COMMENTS

Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law Under the Patriot Act

Susan W. Dean*

* J.D. candidate 2003, Tulane University School of Law; B.A. 1997, George Washington University.

I. INTRODUCTION

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act or Act) was enacted on October 26, 2001, in response to the terrorist attacks of September 11, 2001.[1] The Act expands law enforcement's power to conduct searches, seizures, wiretaps, and other means of electronic surveillance.[2] As a result of these new powers, the Act has aroused controversy from privacy advocates.[3] While law enforcement has lauded the Act's new powers as a necessary means of combating domestic terrorism, privacy advocates worry that these new powers will be used against ordinary, law-abiding Americans.[4]

Part II of this Comment describes computer surveillance law before the enactment of the Patriot Act. This discussion gives a brief description of pen register and trap and trace (pen/trap) statutes, wiretap statutes, and the Electronic Communications Privacy Act (ECPA). Part III explores the new provisions of the Patriot Act and how it changes pen/trap statutes. Part IV discusses criticisms and controversies that have arisen because of these changes. Specifically, it addresses the use of pen/trap devices on computer networks, the nationwide effect of pen/trap court orders, and law enforcement's installation and use of their own pen/trap devices and related reporting concerns.

II. PREVIOUS LAW

A. Pen Register and Trap and Trace Device Law

Pen/trap devices, governed by 18 U.S.C. §§ 3121-3127, collect addressing information of wire and electronic communications.[5] Wiretap statutes, on the other hand, govern the gathering of the content of wire and electronic communications.[6] Pen registers record outgoing addressing information and trap and trace devices record incoming addressing information.[7] For telephone calls, pen/trap devices collect phone numbers dialed for outgoing calls and originating numbers for

---

1. *See, e.g.*, Thomas Stauffer, *Anti-Terror Bills Cause Worry*, ARIZ. DAILY STAR, Oct. 17, 2001, at A1.
2. *See id.*; David Cole, *National Security State*, THE NATION, Dec. 17, 2001, at 4.
3. Stauffer, *supra* note 1, at A1.
4. *Id.*
5. *See* ORIN S. KERR, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 146-47 (2001); 18 U.S.C.A. §§ 3121-3127 (2001).
6. 18 U.S.C.A. §§ 2510-2522.
7. KERR, *supra* note 5, at 148.

incoming calls but they do not collect the contents of communications.[8] For Internet communications, pen/trap law allows law enforcement to gather the addressing information of the communication, such as the To/From information contained in an e-mail header, but not the content of the e-mail.[9] Although pen/trap devices have been applied through court orders to Internet communications, their use is not specifically mentioned in the 1986 pen/trap statute.[10]

To install a pen/trap device, a government attorney must obtain an order from a court authorizing the installation.[11] In the order, the attorney must specify the identity of the person who is the subject of the investigation, the number and the physical location of the telephone line to which the pen/trap device will be attached, and a statement of the alleged offense.[12] The court will authorize the device if it finds "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[13] The order may authorize a pen/trap device for a period not to exceed sixty days but the court may later grant an extension.[14]

B. Wiretap Law

The collection of the content of oral, wire, and electronic communications is governed by 18 U.S.C. §§ 2510-2522, first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[15] ECPA, an amendment to Title III, was enacted in response to new technologies such as the Internet.[16] Specifically, ECPA extended Title III protections to wireless voice communications and electronic communications, such as e-mail.[17]

Title III applies to the interception of the contents of oral, wire, and electronic communications.[18] Telephone calls fall within the definition of

---

8. *Id.*
9. *Id.*
10. Dep't of Justice, Computer Crime & Intellectual Prop. Sec., Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001 (Nov. 5, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.
11. 18 U.S.C.A. § 3123(a)(1).
12. *Id.* § 3121(b)(1)(A)-(D).
13. *Id.* § 3123(a).
14. *Id.* § 3121(c)(1)-(2).
15. *Id.* §§ 2510-2522.
16. *See* Maricela Segura, *Is Carnivore Devouring Your Privacy?*, 75 S. CAL. L. REV. 231, 244-46 (2001).
17. *See id.* at 244-45.
18. 18 U.S.C.A. §§ 2510-2522.

