Fordham Urban Law Journal

Volume 29 | Number 6 Article 3

2002

Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age

Kimberly Horn
Fordham University School of Law

PRIVACY VERSUS PROTECTION: EXPLORING THE BOUNDARIES OF ELECTRONIC SURVEILLANCE IN THE INTERNET AGE

*Kimberly A. Horn**

INTRODUCTION

Although his best selling novel *1984* was written over a half-century ago, George Orwell may have been on to something when he penned the phrase, "Big Brother Is Watching You."[1] While the United States bears no resemblance to the totalitarian state of Oceania, a futuristic world where citizens are under the constant surveillance and mind control of government,[2] our country's concern over governmental surveillance is a definitive reality in the Twenty-First Century.

In fact, even though the debate over the use of certain surveillance tools has quieted since the tragic events of September 11, 2001,[3] the concern over electronic surveillance is far from over.[4]

---

* J.D., Fordham University School of Law, 2002; B.A. Political Science, American University, 1998. I would like to thank Professors Ronald Blum and Daniel Richman for their guidance and inspiration in writing this Note. I would also like to give special thanks to my family for supporting me in all of my endeavors.

1. GEORGE ORWELL, 1984 at 3 (1949).

2. *See id.* at 4-5.

3. *See generally* Congressional Statements, FBI Press Room, *at* http://www.fbi.gov (last visited Apr. 15, 2002) (highlighting all Bureau testimony before Congress from 1998 through 2002). Before the events of September 11, 2001, there was a significant debate in Congress regarding the use of sophisticated new tools to conduct electronic surveillance. *See infra* Part II.A. Yet, since the terrorist acts on that date there have been no congressional hearings on the subject. *See* FBI, Congressional Statements, FBI Press Room, *at* http://www.fbi.gov (last visited Apr. 15, 2002).

4. Neil Robinson, *New Laws Seek to Balance Privacy and Surveillance*, JANE'S INTELLIGENCE REV., Jan. 1, 2002 ("The terrorist attacks in New York and Washington on September 11, 2001 have rekindled a passionate debate about protection of civil liberties and national security."). This is especially true since the passage of The USA Patriot Act, which was signed into law by President Bush on October 26, 2001. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). The USA Patriot Act, as it is ironically dubbed, significantly increases the government's law enforcement powers at the expense of civil liberties. ACLU, *USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances*, ACLU Legislative Analysis on USA Patriot Act, *at* http://www.aclu.org (dated Nov. 1, 2001); *see also* William Safire, *Seizing Dictatorial Power*, N.Y. TIMES, Nov. 15,

This concern is especially apparent among privacy advocates who, for many years, have applied constant pressure and waged numerous legal battles against the government's tactics.[5]

The relationship between privacy advocates and law enforcement has long been a tumultuous one, leaving privacy advocates with an inherent distrust of the devices utilized by law enforcement to conduct electronic surveillance.[6] Yet, this distrust may be completely justified, considering that new technologies have enhanced law enforcement's ability to conduct highly sophisticated surveillance on all citizens.[7] One such method of surveillance is the controversial new system dubbed "Carnivore" by its creators at the Federal Bureau of Investigation ("FBI").[8]

Carnivore is a diagnostic tool designed by the FBI to intercept and collect the electronic communications of criminal suspects.[9] It is a technologically advanced surveillance system designed to counter increasingly sophisticated criminals who use the Internet to conduct illegal activities.[10] Carnivore is an electronic device that is actually installed on a computer network,[11] most frequently on the networks of Internet Service Providers ("ISPs"), and it has the

---

2001 at A31 (calling on the government to hold onto American liberties while defending the United States against those who are trying to trump our freedom).

5. *See, e.g.*, Electronic Privacy Communication Center, *EPIC's Litigation Docket, About EPIC, at* http://www.epic.org (last updated Dec. 21, 1999).

6. Kathryn Balint, *Attack on America Personal Technology*, SAN DIEGO UNION-TRIB., Mar. 11, 2002, at E1; David Pogue, *State of the Art: Thinking About Gadgets For a More Sober World*, N.Y. TIMES, Sept. 20, 2001, at G1 ("Before September 11th, the public outcry for privacy had become almost deafening."). For a discussion of some of privacy advocates' specific criticisms, see *infra* Part II.A.

7. Lisa Guernsey, *Living Under an Electronic Eye*, N.Y. TIMES, Sept. 27, 2001, at G1 (recognizing how advances in computer technology have allowed for greater surveillance capabilities). For a discussion on the purported capabilities of one such surveillance tool, see *infra* Part II.A.

8. *See generally* Neil King, Jr. & Ted Bridis, *FBI's Wiretaps To Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3 (naming the system "Carnivore" because of its unique ability to get to "the meat" of an enormous amount of data). Favoring a more neutral name than "Carnivore", in February 2001, the FBI renamed the controversial system DCS1000, which stands for Digital Collection System. *Washington Wire*, WALL ST. J., Feb. 9, 2001, at A1. This name change, however, has done nothing to lessen the concerns of privacy advocates. Eric J. Sinrod, *EPIC Stalks Big Game in FBI's Carnivore*, N.Y. L.J., Apr. 23, 2002, at 5.

9. FBI, *Carnivore: Diagnostic Tool*, FBI Programs and Initiatives [hereinafter *Carnivore: Diagnostic Tool*], *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited on September 21, 2002).

10. *See infra* Part II.A.

11. During the course of a criminal investigation, Carnivore is installed "at the office of the suspect's Internet service provider." John Schwartz, *Computer Security Experts Question Internet Wiretaps*, N.Y. TIMES, Dec. 5, 2000, at A16.

ability to capture and store information traveling over such networks.[12]

Although Carnivore has been in existence since 1997, it was not until the year 2000 that its existence became public.[13] Upon its unveiling, Carnivore was met with a great deal of controversy and distrust, drawing criticism from privacy groups because of its invasive capabilities.[14] The implementation of Carnivore effectively revived a longstanding debate over the technical and legal capabilities associated with electronic surveillance and the effect of such capabilities on the privacy rights of individuals.[15] This debate has existed since Congress adopted comprehensive federal wiretap legislation with the passage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[16]

Specifically, privacy rights advocates argue that Carnivore invades the rights of innocent Internet users because it must search through and filter out their emails to reach the targeted communications of a criminal suspect.[17] Moreover, because Carnivore has the ability to capture a broad range of communications traveling across an ISPs network, beyond the targeted communications specified in a court warrant, privacy advocates argue that the government has the ability to conduct unauthorized surveillance on innocent Americans.[18]

Although the threat of unauthorized surveillance by law enforcement has always existed and at times been a reality,[19] since its inception, federal wiretap laws have provided safeguards that protect individuals against the consequences of such governmental abuse. Specifically, Title III requires that the interception of communications outside the scope of authorized surveillance must be minimized,[20] and it states that unlawfully intercepted communications

12. *Carnivore: Diagnostic Tool*, *supra* note 9.

13. *Biting Into Carnivore*, SAN DIEGO UNION-TRIB., Apr. 1, 2002, at E3 (noting that Carnivore was unveiled in July 2000).

14. *See infra* Part II.A.

15. Sinrod, *supra* note 8.

16. In fact, privacy considerations were among the most important concerns of Congress in their adoption of Title III. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)). For further discussion of the legislative intent behind Title III, see *infra* Part I.B.

17. King & Bridis, *supra* note 8.

18. John Schwartz, *Fighting Crime Online: Who is in Harm's Way?*, N.Y. TIMES, Feb. 8, 2001, at G1.

19. For a discussion of the FBI's role in illegal surveillance during the Hoover years, see discussion *infra* Part I.B.

20. 18 U.S.C. § 2518(5); *see also infra* text accompanying note 101.

may be found inadmissible in court proceedings.[21] These safeguards recognize the inevitability that traditional eavesdropping devices may record communications beyond those specified in a court order, despite the requirement that the government file particularized, as opposed to general, intercept orders.

