized collection. See *id.*

229. See WHITEBREAD & SLOBOGIN, *supra* note 73, at 340.

230. See discussion *infra* Part VI.

231. *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

purpose of the communication.<sup>232</sup> Accordingly, the ECPA standard of approval for a court order authorizing such a search is low, and judges are provided no discretion in granting a search.<sup>233</sup>

Currently, law enforcement authorities use Carnivore to conduct pen register searches because they believe that the addresses found in the TO and FROM lines of an e-mail are the electronic equivalent of the numbers dialed on a telephone.<sup>234</sup> The addresses on the internet, however, reveal far more than the numbers dialed on a telephone, and thus, the law guiding pen register searches should not apply to Carnivore. As a basic matter, e-mail addresses often reveal the parties who are writing one other, and there is usually no question about whether the message was completed, as it is instantaneously sent to an internet mailbox.<sup>235</sup> While in a particular household or business there may be only one phone number that dials to the outside, individuals usually have their own e-mail addresses—meaning the government can likely identify the individuals who are in communication with one other.<sup>236</sup> Further, as noted above, an IITRI test search for a non-content e-mail address showed that Carnivore collects all information related to the e-mail message, thus showing the length of a communication.<sup>237</sup>

In addition, pen registers are used to gather the address or location of a target's web browsing activities.<sup>238</sup> The IITRI report states that a pen register search can be configured so as not to obtain the Uniform Resource Locator (URL)<sup>239</sup>—"an internet address which tells a browser where to find an internet resource, such as a web page."<sup>240</sup> The search does, however, collect the IP address that a target is browsing. An IP address functions like a URL, but is expressed in numbers.<sup>241</sup> In my own search for the Los

---

232. *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977).

233. *See CDT Summary*, *supra* note 210, at 2. *See also House Carnivore Hearings*, *supra* note 5, at 75 (prepared statement of Robert Corn-Revere, Attorney, Hogan & Hartson) (discussing the constitutional rationale for the minimal standard governing pen register and trap and trace orders).

234. *See Kerr Senate Statement*, *supra* note 3; *House Carnivore Hearings*, *supra* note 5, at 16 (statement of Kevin DiGregory, Deputy Associate Attorney General, Department of Justice).

235. *See ECPA 2000 Hearings*, *supra* note 34, at 64 (statement of Robert Corn-Revere, Attorney, Hogan & Hartson). Given the ease with which one can obtain an e-mail address, individuals will usually set up their own. Further, ISP's often require personal passwords to be used before logging into the system, ensuring that the "owner" of the address is the person logged on. *Id.*

236. *See CDT Summary*, *supra* note 210.

237. *See discussion supra* Part II.B.

238. *See IITRI Report*, *supra* note 2, at 3-22.

239. *Id.*

240. *See Interview with Samuel Choi*, *supra* note 13 (discussing the function of a URL and its relation to an IP address).

241. *See id.*

Angeles Philharmonic (“L.A. Phil”) website, I typed in the organization’s IP address: “http://209.196.151.22/” and was sent to the L.A. Phil home page, just as if I had typed the URL address: “http://www.laphil.org/.”

Having the IP address, law enforcement officers can gain specific information about a suspect’s web-browsing activities, including what files were viewed and whether items were purchased.<sup>242</sup> For example, if someone were browsing a book on the Amazon.com website, a specific IP address could lead an agent to the “shopping cart” page that functions as the equivalent of a receipt.<sup>243</sup> While digits dialed on a telephone are not deemed to be very revealing,<sup>244</sup> the content of one’s web-browsing activity—showing everything from recreational interests to professional transactions—is highly personal. To gain access to this type of information, the government should have to make a finding beyond the relevance standard currently used.<sup>245</sup>

## VI. RECOMMENDATIONS

Providing sufficient privacy protections for transactions over the internet is essential. Reports state that more than forty million Americans use the internet, which is gaining approximately 55,000 users per day.<sup>246</sup> More ideas are shared on the internet than any other medium. In this environment, fear of unrestricted electronic surveillance could have a chilling affect on communications and transactions in cyberspace.<sup>247</sup> A slow down in internet use would logically lead to a reduction in communications and commerce—which would ultimately affect the economy as a whole.<sup>248</sup> Furthermore, the government needs to show its ability to support new technologies by providing analogous statutory protections to technologies that already exist. Growth in new technologies could be stunted if the government does not properly recognize the privacy needs inherent in new mediums.<sup>249</sup> Finally, high social costs are associated

---

242. See *CDT*, *supra* note 130. See *Electronic Surveillance: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (prepared statement of James X. Dempsey, Center for Democracy and Technology), available at 2000 WL 1268432 [hereinafter *Dempsey Statement*]; see also *Leahy Senate Statement*, *supra* note 143 (discussing the potential that internet addressing information provides more detail about a subject than the telephone numbers they dial).