wire communications under Title III because the content of the communication must be the human voice.[19] For a telephone call, the content is the actual conversation between the parties to the call.[20] Internet communications, including e-mail, fall within the catch-all definition of electronic communications.[21] For Internet communications, the content is the entire e-mail message.[22]

Title III prohibits the interception and disclosure of oral, wire, and electronic communications, unless a statutory exception applies.[23] A statutory exception exists for interception and disclosure pursuant to a court order under § 2518.[24] To grant the exception, the application for the court order must show probable cause to believe that the interception will reveal evidence of a § 2516 felony offense.[25] These offenses include counterfeiting, fraud, various other felonies, as well as offenses punishable by death.[26] The application must show that normal investigative techniques have been tried and failed, or that they reasonably appear to be unlikely to succeed or to be too dangerous.[27] It must also show that there is probable cause to believe that the communications facility is being used in a crime and that surveillance will be conducted in a way that minimizes interception of communications that do not provide evidence of a crime.[28] If these requirements are shown, a court order will be granted that permits interception of communications for up to thirty days.[29]

C. The Electronic Communications Privacy Act

In addition to extending Title III protections to Internet communications, the ECPA also established a three-tier system by which the government may obtain stored information from service providers.[30] An 18 U.S.C. § 2516 court order must be obtained for the real-time

---

19. *See id.* § 2510(1); KERR, *supra* note 5, at 152.
20. KERR, *supra* note 5, at 147.
21. *See* 18 U.S.C.A. § 2510(12); KERR, *supra* note 5, at 154.
22. *See* KERR, *supra* note 5, at 147.
23. 18 U.S.C.A. § 2511(1).
24. *Id.* § 2518.
25. *See id.*; KERR, *supra* note 5, at 157.
26. 18 U.S.C.A. § 2516(1)(a)-(p).
27. *Id.* § 2518(1)(c).
28. *Id.* § 2518(5).
29. *Id.* § 2518.
30. *See Fourth Amendment and the Internet, Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary, House of Representatives*, 106th Cong. 7 (Apr. 6, 2000) (statement of Kevin V. Di Gregory, Deputy Associate Attorney General, Dep't of Justice); 18 U.S.C.A. § 2701.

interception of wire or electronic communications.[31] A search warrant must be obtained for the content of wire or electronic communications stored by the service provider for 180 days or fewer.[32] The government, however, may obtain the content of wire or electronic communications stored by the service provider for more than 180 days in one of three ways: (1) through a federal or state warrant, without giving notice to the suspect; (2) through administrative or grand jury subpoena, with notice given to the suspect; or (3) through a court order, if specific facts are given to show reasonable grounds exist to believe that records are relevant to an ongoing investigation.[33]

III. THE PATRIOT ACT

President George W. Bush signed the Patriot Act, passed by the House of Representatives (House) 337 to 79 and the Senate 96 to 1, on October 26, 2001, as a response to the terrorist attacks of September 11, 2001.[34] The President, at the signing of the Act, stated that it "will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones."[35] The Act is designed to facilitate the government's monitoring, detaining, and disruption of terrorist activities.[36] It expands the power of the Federal Bureau of Investigation (FBI) in conducting searches, seizures, and other methods of electronic surveillance.[37] Attorney General John Ashcroft was opposed to any sunset provisions in the bill, which would limit these new powers to only a few years.[38] Although the House bill contained a three-year limit on these new powers, the Senate version contained only some sunset provisions thus giving the Bush Administration almost everything that it wanted.[39]

---

31. *See* 18 U.S.C.A. § 2516.
32. *See id.* § 2703(a).
33. *See id.* § 2703(b).
34. *See* Stauffer, *supra* note 1, at A1; Jess Bravin, *Senate Sends Antiterrorism Bill to Bush*, WALL ST. J., Oct. 26, 2001, at A3.
35. *President Signs Anti-Terrorism Bill, Remarks by the President at the Signing of the Patriot Act, Anti-Terrorism Legislation, East Room* (Oct. 26, 2001), *at* http://www.whitehouse.gov/news/releases/2001/10/20011026-5.html.
36. Jess Bravin & Ted Bridis, *Political Role Reversals Shape Antiterrorism Legislation*, WALL ST. J., Oct. 8, 2001, at A8.
37. *Id.*
38. Ted Bridis & Jess Bravin, *White House Seeks to Remove Time Limits on Surveillance Part of Antiterrorism Bill*, WALL ST. J., Oct. 5, 2001, at A16.
39. Bravin & Bridis, *supra* note 36, at A8.