While the FBI claims it has not used Carnivore to intercept unauthorized communications, critics of the system remain skeptical, and with arguably good reason. These critics are aware that Carnivore is specifically designed to capture electronic communications, which are not protected by the same safeguards as traditional oral and wire communications under Title III.[22] Specifically, because the exclusionary rule,[23] which warrants illegally obtained evidence inadmissible in court, does not apply to electronic communications, the FBI would not be prevented from using unauthorized electronic interceptions against a criminal suspect in court. Facing this reality, and mindful of the FBI's past abuses of power,[24] privacy groups are not willing to accept the FBI's assurances. Instead, these groups and many members of Congress favor reforms that will impose stricter requirements for Carnivore's use.

While the constitutionality of electronic surveillance has had a long legal tradition in the United States, the recent debate over Carnivore signals that the legal battles over law enforcement's surveillance techniques are far from over. In fact, in light of the results of a study of Carnivore's technical capabilities, the legal battles may be just beginning. As a result, Congress may need to step in and address the delicate balance between privacy and law enforcement interests and amend federal wiretap law accordingly. Congress may also have to address the reality of individual privacy expectations in the Internet Age.

The expansion of the Internet superhighway has led to a constant competition between law enforcement and criminals and has

21. 18 U.S.C. § 2518(10); *see also infra* text accompanying note 102.

22. In fact, Carnivore was originally authorized under the Electronic Communications Privacy Act, which sets forth much lower authorization standards for the interception of "electronic communications." *See infra* notes 113-142 and accompanying text for the requirements necessary to intercept electronic communications under the ECPA. Today, The USA Patriot Act specifically authorizes law enforcement to implement Carnivore under the existing ECPA standards for pen registers and trap-and-trace devices. *See infra* Part II.D. As a result, Carnivore may be utilized without a showing of probable cause. *See infra* Part II.D. For further discussion of the necessary standards to implement a pen register or trap-and-trace device, see *infra* notes 127-142 and accompanying text.

23. For a discussion of this legal principle see *infra* note 27 and accompanying text.

24. *See infra* notes 79-84 and accompanying text.

forced law enforcement to implement new technologies that will enable them to detect criminal activity.[25] Accordingly, Congress must keep pace with these technological advancements and enact legislation reflective of our changing world.

Part I of this Note begins with an overview of the common law tradition and congressional intent behind federal wiretap law. It then analyzes the Supreme Court decisions that set the constitutional standards for federal wiretap law and discusses how Congress tailored these standards to safeguard individual privacy rights. Part I also discusses subsequent legislation that was enacted in response to technological advancements in the telecommunications industry. Part I concludes by focusing on current challenges imposed on law enforcement by the proliferation of computer-related crime.

Part II highlights law enforcement's response to the growing dilemma of computer-related crime through the implementation of the controversial Carnivore system. This Part also discusses the arguments surrounding the use of Carnivore and analyzes recent court decisions that have signaled a decline in Internet users' legitimate expectation of privacy. In addition, Part II analyzes the effect that recent litigation may have on the FBI's ability to force ISPs to install Carnivore on their systems, as well as the effect that the terrorist attacks of September 11, 2001 have had on the implementation procedures associated with electronic surveillance.

Part III of this Note argues that Congress must implement tougher standards with respect to electronic surveillance. The Note concludes by arguing that the interception of electronic communications, through devices such as Carnivore, should be held to the same standards as traditional surveillance activities under Title III, and that federal wiretap law must be amended to reflect our changing times.

I. SETTING THE STAGE FOR LEGALIZED SURVEILLANCE

A. The History Behind Federal Wiretap Law

Ratified in 1791, the Fourth Amendment to the Constitution was adopted to safeguard individuals against governmental intrusion. According to the Fourth Amendment:

25. *Cybercrime: Statement Before S. Comm. on Appropriations, Subcomm. for the Dep'ts of Commerce, Justice, State the Judiciary, and Related Agencies*, 106th Cong. 6 (2000) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) [hereinafter *Freeh Testimony*].

> 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 place to be searched, and the persons or things to be seized.[26]

The constitutional limitations imposed by the Fourth Amendment, with respect to the methods law enforcement agents utilize to acquire evidence have provoked substantial debate for over a century.[27] Although law enforcement officials still rely heavily on traditional search warrants to seize personal property, over the years they have recognized the increasing need for more sophisticated techniques to combat the growing crime rate. As these crime-fighting mechanisms have evolved over time, so too has the Court's interpretation of the Fourth Amendment.

The Supreme Court was first asked to consider the constitutionality of electronic surveillance as early as 1928, nearly fifty years after the invention of the telephone.[28] In *Olmstead v. United States*, the Supreme Court held that the warrantless wire tapping of telephones did not violate the Fourth Amendment.[29] Relying on the idea that the Fourth Amendment protected only tangible property,[30] the Supreme Court held that the tapping of telephone wires did not constitute a search and seizure because the surveillance did not amount to the actual "search" or "seizure" of physical prop-

---

26. U.S. CONST. amend. IV.

27. *See generally* Jared J. Nylund, Comment, *Fire With Fire: How the FBI Set Technical Standards For the Telecommunications Industry Under CALEA*, 8 COMMLAW CONSPECTUS 329, 330 (2000). It is interesting to note that just over a century ago, all pertinent evidence was deemed admissible, regardless of the method under which it was obtained. *Id.* (quoting Olmstead v. United States, 277 U.S. 438, 462 (1928) ("American courts of law observed the common law rule that 'if the tendered evidence was pertinent, the method of obtaining it was unimportant.'")). The Supreme Court later recognized an exception to this practice, adopting what is today known as the "exclusionary rule," where evidence obtained in an unlawful manner is deemed inadmissible in court. *See* Weeks v. United States, 232 U.S. 383, 398 (1914) (holding that a lower court's admission of papers seized in direct violation of the constitution constituted "prejudicial error").

28. *See Olmstead*, 277 U.S. at 438; *see also* S. REP. NO. 90-1097, at 35 (1968). *See generally* WAYNE R. LAFAVE & JEROLD H. ISRAEL, *Wiretapping and Electronic Surveillance*, in CRIMINAL PROCEDURE 245, 246 (2d ed. 1992).

29. *Olmstead*, 277 U.S. at 466.

30. *Id.* at 465-66. Finding it unjustifiable to enlarge the language of the Fourth Amendment, the Court stated that there can be no Fourth Amendment violation "unless there has been an official search and seizure of [a defendant's] person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure." *Id.* at 466.

erty, nor did it require law enforcement to trespass upon the defendants' homes or offices.[31]

Following the Court's decision in *Olmstead*, federal law enforcement's ability to prosecute criminals through the use of intercepted communications was severely impaired when Congress passed the Communications Act of 1934 ("§ 605").[32] As originally written, § 605 held in part, that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[33] Yet, despite the purported benefit of protecting the privacy rights of individuals, § 605 did not guarantee absolute protection against government surveillance. For example, the law did not cover wiretapping by consent, and federal law enforcement was able to circumvent its prohibitions by arguing, "that § 605 did not prohibit wiretapping alone, but only [wire]tapping followed by 'divulgence.'"[34] § 605 also did not extend coverage to state law enforcement officials, nor did it account for technological advancements that would produce eavesdropping devices falling outside the prohibitions of the law.[35]

Because § 605 left loopholes regarding the application of the wiretapping prohibition, federal agents continued to use wiretaps to further criminal investigations.[36] This practice continued until 1937, when the Supreme Court held that the wiretapping prohibition did in fact apply to federal law enforcement agents; therefore, any communications intercepted by law enforcement without the prior consent of the sender were deemed inadmissible at trial.[37] In

31. *Id.* at 464.

32. Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064 (current version at 47 U.S.C. §§ 151-714). The amended act now provides for an exception with respect to Chapter 119 of the U.S. Code. *See* THE FBI: A COMPREHENSIVE REFERENCE GUIDE 21 (Athan G. Theoharis et al. eds., 1999) [hereinafter FBI REFERENCE GUIDE].