243. *Dempsey Statement*, *supra* note 242.

244. See *United States v. New York Telephone Co.*, 434 U.S. 159, 167 (1977).

245. See discussion *supra* Part III.B.

246. See *Hatch Senate Statement*, *supra* note 208.

247. See *Victor*, *supra* note 80, at 864.

248. See *id.*

249. See *Leib*, *supra* note 117, at 415.

with monitoring electronic communication. Surveys of workplace surveillance suggest that monitoring results in higher levels of depression, tension, and anxiety, and lower productivity levels.<sup>250</sup> While these results may be specific to workplace monitoring, fear that the government is engaging in a “Big Brother” surveillance program could have a similar impact on private web activity.

#### A. AMENDING THE STATUTORY FRAMEWORK

Electronic information must be provided with sufficient protection in order to support the use of Carnivore as an appropriate search tool. To this end, two bills were proposed in the year 2000 to address some of the current shortcomings in statutory protection of electronic communication.<sup>251</sup> Neither bill made it out of committee, even though some of the recommendations would have added much-needed protections to the statutory framework. One important recommendation was to extend the statutory exclusionary rule to include electronic communication.<sup>252</sup> For real-time interceptions of electronic data, this amendment would have removed a formalistic distinction between traditional wiretaps and electronic taps. As for stored electronic data, such as e-mail, providing statutory exclusion would offer definite protection to information that the Supreme Court has not yet deemed private.

Another essential amendment would be to require annual reports detailing government seizure of stored electronic communications.<sup>253</sup> The reporting requirements proposed in one of the bills were comprehensive and, like wiretap reports, would have required prosecutors to divulge the number of orders made and the results of the seizure in each case.<sup>254</sup> Because there are currently no reports compiled for seizures of e-mail, this requirement is necessary to provide Congressional and public oversight.<sup>255</sup> The need for public monitoring is also pressing. An investigation by *USA Today* reporter Will Roger found that seizures of e-mail increased 800%,

---

250. See *Electronic Surveillance: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (prepared testimony of Jeffrey Rosen, Associate Professor at George Washington University Law School), available at 2000 WL 1268432.

251. See H.R. 5018, 106th Cong. (2000) (proposed by Rep. Charles T. Canady & Rep. Asa Hutchinson); H.R. 4987, 106th Cong. (2000) (proposed by Rep. Bob Barr & Rep. Jo Ann Emerson).

252. See H.R. 5018, 106th Cong. § 2 (2000); H.R. 4987, 106th Cong. § 3 (2000).

253. See H.R. 5018, 106th Cong. § 3 (2000).

254. See *id.* See also *ECPA 2000 Hearings*, *supra* note 34, at 54 (prepared statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

255. See *id.*

from thirty-three in 1997, to 301 in 1999.<sup>256</sup> With computer crime on the rise, it is important to monitor a search capability that is becoming an essential crime-fighting tool.<sup>257</sup>

Additionally, electronic communication in storage for any length of time should only be acquirable upon federal or state warrant. The bill that was before the house, H.R. 4987, recommended that the storage period be extended for up to one year, but this would have only maintained the formalistic and arbitrary cut-off in the current requirement.<sup>258</sup> The public has a reasonable expectation of privacy with regard to electronic data, like e-mail—regardless of whether ISP employees can access such files. This privacy expectation should be recognized and protected under the current scheme available for wire communication.

Orders for the interception of electronic and wire communications should be subject to the same limitations. Currently, an electronic wiretap order can issue on authorization by “any attorney for the government” for “any Federal felony,”<sup>259</sup> while traditional wiretaps require high-level Justice Department approval and are only allowed for a list of enumerated offenses.<sup>260</sup> Congress developed these limitations under Title III because an intrusive wiretap search should be used only for crimes recognized as “intrinsically serious” or characteristic of organized crime.<sup>261</sup> The cautiousness with which Congress approached wiretaps in 1968 should extend to electronic surveillance today. The issues of intrusion and privacy have not disappeared because the medium of communication has changed. In fact, Carnivore’s ability to capture and copy all of the electronic communication that it views suggests that the same level of procedural requirements and privacy protection should be applied to its use.

Additionally, the standard for pen register searches on the internet should be strengthened to require judges to make a finding of fact before issuing such an order. Pen register searches on the internet reveal more than just the numbers dialed on a telephone. They also may show which parties are in communication with one another, provide links to websites, and display the length of a communication. Thus, to issue an order for an electronic pen register or trap and trace search, the judge should find that “specific and articulable facts reasonably indicate that a crime has been, is

---

256. *See id.*

257. *See Kerr Senate Statement, supra* note 3.

258. H.R. 4987, 106th Cong. § 5 (2000).

259. 18 U.S.C. § 2516(3) (1994).