The Patriot Act, which was rushed through both the House and the Senate, makes changes to over fifteen statutes.[40] This Act contains measures that allow the government to detain or deport suspects, eavesdrop on Internet communications, monitor financial transactions, and survey records of religious and political organizations.[41] Specifically, § 216 of the Patriot Act amends the pen/trap statute in three ways: (1) it clarifies that law enforcement may use pen/trap orders on computer networks, (2) it allows pen/trap orders to have nationwide effect, and (3) it allows for the FBI's use of Carnivore but imposes a reporting requirement for its use.[42] Section 216 is a permanent change to federal law and is exempted from sunset provisions contained in § 224.[43]

A. Expansion of Pen/Trap Orders to Computer Networks

The Patriot Act clarifies that pen/trap devices apply to computer networks. References in 18 U.S.C. §§ 3121, 3123, 3124, and 3127 to "line" are amended to "line or other facility."[44] According to the Department of Justice, a "facility" may include a cellular telephone number, a specific cellular telephone, an Internet user account or e-mail address, Internet Protocol (IP) address, or other similar computer network address.[45] Section 3123(b)(1)(C) now allows applicants to submit "the attributes of the communications to which the order applies" thereby allowing any of the identifiers to be used.[46]

The Patriot Act also allows law enforcement to obtain other information used in processing and transmitting wire and electronic communications.[47] The definitions of "pen register" and "trap and trace" are altered from a device that records or decodes "dialing and signaling information" to a device or process that records or decodes "dialing, routing, addressing, and signaling information."[48] This allows for information such as IP addresses, port numbers, and To/From information to be intercepted and disclosed to law enforcement.[49] This

---

40. Valerie L. Demmer, *Civil Liberties and Homeland Security*, THE HUMANIST, Jan./Feb. 2002, at 7.

41. *Id.*

42. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 288-90 (Oct. 26, 2001).

43. *Id.* at 295.

44. 18 U.S.C.A. §§ 3121-3124, 3127 (2002).

45. *See* Dep't of Justice, *supra* note 10.

46. 18 U.S.C.A. § 3123(a)(1).

47. *See* Dep't of Justice, *supra* note 10; 18 U.S.C. § 3123(b)(1)(C).

48. 18 U.S.C.A. § 3127(3)-(4); *see* Dep't of Justice, *supra* note 10.

49. 18 U.S.C.A. § 3127(3)-(4).

information can be retrieved provided that it does not include the contents of the communication.[50]

The Patriot Act also allows for use of pen/trap devices that cannot be physically attached to the facility.[51] It allows pen/trap devices to be "attached or applied" to the target facility.[52] It also revises the definition of "pen register" and "trap and trace device" to include an intangible "process" to collect information in the manner of a physical device.[53] This would allow software and other similar processes to be used to collect information.[54]

B. Nationwide Effect of Pen/Trap Orders

Under previous law, a court could authorize the installation and use of a pen/trap device only "within the jurisdiction of the court."[55] The Patriot Act amended this section to allow for the installation and use of a pen/trap device "anywhere within the United States."[56] The Act allows the court order to apply to any person or entity providing service in the United States whose assistance may facilitate the use of the order.[57] The person or entity does not have to be named in the order for the order to apply to them.[58]

The Patriot Act also empowers courts to authorize the installation and use of pen/trap devices in other geographical locations.[59] Previously, court orders had to specify "the number, and, if known, physical location of the telephone line."[60] Section 3123 (b)(1)(C) was amended so that now court orders only have to specify "the attributes of the communications to which the order applies, including the number or other identifier, and, if known, the location of the telephone."[61] Because of the nationwide effect of these orders, the issuing court must have jurisdiction over the crime under investigation.[62]