33. LAFAVE & ISRAEL, *supra* note 28, at 246 (quoting former 47 U.S.C. § 605 (1934)).

34. *Id.* at 247.

35. *Id.*

36. FBI REFERENCE GUIDE, *supra* note 32, at 21.

37. *See* Nardone v. United States, 302 U.S. 379, 384-85 (1937) [hereinafter *Nardone I*]. In a later case, the Supreme Court extended this exclusionary rule by holding that § 605 bars evidence obtained directly by wiretapping, as well as evidence obtained through leads generated by such wiretapping. *See* Nardone v. United States, 308 U.S. 338, 341 (1939) [hereinafter *Nardone II*]; FBI REFERENCE GUIDE, *supra* note 32, at 21.

addition, the Court dismissed any case where the indictment was based on such illegally obtained evidence.[38]

As the law continued to develop, the Supreme Court extended constitutional protection beyond the mere seizure of tangible items, holding that the Fourth Amendment extended to oral statements recorded without any "technical trespass under the local property law."[39] This decision was later expanded in *Berger v. New York*,[40] a landmark decision that played a significant role in shaping federal wiretap law.

In *Berger*, the Supreme Court struck down a New York statute authorizing electronic eavesdropping by law enforcement officials investigating certain types of crimes.[41] In its decision, the Court held that conversations fall within the meaning of the Fourth Amendment, and that the seizure of conversations constitutes a Fourth Amendment search.[42] In addition, the Court stated that evidence obtained by surveillance conducted in violation of the Fourth Amendment is inadmissible in court.[43]

Concluding that the New York statute was so broad that it failed to meet certain constitutional standards under the Fourth Amendment, the Supreme Court, "delineated the constitutional criteria that electronic surveillance legislation should contain."[44] For example, in addition to providing proof of probable cause, the Court held that there is a Fourth Amendment requirement of "particularity."[45] Particularity means that rather than utilizing a general warrant to conduct searches, law enforcement would be required to delineate in the warrant the specific details regarding the person, place or thing to be seized, as well as the nature of the crime in question and the type of conversation sought.[46] The *Berger* Court also reasoned that there should be "precise and discriminate" procedures in place to minimize the unauthorized interception of con-

38. FBI REFERENCE GUIDE, *supra* note 32, at 21. Yet, even after *Nardone II* was decided, the FBI continued to conduct secret wiretaps of "subversive groups" and of individuals suspected of spying. *Id.* These activities were authorized by President Franklin D. Roosevelt, who justified his "secret directive" by claiming that the Supreme Court's rulings did not prohibit the government from obtaining intelligence for national defense purposes. *Id.*

39. Silverman v. United States, 365 U.S. 505, 511 (1961).

40. 388 U.S. 41 (1967).

41. *Id.* at 44.

42. *Id.* at 51.

43. *Id.* at 55.

44. S. REP. NO. 90-1097, at 36 (1968). *See generally Berger*, 388 U.S. at 54-64.

45. *Berger*, 388 U.S. at 55.

46. *Id.* at 55-56; *see also* S. REP. NO. 90-1097, at 43.

versations unconnected to the crime being investigated.[47] Expressing concern over the authorization and extensions of surveillance pursuant to a single showing of probable cause, the Court maintained that the continuance of electronic surveillance should be permitted only upon renewed showings of probable cause.[48] In addition, the Court stated that the executing officer should have to "make a return" on the eavesdropping warrant to prove what was seized, and that there must be a showing of exigent circumstances to overcome the defect of not giving prior notice for the search.[49]

Nearly six months after the *Berger* decision laid out the constitutional requirements that the Supreme Court dictated should embody electronic surveillance legislation, the Court reaffirmed these standards in *Katz v. United States*.[50] In *Katz*, the Supreme Court held that, "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which [the petitioner] justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[51] The Court made it clear that there was no constitutional significance in the fact that the electronic listening device used to make the interception did not physically "penetrate" the wall of the phone booth.[52] Furthermore, *Katz* concluded that, although the agents conducting the surveillance exercised restraint, their failure to obtain prior judicial approval was "per se unreasonable under the Fourth Amendment."[53] The Court held that such "antecedent justification" was a "constitutional precondition" for electronic surveillance.[54]

Recognizing the obvious need for national legislation to set uniform standards and to implement "comprehensive, fair and effective reform,"[55] Congress adopted the constitutional standards laid out in *Berger* and *Katz* as a guide for drafting federal wiretap legislation.[56] As a result, less than one year after these landmark decisions, Congress implemented comprehensive federal wiretap legislation with the passage of Title III of the Omnibus Crime Con-

47. *Berger*, 388 U.S. at 58. *See generally* LAFAVE & ISRAEL, *supra* note 28, at 267.
48. *Berger*, 388 U.S. at 59.
49. *Id.* at 60; S. REP. NO. 90-1097, at 43.
50. 389 U.S. 347, 353 (1967); *see also* S. REP. NO. 90-1097, at 43.
51. *Katz*, 389 U.S. at 353.
52. *Id.*
53. *Id.* at 357.
54. *Id.* at 359; *see also* S. REP. NO. 90-1097, at 44.
55. S. REP. NO. 90-1097, at 38.
56. *Id.* at 44.

trol and Safe Streets Act of 1968.[57] Under Title III, Congress prohibited all wiretapping and electronic surveillance, except by persons authorized under law, including law enforcement officials engaged in the investigation of certain crimes.[58] According to the Circuit Court for the District of Columbia, "In enacting Title III, Congress sought to regulate . . . the use of electronic surveillance as an investigative tool and the disclosure of materials obtained through such surveillance."[59]

Title III was enacted in response to the Court's recognition that electronic surveillance did not constitute a violation of the Fourth Amendment, as long as such surveillance was conducted in a legal manner. Although Congress recognized that electronic surveillance was an essential law enforcement mechanism,[60] it also hoped to safeguard individual privacy rights by delineating a rigorous set of requirements for how such surveillance could be conducted.[61] By incorporating the criteria set forth in *Berger* and *Katz*, Congress created a strict standard for surveillance that extends beyond the requirements of the Fourth Amendment.[62]

At the time of its passage, Title III was seen as an "essential tool to law enforcement officials in waging all-out war against organized crime."[63] This continues to be true today, as electronic surveillance is seen as "one of the most important capabilities"[64] in gathering evidence to fight many different types of crime, including terrorism

57. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 212 (codified as amended 18 U.S.C. §§ 2510-2522 (2000)); *see also* Susan Kopecky, Note, *Dealing With Intercepted Communications: Title III of the Omnibus Control and Safe Streets Act in Civil Litigation*, 12 REV. LITIG. 441, 442 (1993) (noting that Title III was "the first comprehensive federal legislation pertaining to wiretapping and electronic surveillance").

58. *See* 18 U.S.C. § 2511. However, Title III is applicable to intercepted evidence in all cases, including civil and criminal cases. Kopecky, *supra* note 57, at 442.

59. Chong v. DEA, 929 F.2d 729, 732 (D.C. Cir. 1991) (citing Gelbard v. United States, 408 U.S. 41, 46 (1972)).

60. *See infra* notes 63-66 and accompanying text.

61. For a detailed analysis of the safeguards imposed by Title III, see *infra* Part I.B. It remains unclear whether Congress's central goal in enacting Title III was to secure civil liberties or to ensure authorization for law enforcement activities. For instance, it has been suggested that Title III was passed to "address the privacy concerns created by the ever-increasing development and use of electronic surveillance equipment." Kopecky, *supra* note 57, at 442. At the same time, however, Kopecky acknowledges that Title III was enacted as a way to authorize the government to acquire "information needed to maintain effective law enforcement." *Id.* For further discussion, see *infra* notes 72-76 and accompanying text.