260. *See* 18 U.S.C. § 2516(1) (1994).

261. S. REP. NO. 90-1097, at 108 (1968).

being, or will be committed, and information likely to be obtained by such installation and use is relevant to the on-going investigation of that crime.”<sup>262</sup> This standard is the same one the Supreme Court devised in *Terry v. Ohio*, which is now required for police before they “stop and frisk” suspects.<sup>263</sup> This “reasonable indication” standard is far less onerous than probable cause, but it requires judges to use their discretion and make decisions to approve or deny searches based on the facts. Obligating judges to make a factual determination in approving each pen register order is desirable because such surveillance should only be used in valid investigations.<sup>264</sup> This would ensure that Carnivore’s pen register and trap and trace capabilities only be used to gather information on a crime that may be committed—as opposed to fishing for any evidence that may point to a crime.<sup>265</sup>

In addition, the reporting requirements currently applied to wiretaps should be expanded to include pen register or trap and trace searches. Currently, the Attorney General is required to report annually to Congress on the raw number of these searches conducted, but not with the same level of detail required for wiretap reports.<sup>266</sup> The report should distinguish between the instances when Carnivore is used and when traditional wiretap technologies are used to conduct the search. Further, the report should include statistics on the length of time for the wiretap and the number of arrests and prosecutions that resulted from the search. This report should be included in the annual wiretap report to facilitate monitoring all of the data together.<sup>267</sup>

#### B. CHRISTOPHER SLOBOGIN’S PROPORTIONALITY PRINCIPLE

The current framework for search and seizure in wiretaps creates a dichotomy of protection. On one end of the continuum, wiretap warrants require a probable cause belief that a crime is being committed, which is

---

262. H.R. 5018, 106th Cong. § 4 (2000).

263. 392 U.S. 1 (1968).

264. See *CDT Summary*, *supra* note 210. See also *ECPA 2000 Hearings*, *supra* note 34, at 28–29 (testimony of Rep. Asa Hutchinson) (asserting that the reasonable indication standard provides sufficient protection to pen register information as it requires the officer to articulate “specific and articulable facts” that a crime is or will be committed).

265. See *id.*

266. See 18 U.S.C. § 3126 (1994).

267. See *ECPA 2000 Hearings*, *supra* note 34, at 64–65 (prepared statement of Robert Corn-Revere, Attorney, Hogan & Hartson).

equivalent to approximately a fifty percent chance that the belief is true.<sup>268</sup> On the other end, the standard for a pen register search requires that the seized information be “relevant” to an ongoing investigation. The level of certainty under the relevance standard has been characterized as accurate between five and ten percent of the time.<sup>269</sup> Very little guidance exists between these two levels of certainty. In response to the inadequate protection for personal privacy, Professor Christopher Slobogin suggests a balancing formula that he calls the “proportionality principle.”<sup>270</sup> This framework was first presented in *Terry v. Ohio*, where the Supreme Court held that in order to stop and frisk a suspect, the police need a reasonable suspicion—not the higher standard of probable cause.<sup>271</sup> The standard of reasonable suspicion requires the law enforcement officer to point to specific facts that would reasonably warrant the intrusion.<sup>272</sup> Slobogin suggests that this standard become a conceptual framework for all Fourth Amendment questions.<sup>273</sup> Using the proportionality principle as a guide, the operative question becomes how much of an explanation the government needs to supply for a given intrusion.<sup>274</sup>

Slobogin suggests that research on how the public rates the intrusiveness of various types of police actions should inform the current state of the law.<sup>275</sup> Through the process of balancing the reasonable intrusiveness of the search against the needs of law enforcement, Slobogin argues that we could develop differing levels of protection that would actually be meaningful to the public. The levels of protection in the search and seizure of electronic communication would, therefore, be analogous to the different levels of scrutiny in the individual rights context.<sup>276</sup> Slobogin asserts that while this balancing approach is difficult, it is the only way to avoid the current dichotomy, where some government intrusions must meet the high threshold of probable cause and other searches require no factual finding at all.<sup>277</sup>

---

268. See Christopher Slobogin, *Let's Not Bury Terry: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1083 (1998). See also Telephone interview with Christopher Slobogin, Professor of Law, Florida College of Law (Feb. 21, 2001).

269. See Slobogin, *supra* note 268, at 1084.

270. See *id.* at 1054.

271. See 392 U.S. 1, 21–22 (1968).

272. See *id.* at 21.

273. See Slobogin, *supra* note 268, at 1054.

274. See *id.* at 1084.

275. See *id.* at 1075.

276. See *id.* at 1069.

277. See *id.* at 1095.

## VII. CONCLUSION

Proper operation of the Carnivore system within the law requires both a system upgrade and amendments to the current statutory framework. The program must provide an auditing system to ensure that government agents are not overstepping the bounds of the search outlined in the court order. Different versions of the software should be developed for real-time searches based on probable cause, and for pen register searches based on the much lower relevance standard. In addition, the statutory framework must be amended to provide electronic communications with protections similar to those afforded to oral and wire communications.