---

50. *Id.*
51. *See* Dep't of Justice, *supra* note 10.
52. *See id.*; 18 U.S.C.A. § 3123(b)(1)(a).
53. 18 U.S.C.A. § 3127(3)-(4).
54. *See* Dep't of Justice, *supra* note 10.
55. 18 U.S.C.A. § 3123(a).
56. *Id.* § 3123(a)(1).
57. *Id.*
58. *Id.*
59. *See id.* § 3123(b)(1)(C); Dep't of Justice, *supra* note 10.
60. 18 U.S.C.A. § 3123(b)(1)(C); *cf. id.* (2001).
61. *Id.*
62. Dep't of Justice, *supra* note 10.

C. Carnivore and Law Enforcement Reports on Use of These Devices on Computer Networks

The Patriot Act authorizes law enforcement, through a court order, to attach its own pen/trap device to a facility.[63] This allows for the use of DCS1000 (commonly known as Carnivore), the FBI's diagnostic tool that has the ability to intercept and collect Internet communications.[64] Law enforcement may choose to install Carnivore when service providers are unable to carry out the court order themselves.[65]

The Act adds a reporting requirement for cases in which law enforcement installs its own device, such as Carnivore, on a packet switched data network of a provider to collect information.[66] The amendments require that law enforcement provides the following information to the court under seal within thirty days: (1) the officers who installed or accessed the device to obtain information; (2) the date and time the device was installed, uninstalled, and accessed; (3) the configuration of the device at installation and any modifications thereof; and (4) any information collected by the device.[67]

IV. CRITICISMS OF THE PATRIOT ACT'S PEN REGISTER AND TRAP AND TRACE AMENDMENTS

While the Patriot Act has been criticized for many of its provisions, this Comment will only focus on criticisms of the changes to pen/trap device law. Specifically, it will discuss (1) expansion of pen/trap devices to computer networks, (2) nationwide effect of pen/trap orders, and (3) use of Carnivore and related reporting requirements.

A. Concerns of Expansion of Pen/Trap Orders to Computer Networks

Although pen/trap have been used for many years on computer communications, the Patriot Act clarifies that pen/trap devices apply to computer networks.[68] The Act allows "dialing, routing, addressing, or signaling information" to be retrieved provided that the information does not include the contents of the communication.[69] Since the Act does not

---

63. *See id.*
64. Fed. Bureau of Investigation, FBI Programs and Initiatives—Carnivore Diagnostic Tool, *available at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm.
65. *See* Dep't of Justice, *supra* note 10.
66. 18 U.S.C.A. § 3123(a)(3)(A).
67. *Id.*
68. *See* Dep't of Justice, *supra* note 10; 18 U.S.C.A. §§ 3121-3124, 3127.
69. 18 U.S.C.A. § 3127(3)-(4).

precisely define these terms, critics have cited numerous complaints that content will also be intercepted.

1. Interception of Website Content Due to Lack of Specificity in Definitions

Although investigators may obtain "dialing, routing, addressing, or signaling information," this phrase is not defined in the Patriot Act.[70] Critics argue that websites may be considered "dialing, routing, addressing, or signaling information," thus allowing law enforcement to intercept which websites a person had visited.[71] Privacy advocates fought the application of pen/trap devices to Internet communications because Web addressing information inevitably reveals something about the content of communications.[72]

The Patriot Act leaves unanswered how much Internet information can be captured—whether just the overall address or a list of documents viewed.[73] Although the Patriot Act excludes content from interceptions allowed under the pen/trap statutes, content is easily ascertained once there has been interception and disclosure of a website because it is impossible to obtain the address information from a website without seeing its content.[74] "This is like giving law enforcement the power—based only on its own certification—to require the librarian to report on the books you had perused while visiting the public library."[75] This new amendment would possibly give too much content information to law enforcement without normal procedural safeguards.