62. *Infra* notes 77-78 and accompanying text.

63. S. REP. NO. 90-1097, at 145 (1968).

64. *Carnivore: Diagnostic Tool*, *supra* note 9.

and drug trafficking. Recognizing the importance of electronic surveillance, many states have developed laws similar to Title III, authorizing state courts to issue orders for oral, wire, or electronic surveillance.[65] As of 1999, a total of forty-five jurisdictions had such laws.[66]

B. Privacy Versus Protection: Congress Strikes a Balance

While there is little doubt that the use of electronic surveillance is critical to law enforcement's crime fighting efforts,[67] the authority granted to law enforcement by Title III was difficult to achieve. As is evident from its legislative history, the passage of Title III sparked considerable debate, leaving many legislators concerned about Title III's effect on individual privacy rights. In particular, some members of Congress believed that the authority granted to law enforcement presented a "grave threat to privacy," with one senator characterizing Title III as the "End to Privacy Act."[68]

During its debate over Title III, Congress recognized the tremendous impact that technological advancements could have on privacy rights. Congress understood that the privacy of communications was "seriously jeopardized" by the technological advancements in surveillance,[69] and that such advancements could ultimately lead to abuse by law enforcement.[70] Accordingly, privacy protections were an "overriding" concern of Congress, in its consideration of Title III.[71]

Recognizing that the current status of the law "serve[d] neither the interests of privacy nor of law enforcement,"[72] Congress passed Title III in 1968. Despite congressional concerns over privacy, Congress ultimately concluded that the advantages of such legisla-

65. LEONIDAS R. MECHAM, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, 2000 WIRETAP REPORT 7 (2002) [hereinafter 2000 WIRETAP REPORT], *available at* http://www.uscourts.gov/wiretap00.

66. *Id.* These jurisdictions include the federal government, the District of Columbia, the Virgin Islands, and forty-two states.

67. *See generally id.* at 10-11 (noting the importance of electronic surveillance in obtaining arrests and convictions). Although electronic surveillance is most often associated with criminal litigation, it is important to note that Title III also applies to evidence intercepted in civil cases. Kopecky, *supra* note 57, at 442.

68. S. REP. NO. 90-1097, at 116.

69. *Id.* at 36.

70. *Id.* at 116.

71. Gelbard v. United States, 408 U.S. 41, 48 (1972).

72. S. REP. NO. 90-1097, at 36-37 (quoting THE REPORT OF THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY (1967)) (internal quotations omitted).

tion outweighed the disadvantages.[73] Specifically, Congress recognized that conducting surveillance was an essential element in law enforcement's ability to detect crime.[74] Rather than stifle law enforcement's efforts to gather vital information by denying it the ability to conduct surveillance, Congress realized that it could safeguard the privacy of oral and written communications by defining the circumstances under which such surveillance would be authorized.[75] As a result, Title III was offered as an attempt to strike a balance between the two competing interests: privacy and protection.[76]

To prevent law enforcement from using electronic surveillance to infringe upon individual privacy rights, the drafters of Title III instituted "an elaborate system of checks and safeguards"[77] that extended beyond the probable cause requirement of the Fourth Amendment.[78] Congress set out specific guidelines related to surveillance, including provisions for the initiation of surveillance, limited disclosure, and penalties for unauthorized interception. Such safeguards were crucial, considering the widespread abuses by the FBI during this period under the leadership of J. Edgar Hoover.[79]

During Hoover's reign as the Director of the Bureau of Investigation from 1924 to 1972, illegal wiretaps and break-ins were common practice for federal agents who sought to gather intelligence on the "subversive activities" of radical groups, political leaders,

---

73. *Id.* at 139. Citing their responsibilities as legislators, one senator wrote, "There is a point at which individual privacy and rights yield to the public safety." *Id.* at 137.

74. *Id.* ("Modern surveillance techniques are urgently needed if law enforcement institutions are successfully to perform their sworn duty of protecting the public."); *see also In re* An Order Authorizing the Interception of Wire Communications, 413 F. Supp. 1321, 1331 (1976). Congress was especially concerned about the growth of organized crime. *See* S. REP. NO. 90-1097, at 145.

75. *See* Chong v. DEA, 929 F.2d 729, 732 (D.C. Cir. 1991); *see also Gelbard*, 408 U.S. at 48.

76. *In re* Persico, 491 F.2d 1156, 1159 (2d. Cir. 1974); S. REP. NO. 90-1097, at 155. According to Senate Report 1097, Title III was constructed for the dual purpose of "protecting the privacy of wire and oral communications, and delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. REP. NO. 90-1097, at 36; *see also* United States v. Clemente, 482 F. Supp. 102 (S.D.N.Y. 1979), *aff'd* 633 F.2d 207 (2d Cir. 1980).

77. S. REP. NO. 90-1097, at 138.

78. *Clemente*, 482 F. Supp. at 107.

79. Ironically, Hoover was appointed Director of the Bureau of Investigation, which was later renamed the Federal Bureau of Investigation, in 1924 in an effort to eradicate the surveillance abuses during World War I, to "ensure tighter discipline" within the Bureau, prevent future political spying, and improve the Bureau's public image. FBI REFERENCE GUIDE, *supra* note 32, at 11.

and public officials, including Dr. Martin Luther King, Jr. and other civil rights leaders.[80] These searches, although illegal, were part of a "secret directive"[81] to eliminate the threat of communism and organized crime within U.S. borders. Because of the secretive nature of these operations, the activities of the FBI were not monitored closely, leading to widespread abuses of power,[82] that were ultimately subject to public disclosure. The public uproar over the government's "unchecked" ability to eavesdrop on American citizens prompted the Senate to conduct lengthy hearings in the mid-1960s regarding the FBI's surveillance activities.[83] In light of the disclosures made during the 1960s and 1970s, Hoover was considered by many to be "the perpetrator of massive, systemic and vicious violations of the constitutional rights of American citizens."[84]

One of the most significant safeguards built into Title III is the requirement that law enforcement officials obtain judicial authorization prior to conducting electronic surveillance.[85] This requirement is significant because, unlike a typical search warrant, which only requires a Fourth Amendment showing of probable cause for judicial approval, the requirements to obtain a Title III intercept order are far more stringent. For example, law enforcement officials must obtain authorization from a senior official at the Justice Department before they may apply to the court for an order authorizing interception.[86] After this approval is obtained, the interception application must then be filed with a federal district judge,

80. The FBI admittedly used "improper and illegal methods" in its wiretapping surveillance of Dr. King and in its efforts to collect personal files on various congressmen. KATHRYN S. OLMSTEAD, CHALLENGING THE SECRET GOVERNMENT: THE POST-WATERGATE INVESTIGATIONS OF THE CIA AND FBI 37 (1996); *see also* FBI REFERENCE GUIDE, *supra* note 32, at 22.

81. FBI REFERENCE GUIDE, *supra* note 32, at 21. This "secret directive" was originally authorized by President Roosevelt in the wake of *Nardone I*. *See supra* notes 37-38 and accompanying text.

82. FBI REFERENCE GUIDE, *supra* note 32, at 21.

83. Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1364. While these hearings shed light on the problem and ultimately prompted Congress to consider Title III, a great deal of the FBI's illegal practices were not disclosed until the aftermath of the Watergate scandal. *See generally* FBI REFERENCE GUIDE, *supra* note 32, at 111.

84. FBI REFERENCE GUIDE, *supra* note 32, at 101.

85. 18 U.S.C. § 2518(1) (2000). There is, however, an exception that allows for immediate interception in certain emergency situations. In such situations, law enforcement must apply for a judicial order no more than 48 hours after the interception. 18 U.S.C. § 2518(7); *see also* LAFAVE & ISRAEL, *supra* note 28, at 249.