*Addendum*

*On September 11, 2001 terrorists attacked the United States, killing thousands of people by hitting key financial and military centers. In the wake of these attacks, Congress passed The USA Patriot Act (“The Patriot”),<sup>278</sup> a bill created by the Bush Administration providing for the expansion of law enforcement powers in intelligence gathering, criminal procedure and immigration investigations.<sup>279</sup> In the arena of electronic surveillance, the bill primarily expands law enforcement powers under the Foreign Intelligence Surveillance Act (“FISA”),<sup>280</sup> however, some provisions affect the application of Title III and the ECPA—covering criminal investigations. To analyze the impact of this bill, this Note will briefly discuss FISA, in an effort to recognize the significant changes to the statutory scheme.*

*Governing foreign intelligence, FISA provides that the government may conduct electronic surveillance, when the application certifies that there is probable cause to believe that the target of the search is a foreign power.<sup>281</sup> When the order applies to a “United States Person”<sup>282</sup> the application must show that the information is necessary “to prevent threat of death or serious bodily harm.”<sup>283</sup> For non-U.S. Persons, the*

---

278. See H.R. 3162 (2001).

279. See U.S. Attorney General John Ashcroft’s Address at the U.S. Conference of Mayors, available at [http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/ashcrofttext\\_1025](http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/ashcrofttext_1025) (last visited Oct. 29, 2001).

280. See 50 U.S.C. §§ 1801–1811, 1841–1863 (1994).

281. See 50 U.S.C. § 1805(a)(3)(A).

282. See 50 U.S.C. § 1801(i). In relevant part, the Act defines U.S. Person as a citizen of the United States or an alien lawfully admitted for permanent residence. See *id.*

283. See 18 U.S.C. § 1805(f)(2).

information acquired must merely relate to national defense, security or the conduct of foreign affairs.<sup>284</sup> The Act permits surveillance in the form of full content searches and a pen register and trap and trace searches.<sup>285</sup> FISA surveillance does not contain many of the same checks and balances that govern the law guiding criminal investigations.<sup>286</sup>

Prior to the passage of the Patriot, FISA procedures applied when the investigation was for the purpose of foreign intelligence.<sup>287</sup> The Patriot has amended this provision to provide FISA surveillance where foreign intelligence is the “significant purpose.”<sup>288</sup> This amendment brings many more investigations under the ambit of FISA as it applies even where government agents are primarily searching for evidence of a domestic crime.<sup>289</sup>

The Patriot also provides for nation-wide service of pen register and trap and trace orders,<sup>290</sup> allowing agents to attach the device to any electronic line they deem necessary. The ACLU has noted that this provision operates as a “blank warrant” undercutting the judiciary’s ability to monitor the search.<sup>291</sup> This “roving” wiretap provision is significant as it potentially allows the government to monitor all telephone and computer lines in a public space, such as a university, if it determines the suspect is using one of them.

Additionally, the Patriot provides that businesses may voluntarily disclose customer records where it deems necessary to prevent an emergency involving death, or serious physical injury.<sup>292</sup> For example, an AOL employee may hand over customer records if he or she deems that the person is involved in aiding or initiating terrorist activities. This exception to a previous prohibition on divulging private records, has the potential of creating thousands of “civilian agents”—encouraging lay people to

---

284. See 18 U.S.C. § 1805.

285. See 18 U.S.C. § 1842(a)–(d).

286. See ACLU Legislative Analysis: USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances, at <http://www.aclu.org/congresss/1110101a.html> (last visited Nov. 11, 2001) [hereinafter *ACLU Patriot Analysis*].

287. See 18 U.S.C. § 1804(a)(7)(B).

288. See H.R. 3162 § 218 (2001) (amending 18 U.S.C. § 1802(b)).

289. See *ACLU Patriot Analysis*, *supra* note 286.

290. See H.R. 3162 § 218 (2001). Recall that the ECPA requires the agent to certify “the number, and if known, physical location . . . to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order.” See 18 U.S.C. § 3123(a)(1)(C).

291. See *ACLU Patriot Analysis*, *supra* note 286.

292. See H.R. 3162 § 212 (2001) (amending 18 U.S.C. § 2702 by creating an exception to the prohibition on divulging customer records).

*determine who should be suspected of terrorist activities. In these times of high anxiety, granting this level of subjective power is unwise.*

*The bill includes a sunset clause, providing that its provisions will cease to have effect on December 31, 2005.<sup>293</sup> It is the author's hope that the public will remain vigilant in the interim in an effort to inform the legislature on the constitutional impact of the current scheme.*

---

293. H.R. 3162 § 224 (2001).