2. Difficulty of Determining Content Versus Non-Content Information in Internet Communications

Critics have argued that the term "content" is unclear in the Patriot Act and, since it has not been tested in the context of Internet communications, law enforcement may have a difficult time separating

---

70. *Id.*

71. *See* Kelly Patricia O'Meara, *Police State*, INSIGHT ON THE NEWS, Dec. 3, 2001, at 12; Elec. Frontier Found., EFF Analysis of the Provisions of the USA Patriot Act (Oct. 31, 2001), *available at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

72. *See* Kevin Galvin, *Rights and Wrongs; Why New Law-Enforcement Powers Worry Civil Libertarians*, SEATTLE TIMES, Dec. 6, 2001, at A3.

73. *See id.*

74. *See id.*

75. Am. Civ. Liberties Union, How the USA Patriot Act Limits Judicial Oversight of Telephone and Internet Surveillance (Oct. 23, 2001), *at* http://www.aclu.org/congress/l102301g.html.

content from noncontent information.[76] Content "when used with respect to any wire, oral, or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."[77] The problem of content versus addressing information lies in the way that e-mail is transmitted.[78] E-mail messages move in packets that include both address and content information.[79] Thus, law enforcement must separate the address information from the content to comply with the requirements of a pen/trap court order.[80] Thus, "those executing and reviewing pen register and trap and trace orders will be left largely to their own devices in determining what they may obtain and review."[81]

Critics argue that, while the content of the e-mail is what law enforcement is interested in the most, Congress is relying on law enforcement to disregard content while separating it from the addressing information.[82] "In other words, the presumption is that law enforcement is only interested in who is being communicated with and not what is said, which critics say is unlikely."[83] Critics maintain that it will be important to monitor law enforcement to see what they obtain in Internet communications beyond the To/From header information in e-mail.[84]

B. Nationwide Reach of Pen/Trap Orders

The Patriot Act does not change the requirement that to install a pen/trap device, a government attorney must obtain an order from a court authorizing the installation.[85] The Patriot Act does, however, lengthen the reach of courts in authorizing pen/trap devices.[86] Under previous law, a court could authorize the installation and use of a pen/trap device only "within the jurisdiction of the court."[87] The Patriot Act amended this section to allow for the installation and use of a pen/trap device "anywhere within the United States."[88] This grants federal courts the

---

76. Ronald L. Plesser et al., *Summary and Analysis of Key Sections of the USA Patriot Act of 2001*, 2 No. 4 PRIVACY & INFO. L. REP. 1 (Dec. 2001).

77. 18 U.S.C.A. § 2510(8) (2001).

78. Nancy Chang, *How Does the USA Patriot Act Affect Bill of Rights?*, N.Y.L.J., Dec. 6, 2001, at 1.

79. *Id.*

80. *See* O'Meara, *supra* note 71, at 12.

81. Elkan Abramowitz & Barr A. Bohrer, *In the Name of Counter-Terrorism*, N.Y.L.J., Nov. 6, 2001, at 6.

82. *See* O'Meara, *supra* note 71, at 12.

83. *Id.*

84. *See* Plesser et al., *supra* note 76, at 1.

85. *Compare* 18 U.S.C.A. § 3123(a)(1) (2001), *with id.* (2002).

86. *Id.*

87. *Id.* § 3123(a) (2001).

88. *Id.* § 3123(a)(1) (2002).

authority to issue pen/trap orders that are valid anywhere in the United States, not just within their own jurisdictions.[89] It also allows the order to apply to any person or entity providing service in the United States whose assistance may facilitate the use of the order but the person or entity does not have to be named in the order for the order to apply to them.[90]

1. Law Enforcement's View

The Patriot Act allows pen/trap court orders to have nationwide reach.[91] Under previous law, many court orders had to be issued if the carrier did not pass source information with each telephone call.[92] This may have required law enforcement to obtain three court orders: one for a local exchange carrier, one for a local Bell Operating company, and one for a long distance carrier.[93] To facilitate these court orders, a prosecutor in a new district from the local judge had to acquire the order, and neither the prosecutor nor the judge may have had any interest in the case.[94] The Justice Department has stated that "this duplicative process of obtaining a separate order for each link in the communications chain has delayed or—given the difficulty of real-time tracing—completely thwarted important investigations."[95]

In the Patriot Act, law enforcement only has to obtain one court order, which it can apply in other jurisdictions. "Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order."[96] This order is valid as long as the issuing court has jurisdiction over the crime under investigation.[97] This new process will undoubtedly lead to quicker installations and use of pen/trap devices and less time expended by prosecutors.