86. 18 U.S.C. § 2516(1).

who will either deny the application or issue an order permitting interception.[87]

Pursuant to 18 U.S.C. § 2518, a federal judge may issue an intercept order only if the judge determines that a number of requirements have been met.[88] One such requirement is specificity. Not only must the application specify the identity of the person upon whom the surveillance is being conducted,[89] but it must also specify the nature and location of the intercepted communications,[90] as well as describe the type of communications that law enforcement is seeking to intercept.[91] In addition, the application must identify the agency authorized to intercept such communications[92] and the period under which law enforcement wishes to conduct surveillance.[93] Although Title III permits extensions to the standard thirty-day period of uninterrupted surveillance,[94] such extensions are granted only if law enforcement makes a renewed showing of probable cause.[95] A judicial order may also require the government to file reports with the federal judge at specified intervals.[96]

According to § 2518(3), law enforcement must also establish probable cause to obtain an interception order under Title III. Law enforcement must prove that they have probable cause to believe the individual in question is involved in criminal activity relating to one of the enumerated offenses under Title III,[97] and that communications concerning that activity will be obtained through the interception.[98] In addition, law enforcement must have probable cause to believe that the facilities upon which they seek to conduct surveillance are commonly used by the individual in question, or are being used in connection with the criminal activity.[99]

To secure an intercept order, Title III also requires a showing of necessity and minimization. For example, law enforcement may

87. *See generally* 18 U.S.C. § 2518(1)-(3). Judicial approval of intercept applications must be obtained by an appointed federal district judge, rather than a federal magistrate. *See generally* U.S. CONST. art. II, § 2, cl. 2; U.S. CONST. art. III, § 1.

88. *See generally* 18 U.S.C. § 2518(1)-(4) (laying out the requirements for obtaining an intercept order).

89. *Id.* § 2518(4)(a).

90. *Id.* § 2518(4)(b).

91. *Id.* § 2518(4)(c).

92. *Id.* § 2518(4)(d).

93. *Id.* § 2518(4)(e).

94. *Id.* § 2518(4)(e).

95. *Id.* § 2518(5); *see also* LAFAVE & ISRAEL, *supra* note 28, at 250.

96. 18 U.S.C. § 2518(6).

97. *Id.* § 2518(3)(a). The list of offenses can be found at 18 U.S.C. § 2516.

98. *Id.* § 2518(3)(b).

99. *Id.* § 2518(3)(d)

not resort to electronic surveillance unless normal investigative procedures have either failed or are too dangerous.[100] Section 2518(5) also provides that surveillance should be conducted in a timely manner so that the interceptions of communications, not otherwise subject to surveillance, are minimized.[101] Furthermore, in the event that communications are intercepted unlawfully, such interceptions may be suppressed upon motion to the court.[102]

In addition to the stringent requirements necessary for the initiation of electronic surveillance, Title III seeks to safeguard the privacy rights of individuals by establishing rules regarding the disclosure of intercepted communications, as well as the illegal interception of communications. Title III clearly establishes the limited circumstances under which intercepted communications may be disclosed,[103] and sets out a penalty scheme for unauthorized surveillance activity.[104]

Furthermore, law enforcement's use of electronic surveillance is closely monitored. Title III requires the Administrative Office of the United States Courts ("AO") to file an annual report with Congress.[105] These reports must provide specific information with regard to the federal and state applications for intercept orders, including the nature of the offenses under investigation, the cost of surveillance and the number of convictions directly resulting from the surveillance.[106]

100. *Id.* § 2518(3)(c); *see also* Chong v. DEA, 929 F.2d 729, 732 (D.C. Cir. 1991).

101. 18 U.S.C. § 2518(5); *see also* United States v. Clemente, 482 F. Supp. 102, 108 (S.D.N.Y. 1979), *aff'd* 633 F.2d 207 (2d Cir. 1980).

102. 18 U.S.C. § 2518(10). The inadmissibility of unlawfully intercepted evidence is commonly referred to as the exclusionary rule. *See supra* note 27.

103. *See* 18 U.S.C. § 2517(1)-(3) (permitting disclosure of intercepted communications only under three circumstances).

104. *See id.* § 2511(4)-(5) (noting that unlawful interceptions are a crime, punishable by fine or imprisonment); *see also id.* § 2520 (authorizing the recovery of civil damages by persons whose communications have been disclosed in violation of Title III).

105. 2000 WIRETAP REPORT, *supra* note 65, at 5; *see also* 18 U.S.C. § 2519(3). According to § 2519(1)-(2), federal and state judges, as well as prosecutors, have a certain time period in which to file reports with the director of the AO concerning each application they have either submitted or reviewed. 2000 WIRETAP REPORT, *supra* note 65, at 6.

106. 2000 WIRETAP REPORT, *supra* note 65, at 5.

C. Congress Reacts to Technological Advancements: The Introduction of New Legislation Broadens the Authority of Federal Law Enforcement

Since Title III was enacted into law in 1968, there has been a tremendous proliferation in communications technology.[107] Advancements in telecommunications technology have added a whole new meaning to the term "communication," as individuals are now able to correspond electronically on a level not anticipated by previous legislators. Recognizing that the privacy of such electronic communications "could not be guaranteed absent legislation,"[108] Congress responded by adopting new legislation that ultimately broadened the power of federal law enforcement. Specifically, Congress passed the Electronic Communications Privacy Act of 1986[109] and the Communications Assistance for Law Enforcement Act of 1994.[110]

1. *The Electronic Communications Privacy Act of 1986*

In an effort to provide uniform legal standards with regard to the interception of non-voice communications,[111] Congress passed The Electronic Communications Privacy Act of 1986 ("ECPA").[112] This Act is significant because, among other things, it amended Title III, extending the protections against unauthorized interceptions to "electronic communications."[113] This extension was deemed necessary because technological advances in communications had left a gap in the coverage of federal wiretap law.[114] According to § 2510(12), "electronic communications" are defined as "any transfer of signs, signals, writing, images, sounds, data, or in-

107. For example, since that time, the world has seen the advent of the Internet, cellular telephones and portable computers.

108. *The Fourth Amendment and the Internet: Statement Before H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 4 (2000) (statement of Gregory T. Nojeim, Legislative Counsel, ACLU) [hereinafter *Nojeim Testimony*].

109. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C. (2000)).

110. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001-1010 and various sections of 18 U.S.C. and 47 U.S.C. (2000)).

111. *See* S. REP. No. 99-541, at 4 (1986).

112. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C. (2000)).

113. 18 U.S.C. § 2510(12) (2000).

114. Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995).

telligence . . . transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[115]

In addition to amending Title III, the ECPA is also significant for introducing two new chapters into federal law.[116] Specifically, under "Chapter 121," Congress created requirements for the authorized access of stored wire and electronic communications.[117] According to § 2702(b), such communications may be accessed by the communications service provider, in addition to law enforcement officials who have met the requisite standard.[118] This chapter is significant, because unlike "real-time" interception of electronic communications, which requires the government to obtain a court order under the auspices of Title III,[119] governmental access to stored communications requires adherence to a far less demanding standard.[120]

In fact, § 2703 sets out various means by which the government may compel an electronic service provider to disclose the contents of a subscriber's or customer's electronic communication.[121] According to § 2703(a), if the communication has been in storage in the service provider's system for one hundred and eighty days or less, the government may obtain that information provided it has a search warrant issued by a federal magistrate based on a showing of probable cause.[122] Yet, once that same information has been in electronic storage in excess of one hundred and eighty days, the requisite standard for access becomes even less demanding.[123] Specifically, the government may obtain the stored information through an administrative subpoena combined with delayed notice to the subscriber, or through a warrant if no notice is given.[124] The government can also obtain these stored communications by

115. 18 U.S.C. § 2510(12); *see also* LAFAVE & ISRAEL, *supra* note 28, at 271.

116. *See* Electronic Communications Privacy Act of 1986, ch. 121 & 206, 100 Stat. 1848 (introducing Chapter 121, "Stored Wire and Electronic Communications and Transactional Records Access" and Chapter 206, "Pen Registers and Trap and Trace Devices.").

117. *See* Electronic Communications Privacy Act of 1986, ch. 121, §§ 201-202, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2701-2710 (2000)). Stored communications are electronic communications, such as email, that have been retained in an electronic communications system. 18 U.S.C. § 2703.

118. 18 U.S.C. § 2702(b).

119. *See Nojeim Testimony*, *supra* note 108, at 5.

120. *Id.*; *see also* 18 U.S.C. § 2703(d).

121. 18 U.S.C. § 2703 (listing the requirements for government access).

122. *Id.* § 2703(a); *see also Nojeim Testimony*, *supra* note 108, at 5.

123. 18 U.S.C. § 2703(b).

124. *Id.* § 2703(b)(1)(A)-(B)(i).

presenting a court order.[125] Unlike the strict requirements that must be met to secure a court order under Title III, under § 2703(d) the government need only show, "that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[126] Accordingly, this standard falls far short of the probable cause requirement of the Fourth Amendment.

The ECPA also adopted a uniform procedure governing the use and authorization requirements for pen registers and trap-and-trace devices.[127] According to the ECPA, a pen register is a device that identifies and records the telephone numbers dialed in an outgoing call, while a trap-and-trace device identifies and records the telephone numbers from which incoming calls originate.[128] Through their attachment to a particular telephone line, such devices allow law enforcement to trace the source of a suspect's outgoing and/or incoming calls.[129] The introduction of statutory language governing the use of these devices is significant because it marks the first time that such devices were bound by a statutory scheme. Because neither device has the ability to capture the content of a communication, the use of such devices has never been regulated by either Title III,[130] or the Fourth Amendment.[131] In fact, the Supreme Court has held that because there is no legitimate expectation of privacy with respect to numbers dialed on a telephone, pen registers do not constitute a "search" requiring Fourth Amendment protection.[132]

Although the Supreme Court has refused to protect telephone numbers under the Fourth Amendment, the ECPA is significant because it requires law enforcement to obtain court orders to use

125. *Id.* § 2703(b)(1)(B)(ii).

126. *Id.* § 2703(d).

127. *See* Electronic Communications Privacy Act of 1986, ch. 206, 100 Stat. 1848. Inserted as "Chapter 206" under Title 18 of the United States Code, these requirements were codified into law as 18 U.S.C. §§ 3121-3127. *See id.*

128. 18 U.S.C. § 3127(3)-(4).

129. *See* United States Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000). These devices do not give law enforcement access to the content of the telephone conversations; rather they provide authorities with the same information that telephone companies have. *See* 18 U.S.C. §§ 3127(3)-(4).

130. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 166-67 (1977) (finding that because pen registers do not acquire the contents of communications, they therefore do not "intercept" such communications within the meaning of Title III).

131. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979); *see also* Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995).

132. *See Smith*, 442 U.S. at 745-46.

pen register and trap-and-trace devices.[133] Yet, unlike the heightened probable cause standard that must be met under Title III and the Fourth Amendment, to obtain a court order for a pen register or trap-and-trace device, the government must certify only "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[134] In addition, any attorney for the government may make such an application to the court, without prior approval from senior officials at the Department of Justice.[135]

Despite the significant changes in federal wiretap law imposed by the ECPA, there are some shortcomings that have sparked considerable debate.[136] While the ECPA expanded the scope and protections of federal law to encompass electronic communications, it did so without strictly adhering to the standards set forth in Title III. In addition to establishing less demanding standards for the search and seizure of stored electronic communications and the use of pen register devices,[137] the ECPA provides less protection for electronic communications intercepted under Title III than it does for voice communications.[138] For example, any government attorney can authorize an application for an order to intercept electronic communications,[139] and law enforcement can make interceptions relating to any federal felony.[140] In addition, the statutory exclusionary rule does not apply to electronic communications.[141] As a result, even if law enforcement agents unlawfully intercept electronic communications, these communications can still be admissible as evidence in court.[142]

---

133. *See* 18 U.S.C. § 3121(a).

134. *Id.* § 3122(b)(2); *see also United States Telecom Ass'n*, 227 F.3d at 454.

135. 18 U.S.C. § 3122(a).

136. *See Nojeim Testimony*, *supra* note 108, at 4-6.

137. *See supra* text accompanying notes 117-135.

138. *Nojeim Testimony*, *supra* note 108, at 4.

139. *Id.* at 5. In contrast, the interception of voice communications under Title III requires authorization from a senior official at the Justice Department. *See supra* note 86 and accompanying text.

140. *Nojeim Testimony*, *supra* note 108, at 5. Under Title III, voice communications can only be intercepted if they relate to one of the offenses listed in 18 U.S.C. § 2516. *See supra* note 97 and accompanying text.

141. *See* 18 U.S.C. §§ 2515, 2518(10)(a) (applying the mandatory suppression of illegally obtained evidence to wire and oral communications only, and not to email); *see also Nojeim Testimony*, *supra* note 108, at 5; LAFAVE & ISRAEL, *supra* note 28, at 271.

142. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 n.6 (5th Cir. 1994); *see also* Ted Bridis, *Updating of Wiretap Law for E-mail Age is Urged by the Clinton Administration*, WALL ST. J., July 18, 2000, at A3.

Because of the lower standards implemented by the ECPA, critics argue that electronic communications are not being given the protection that Congress intended.[143] They argue that law enforcement has the upper hand because it can avoid complying with Title III's strict requirements by simply waiting until an electronic communication becomes stored in the computer network (which happens immediately after delivery), rather than intercept the communication en route.[144] They also argue that because the exclusionary rules do not extend to cover electronic communications, there is no incentive for law enforcement agents to comply with the proper procedures.[145]

Expressing concern over the relative ease with which law enforcement may intercept electronic communications, especially in light of the FBI's Carnivore system, privacy groups and members of Congress have proposed that the ECPA be amended to provide stricter standards. One such proposal, House Bill 5018, The Electronic Communications Privacy Act of 2000, was scheduled for a mark-up before the House Judiciary Committee.[146] This Act proposed that the authorization standard for pen register and trap-and-trace devices be raised to require a "reasonable suspicion" of crime, and that the exclusionary rule of Title III be extended to cover all electronic communications, including those that are stored.[147] It also would have extended coverage of the reporting requirements under § 2519 of Title III to stored communications.[148] Yet, despite the additional safeguards proposed by House Bill 5018, privacy advocates remained apprehensive, characterizing the bill as inadequate.[149] Specifically, they were concerned that the bill did not mention Carnivore, and that Congress would implement proposals that would ease restrictions on electronic surveillance, rather than enhance privacy protections.[150] Ultimately, the bill

143. *Nojeim Testimony*, *supra* note 108, at 5.

144. *Id.*

145. *See id.*

146. *See* Letter from Laura W. Murphy, Director, ACLU, to Reps. Henry Hyde & John Conyers, Chairman and Ranking Member, H.R. Comm. on the Judiciary (Sept. 18, 2000), *at* http://www.aclu.org/congress/1091800.html (citing H.R. 5018, 106th Cong. (2000)).

147. *Id.* at 2-4.

148. *Id.* at 4-5.

149. *Id.* at 1.

150. *See id.* at 1-5. Privacy advocates were very concerned about a Clinton Administration proposal that called for the implementation of nationwide pen register and trap-and-trace orders, among other things. *Id.* at 5. These concerns may no longer be warranted considering Attorney General Ashcroft's position on this topic. *See infra* text accompanying notes 266-267.

died before the end of the congressional session, and nothing new has been proposed since that time.