---

89. *Id.*
90. *Id.*
91. *Id.*
92. *See* Dep't of Justice, *supra* note 10.
93. *Id.*
94. *Id.*
95. *Id.*
96. *Id.*
97. *Id.*

2. Possible Fourth Amendment Concerns

The nationwide effect of pen/trap devices, called "roving wiretaps" by critics, leads to Fourth Amendment concerns. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the places to be searched, and the persons or things to be seized.[98]

The Patriot Act raises Fourth Amendment concerns because its provisions allow a judge to issue a pen/trap order without particularly describing the place to be searched.[99] Instead, a single judge may grant an order even when the investigation or communications cross multiple jurisdictions.[100] The Supreme Court has held, however, that information gathered by pen/trap devices is not protected by the Fourth Amendment because the public does not have a reasonable expectation of privacy in telephone numbers they dial.[101] Since pen/trap devices on Internet communications arguably intercept more than addressing information, senders of e-mail may have a reasonable expectation of privacy in content information that they transmit over the Internet. This issue remains uncertain, however, because it has not been tested by the Supreme Court.

3. Judicial Oversight Concerns

Critics, including the American Civil Liberties Union (ACLU), have argued that the nationwide service of pen registers marginalizes the role of the judiciary by giving law enforcement the equivalent of a blank warrant in the physical world.[102] The ACLU argues that these new provisions are the equivalent of a blank warrant in which the court issues the order and law enforcement fills in the places to be searched.[103] Blank

---

98. U.S. CONST. amend. IV.

99. *See* 18 U.S.C.A. § 3123(a)(1) (2001).

100. *See id.*; Jonathan M. Winer & Debra D. Bernstein, *New Anti-Terrorist Law Has Significant Search and Seizure and Money Laundering Implications for U.S. Companies*, PRIVACY & INFO. L. REP., Dec. 2001, at 10.

101. Smith v. Maryland, 442 U.S. 735, 742 (1979); *see also* Segura, *supra* note 16, at 261-62.

102. *See* Am. Civ. Liberties Union, *supra* note 75; Am. Civ. Liberties Union, USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances (Nov. 1, 2001), *available at* http://www.aclu.org/congress/l10101a.html [hereinafter Am. Civ. Liberties Union (Nov. 1, 2001)].

103. Am. Civ. Liberties Union (Nov. 1, 2001), *supra* note 102.

warrants are not consistent with the Fourth Amendment, which requires that warrants specify the place to be searched.[104]

Judges who issue these orders are unable to monitor what is searched, as well as the extent of the search, thus weakening the role of the judiciary.[105] Critics have argued that the Fourth Amendment's directive is "meaningless when the government's surveillance activities are virtually undetectable and unaccountable and when the governmental agent's discretion has few realistic bounds."[106] These new provisions allow law enforcement too much discretion in filling in the place to be searched without adequate checks by the judiciary.

4. Standards of Proof for Pen/Trap Device Orders

The Patriot Act extends a low threshold of proof to Internet communications. The ACLU argues that the Act extends a low standard of proof to actual "content" information that can be gleamed from finding out what websites a person had visited.[107] Content information is subject to wiretap law rather than pen/trap device law.[108] Judges may issue wiretap orders only if there is probable cause to believe that interception will reveal evidence of a § 2516 felony offense.[109] For pen/trap devices, the Act provides that

> the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere in the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.[110]

According to the ACLU, the pen/trap device standard of proof is problematic because pen/trap devices, when used on Internet communications, reveal more information than simply the numbers dialed on a telephone.[111] It is also troubling because, while the wiretap statute allows judges to determine on the basis of the facts that there is probable cause, the pen/trap statute mandates that the judge must grant

---

104. *Id.*

105. *Id.*

106. Mark Young, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1021-22 (2001).

107. *See* Am. Civ. Liberties Union (Nov. 1, 2001), *supra* note 102; Galvin, *supra* note 72, at A3.