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

With the developments in communications technology imposing greater challenges on law enforcement agencies,[151] Congress also recognized the need for increased cooperation between law enforcement officials and telecommunications companies.[152] Although Title III and the ECPA already required telecommunications companies to cooperate with law enforcement officials conducting electronic surveillance, neither act outlined the specific responsibilities of the telecommunications industry.[153] As a result, Congress passed The Communications Assistance for Law Enforcement Act of 1994 ("CALEA"),[154] which was the first statute to impose an "affirmative obligation" on telecommunications companies to modify the design of their equipment and facilities to accommodate law enforcement and facilitate electronic surveillance.[155]

Under CALEA, telecommunications service providers are required to "ensure that their systems are technically capable of enabling law enforcement agencies operating with proper legal authority to intercept individual telephone calls and to obtain certain 'call-identifying information.'"[156] While the final congressional bill did not provide specific technical requirements for compliance, Congress delegated the initial determination of such standards to industry participants.[157]

Recognizing the inevitability of disagreement between the industry and law enforcement officials, Congress determined that the

151. *See* discussion *supra* Part II.A.

152. *See Carnivore and the Fourth Amendment: Statement Before the H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 4 (July 24, 2000) (statement of Robert Corn-Revere, Esq., Hogan & Hartson, LLP) [hereinafter *Corn-Revere's July Testimony*].

153. Nylund, *supra* note 27, at 333. The FBI worried that with increasing competition among the telecommunications companies, it would have a much harder time securing cooperation for surveillance activities unless there was some sort of "universal compliance." *See Corn-Revere's July Testimony*, *supra* note 152, at 4.

154. Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414.

155. *The Fourth Amendment and the Internet: Statement Before the H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. (Apr. 6, 2000) (statement of Robert Corn-Revere, Esq., Hogan & Hartson, LLP) [hereinafter *Corn-Revere's April Testimony*].

156. United States Telecom Ass'n v. FCC, 227 F.3d 450, 453 (D.C. Cir. 2000).

157. *See* Nylund, *supra* note 27, at 335.

Federal Communications Commission ("FCC"), acting as a mediator,[158] would conduct public proceedings to resolve any conflicts.[159] Accordingly, the FCC resolved the challenges to the proposed standards in August of 1999, when it issued its Third Report and Order.[160] In the Third Report and Order, the FCC set out the technical standards required to achieve compliance under CALEA. These standards combined the "J-Standard,"[161] originally advocated by the industry, with six out of nine additional "punch list items" requested by the FBI.[162]

In an effort to invalidate some of these technical standards, including four of the FBI's "punch list items," the telecommunications industry and privacy rights advocates challenged portions of the FCC's Third Report and Order in federal court.[163] These groups argued that the FCC exceeded its statutory authority by "expand[ing] the types of call-identifying information that carriers must make accessible to law enforcement agencies."[164] Deciding the case, the Court of Appeals for the District of Columbia upheld the inclusion of two of the challenged technical requirements[165] and vacated the portions of the FCC's Third Report and Order that required telecommunications companies to implement certain advanced surveillance capabilities.[166] Specifically, the court vacated portions relating to the remaining four "punch list items," and remanded the case to district court.[167] Signaling a victory for privacy advocates, the court ruled that the FCC's inclusion of these four challenged "punch list items" lacked "reasoned decisionmaking."[168]

---

158. *Id.* at 336.

159. *See Corn-Revere's July Testimony*, *supra* note 152, at 5.

160. *In re* Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794 (1999) [hereinafter Third Report and Order]; *see also* Nylund, *supra* note 27, at 336.

161. *United States Telecom Ass'n*, 227 F.3d at 455. The J-Standard, technically known as the Interim Standard/Trial Use Standard J-STD-025, is a document which "outlines the technical features, specifications, and protocols" that are required for telecommunications carriers to make information available to authorized law enforcement agents. *Id.* The Telecommunications Industry Association adopted this standard after two years of negotiations with the FBI. *Id.*

162. *Id.* at 456 (noting that the FBI petitioned the FCC to modify the J-Standard to include nine additional capabilities it deemed necessary for compliance with CALEA); *see also* Nylund, *supra* note 27, at 336.

163. *United States Telecom Ass'n*, 227 F.3d at 457.

164. *Id.* at 453.

165. *Id.* at 464-66.

166. *Id.* at 466.

167. *Id.* at 463.

168. *Id.*

D. The New Challenge: Law Enforcement Reacts to the Growth of Cyber Crime

The Internet transcends local, state and international boundaries, in effect transforming the way we work, play and live on a daily basis. With worldwide Internet usership projected at "250 to 300 million people by the end of the year 2000,"[169] it appears as if the phenomenon often referred to as the "information superhighway" will continue to grow at a rapid pace.

Although the Internet superhighway has revolutionized global communications and commerce, it has also paved a new avenue upon which to conduct criminal activity.[170] In fact, according to the FBI, over the last five years, there has been a "steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet."[171] Acting as a "virtual community,"[172] the Internet allows all of its users, including criminals, to interact in a highly sophisticated manner. Criminals no longer have to rely on communicating over traditional telephone lines, but instead can use computers as instruments to commit crime.[173]

The advent of Internet-related crime has posed a formidable challenge for law enforcement.[174] Not only has such crime complicated the enforcement of old laws and frustrated investigators' ef-

169. *Communities Virtual and Real: Social and Political Dynamics of Law in Cyberspace*, 112 HARV. L. REV. 1586, 1586 n.1 (1999) [hereinafter *Communities*] (citing Donald J. Karl, *State Regulation of Anonymous Internet Use After* ACLU of Georgia v. Miller, 30 ARIZ. ST. L.J. 513, 514 (1998)) .

170. *See* Howard W. Goldstein & Richard A. Izquierdo, *Challenges Posed by Internet Crime*, N.Y. L.J., Sept. 7, 2000, at 5. According to the FBI, computer networks are being utilized to commit new types of crime as well as to "facilitat[e] . . . traditional criminal behavior." *Freeh Testimony*, *supra* note 25; *see also* Schwartz, *supra* note 18 ("All manner of crimes – child pornography, fraud, identity theft, even terrorism – are being perpetrated using the Internet as a tool.").

171. *Internet and Data Interception Capabilities Developed by FBI: Statement Before the H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 5 (July 24, 2000) (statement of Donald M. Kerr, Assistant Laboratory Division, Federal Bureau of Investigation) [hereinafter *Kerr Testimony*]. According to former FBI Director Louis J. Freeh, cybercrime is "one of the fastest evolving areas of criminal behavior and a significant threat to our national and economic security." *Freeh Testimony*, *supra* note 25.

172. *Communities*, *supra* note 169, at 1586.

173. *See generally* Goldstein & Izquierdo, *supra* note 170. The article points out that computers are often: (i) the object of crime; (ii) the subject or site of the crime; and (iii) the instrument used to commit the crime. *Id.* (citing Michael Hatcher et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 401 (1999)).

174. *Freeh Testimony*, *supra* note 25 ("The rapid advance of data technologies and the unregulated nature of the Internet has resulted in a myriad of technologies and protocols which make the interception of data communications extremely difficult.").

forts of coordination, but it has also hindered the detection of criminal activity.[175] It is, therefore, inevitable that law enforcement will continually have to update its crime-fighting techniques to match the technological advancements of the criminal world.[176]

Law enforcement has responded to the growing challenge of computer crime by forming special task forces to investigate cybercrimes,[177] and by broadening the scope of its electronic surveillance activities.[178] Law enforcement has placed a renewed emphasis on the search and seizure of stored computer files and electronic data,[179] and it has also developed new software to monitor the activities of online users.[180] In addition, according to the *1999 Wiretap Report* issued to Congress, there has been a dramatic increase in the number of wiretap authorizations over the past ten years.[181] In fact, from 1998 to 1999 alone, there was a six percent increase in the number of orders issued by federal judges.[182] Furthermore, out

175. *Id.* (noting that advances in technology have "taken a serious toll" on the government's ability to protect its citizens through the use of lawful electronic surveillance); *see also* Goldstein & Izquierdo, *supra* note 170.