108. *See* 18 U.S.C.A. §§ 2510-2522 (2002).

109. *See* KERR, *supra* note 5, at 157; 18 U.S.C.A. § 2518(3)(a).

110. 18 U.S.C.A. § 3123(a)(1).

111. Am. Civ. Liberties Union (Nov. 1, 2001), *supra* note 102.

the order.[112] "Even if the judge disagrees, and believes that law enforcement officers are on a fishing expedition that will yield up no relevant information, the judge must issue the order."[113]

Alan Davidson, Associate Director of the Center for Democracy and Technology, suggests that there should be an increased standard for use of pen/trap orders.[114] Specifically, he argues that judges should be required to find that specific and particular facts reasonably indicate that criminal activity is taking place and that the information collected is relevant to the investigation.[115] This increased standard of proof for pen/trap orders would provide for more judicial oversight by judges and not subject judges to mere rubber-stamping of pen/trap court orders.

5. Service Providers' Concerns

In the Patriot Act, providers are directed to not disclose the existence of a pen/trap device or the existence of an investigation to their customers without authorization by the court.[116] Because of this potential liability, the Act provides that they may be immunized from suit or eligible for a good faith defense if they comply with this authority.[117] First, the Act allows a service provider to receive a written certification from law enforcement confirming that the order applies to them.[118] Second, the Act clarifies that compliance with a court order makes a service provider eligible for statutory immunity.[119]

Critics have argued that these new provisions will result in providers being asked to render assistance even though they are not named in the order and the assistance being requested is not defined in the order.[120] "Nevertheless, nationwide service could make it very difficult for local or regional service providers to oppose, modify, or contest court orders because it will require service providers to travel to numerous courts, in multiple jurisdictions, to address concerns over the breadth of court orders."[121] According to the ACLU, small ISPs are unlikely to challenge

---

112. *See* Elec. Frontier Found., *supra* note 71.

113. Am. Civ. Liberties Union, *supra* note 75.

114. *Cyber Security Enhancement Act of 2001, Hearing Before the Subcommittee on Crime of the Committee on the Judiciary, House of Representatives*, H.R. 3482, 107th Cong. 9 (Feb. 12, 2002) (statement of Alan Davidson, Staff Counsel, Center for Democracy and Tech.).

115. *Id.*

116. 18 U.S.C.A. § 3123(d)(2) (2002).

117. *See* Plesser et al., *supra* note 76, at 1; 18 U.S.C.A. § 3124(d)-(e).

118. *See* 18 U.S.C.A. § 3123(a)(1).

119. *See id.* § 3124(e).

120. Plesser et al., *supra* note 76, at 1.

121. *Id.*

court orders because of the time and expense involved.[122] This may result in ISPs abiding by pen/trap court orders that they find objectionable.

C. Carnivore and Reporting Concerns

The Patriot Act was enacted as a response to new technologies. Of these new technologies, Carnivore has been the most controversial. The Patriot Act allows for use of pen/trap devices that can not be physically attached to the facility.[123] This allows for the use of Carnivore, the FBI's solution to the problem of separating content from addressing information.[124] According to the FBI, Carnivore is a diagnostic tool that "provides the FBI with a 'surgical' ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept."[125] It is a computer-based search, which allows investigators to search keywords, e-mail addresses, or IP addresses.[126]

Carnivore has two modes of operation.[127] First, it can monitor and record the full content of a user's e-mail.[128] This full search of the content of messages is conducted under Title III statutes.[129] Second, Carnivore is able to acquire the address information for the origin and the destination of communications to and from the sender.[130] This is arguably similar to telephone numbers gathered under pen/trap devices and, is, therefore, governed by the pen/trap portion under the Patriot Act amendments.[131]

The Patriot Act adds a reporting requirement in cases in which law enforcement installs its own pen/trap device on a packet switched data network of a provider to collect information.[132] Carnivore is such a device and, therefore, law enforcement must heed to new reporting requirements and provide information to the court within thirty days of Carnivore's use.[133]

---

122. Am. Civ. Liberties Union (Nov. 1, 2001), *supra* note 102.
123. *See* Dep't of Justice, *supra* note 10.
124. Fed. Bureau of Investigation, *supra* note 64.
125. *Id.*
126. *See* Segura, *supra* note 16, at 233-34; Young, *supra* note 106, at 1029-30.
127. Segura, *supra* note 16, at 234.
128. *Id.*
129. *Id.* at 260.
130. *Id.* at 234.
131. 18 U.S.C.A. § 3123(a)(3) (2002).
132. *See id.*
133. *See id.* § 3123(a)(3)(A).

1. Law Enforcement's View

The Department of Justice and the FBI argue that Carnivore and other electronic interception devices are needed because of the increased use of communications networks in criminal activity.[134] Deputy Attorney General Kevin Di Gregory has defined Carnivore as "simply an investigative tool that is used online only under narrowly defined circumstances, and only when authorized by law, to meet our responsibilities to the public."[135] Both the Department of Justice and the FBI maintain that Carnivore is a minimizing tool that permits law enforcement to gather information that it has authorization to intercept but filters out other information it is not authorized to intercept.[136] Carnivore is a protector of privacy because of its filtering mechanisms.[137] "Carnivore serves to limit the messages viewable by human eyes to those which are strictly included in the court order."[138] The Department of Justice and the FBI also maintain that there are many mechanisms in place to prevent the misuse of Carnivore and to remedy any misuse that may occur.[139]

2. Privacy Concerns

Privacy advocates disagree with the Department of Justice and the FBI in its diagnosis of Carnivore as a privacy protection tool and argue that the Patriot Act will expand Carnivore's use. The Act authorizes law enforcement to install Carnivore after obtaining a court order that may be obtained upon only a minimal showing.[140] When Carnivore is installed on a system, it taps everyone's e-mail on the ISP, not just the suspect's e-

---

134. *See Fourth Amendment Issues Raised by the FBI's "Carnivore" Program, Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary, House of Representatives*, 106th Cong. 11 (July 24, 2000) (statement of Kevin V. Di Gregory, Deputy Associate Attorney General, Dep't of Justice); Fed. Bureau of Investigation, *supra* note 64.

135. *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program, Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary, House of Representatives*, 106th Cong. 19 (July 24, 2000) (statement of Kevin V. Di Gregory, Deputy Associate Attorney General, Dep't of Justice).

136. *Id.*; Fed. Bureau of Investigations, *supra* note 64.

137. Fed. Bureau of Investigations, *supra* note 64.

138. *Id.*

139. *Id.*; *see Fourth Amendment Issues Raised by the FBI's "Carnivore" Program, Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary, House of Representatives*, 106th Cong. 19 (July 24, 2000) (statement of Kevin V. Di Gregory, Deputy Associate Attorney General, Dep't of Justice).

140. David G. Goldstone, *Memorandum: Re: Provisions of the USA Patriot Act of 2001—Relating to Electronic Communications and Computer and Computer Storage Service*, PRACTICING LAW INSTITUTE, CORPORATE LAW AND PRACTICE HANDBOOK SERIES, Jan. 23, 2002, at 108.

mail.[141] "Since an ISP can have thousands of users, using Carnivore is like having the FBI tap the phone of everyone in your county because they think your neighbor across the street may be a foreign agent."[142]

According to critics, it is difficult to determine which mode of operation Carnivore is using.[143] The operator of Carnivore may switch modes using a computer and the program itself does not keep track of its search.[144] This allows the operator of Carnivore to have full discretion, while remaining untraceable and unaccountable.[145] Therefore, any oversight by a judge can be circumvented.[146]

V. CONCLUSION

The Patriot Act has undoubtedly changed law enforcement's ability to utilize pen/trap devices on Internet communications. The Patriot Act gives law enforcement new tools to combat domestic terrorism in the wake of September 11th. It will be important, however, to monitor law enforcement in their use of these tools to make sure that constitutional bounds are not exceeded.

---

141. *See* Derek M. Jennings, *Patriot Games*, INDEPENDENT ONLINE, *at* http://www.indyweek.com/durham/2001-11-07/jennings.html.

142. *Id.*

143. Young, *supra* note 106, at 1072.

144. *Id.*

145. *Id.*

146. *Id.*