176. Robinson, *supra* note 4 (stating that systems such as Carnivore have become more attractive to law enforcement "as the only way that governments can keep up with the technological measures being adopted by criminals, terrorists and opponents"). Recognizing the difficulties in tracking sophisticated criminals, in 2000 the Department of Justice proposed that judges be given the authority to issue pen register and trap and trace orders with nationwide coverage. *See Nojeim Testimony*, *supra* note 108, at 6

177. Bridget G. Brennan, Remarks at Fordham Law School (October 24, 2000).

178. Schwartz, *supra* note 18 ("[A]s the world has gone digital, criminals have as well, and Internet taps are requested in a growing number of cases.").

179. *See* Edward A. Rial & Karen S. Popp, *Search Warrants: Seizing Electronic Data*, NAT'L L.J., Nov. 20, 2000, at B6. The authors point out that computer searches have become more common as law enforcement officials recognize the advantage of obtaining electronic documents. *Id.* Such benefits include: (i) the ability to recover "lost" or "destroyed" documents; (ii) the ability to identify the author of a document, as well as the time and date a document was created; and (iii) the ability to recognize whether a document has been altered by comparing existing documents with previous versions on backup. *Id.* Through standard search warrants, authorities have the ability to search and seize such computer data and/or computer hardware. *Id.*

180. *See generally* King & Bridis, *supra* note 8 (noting that Carnivore, the FBI's new "superfast" system, has the ability to search email to track criminal suspects).

181. LEONIDAS R. MECHAM, ADMIN. OFFICE OF THE U.S. COURTS, 1999 WIRETAP REPORT 5, 7 (2002) [hereinafter 1999 WIRETAP REPORT], *available at* http://www.uscourts.gov/wiretap99. The number of federal authorizations alone has increased by nearly ninety-four percent. *Id.* at 5. Although wiretapping is often used as a last resort, the FBI considers it an essential tool in fighting crime. Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibition on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 477-78 (1994) (citing Dorothy Denning, *To Tap or Not To Tap*, COMM. ACM, Mar. 1993, at 26, 29).

182. 1999 WIRETAP REPORT, *supra* note 181, at 7. Specifically, federal judges authorized 601 applications, while state judges authorized 749. *Id.*

of the total 1,350 wiretap applications applied for in 1999, federal judges authorized all 1,350 of them, representing a one hundred percent approval rate.[183]

In addition to increasing the frequency by which it utilizes traditional surveillance techniques, law enforcement has also developed other highly sophisticated mechanisms to keep pace with the technological capabilities of criminals. One such mechanism, Carnivore, was developed by the FBI in response to the increasing number of investigations in which criminals use the Internet, specifically electronic mail ("email"), to communicate with each other and their victims.[184] Following implementation procedures under the ECPA, Carnivore allows law enforcement to retrieve information associated with a criminal suspect's electronic communication. This system, specifically the breadth of its capabilities, has resulted in a great deal of controversy over the past two years.[185]

Part II provides an in-depth analysis of the Carnivore system and discusses the recent debate raging over its use. Part II continues by highlighting an important consideration in the debate over privacy versus protection. Specifically, it explores the premise that to be worthy of Fourth Amendment protection, individuals must have a legitimate expectation of privacy. This section also discusses recent litigation and statements that, prior to September 11, 2001, signaled a willingness on the part of the courts and the Bush administration to address and possibly remedy privacy concerns. Part II concludes by summarizing how the country's priorities have changed since the events of September 11. This section also highlights the current debate over the constitutionality of the USA Patriot Act, a purported "antiterrorism" bill passed in the aftermath of September 11.

183. *Id.* ("Judges approved all applications."). Ironically, the *1999 Wiretap Report* accurately reflects the evolution of communications technology, citing the electronic wiretap as the most common method of surveillance that year. *Id.* As opposed to telephone wiretaps, which ranked second in utilization, electronic wiretaps constitute surveillance of "digital display pagers, voice pagers, cellular phones, and electronic mail." *Id.* at 10.

184. *Carnivore: Diagnostic Tool*, *supra* note 9.

185. *See Evidence of FBI Evasions Feeds Carnivore Doubts*, USA TODAY, Nov. 30, 2000, at 16A [hereinafter *Evidence of FBI Evasions*].

II. Our Changing World: The Clash Between Technological Advancements and Individual Privacy Rights

A. Carnivore: Friend or Foe?

Carnivore is a software-based system utilized by the FBI to implement judicially authorized surveillance of electronic communications.[186] Installed for the purpose of conducting criminal investigations, Carnivore is a "powerful Internet wiretapping device"[187] that has the ability to search for and retrieve information pertaining to the electronic communications of particular criminal suspects.[188] Carnivore is used when other methods of gathering such evidence "do not meet the needs of investigators or the restrictions placed by the court."[189]

In addition to scanning millions of emails per second,[190] Carnivore is capable of intercepting information regarding instant messaging, Web site access, and chat groups.[191] According to the FBI, Carnivore acts as a "sniffer," looking for specific information coming across an ISP's network.[192] Through the use of Carnivore, agents are able to filter intercepted data "to eliminate material not authorized for capture," and then store the data for review by the FBI and the authorizing court.[193] Because Carnivore is an electronic device installed on the network of an ISP, the FBI relies on the technical assistance and cooperation of ISP personnel in order to conduct its surveillance.[194]

---

186. *Carnivore: Diagnostic Tool*, *supra* note 9.

187. David S. Cloud, *At Justice Department, a Conservative Takeover Looms*, WALL ST. J., Dec. 26, 2000, at A12.

188. John Schwartz, *Wiretapping System Works on Internet, Review Finds*, N.Y. TIMES, Nov. 22, 2000, at A19.

189. ILL. INST. TECH. RESEARCH INST., INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM: DRAFT REPORT viii (2000) [hereinafter INDEPENDENT REVIEW OF CARNIVORE]. For example, Carnivore is used when an Internet Service Provider, through its own software, is unable to provide the FBI with the necessary data. *Id.*

190. King & Bridis, *supra* note 8.

191. Nick Wingfield & Don Clark, *Internet Companies Decry FBI's E-Mail Wiretap Plan*, WALL ST. J., July 12, 2000.

192. *Kerr Testimony*, *supra* note 171, at 4; *see also* Ted Bridis & Neil King, Jr., *Carnivore E-Mail Won't Eat Up Privacy*, WALL ST. J., July 20, 2000, at A28. According to the FBI, Carnivore allows agents "to identify a point through which Internet traffic passes to and from a suspect named in a court order. The data is copied at that access point, filtered . . . [and] stored for review." Schwartz, *supra* note 18.

193. Schwartz, *supra* note 18.

194. *Kerr Testimony*, *supra* note 171, at 5. The FBI uses a special team of technical agents to install and configure the equipment to comply with the collection restric-

Initially conceived under the name "Omnivore" in 1997, the introduction of Carnivore served as a technological update which came into effect in June 1999.[195] Although Carnivore is nearly three years old, until recently many people did not know of its existence. In fact, the Carnivore system had been a well-kept secret until its capabilities became widely reported in the press.[196]

After the initial reports on Carnivore sparked enormous interest by the news media, Carnivore quickly became an "issue of major public concern," prompting the Electronic Privacy Information Center ("EPIC") to file a Freedom of Information Act ("FOIA") lawsuit against the FBI.[197] This lawsuit sought to obtain FBI documents delineating Carnivore's source code, to assure privacy groups that the system's capabilities could not go beyond their advertised reach.[198] The EPIC's document request was subsequently granted, and on August 2, 2000, Judge Robertson of the United States District Court for the District of Columbia ordered the FBI to set a schedule for the release of such documents.[199] Although

---

tions set forth in the court order. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at viii.

195. Press Release, Electronic Privacy Information Center, FBI Releases Carnivore Documents to EPIC: Privacy Group Says Disclosure Insufficient (Oct. 2, 2000) [hereinafter EPIC October Press Release], *at* http://www.epic.org/privacy/carnivore.

196. *See* Electronic Privacy Information Center, *The Carnivore FOIA Litigation*, Hot Topics: Carnivore [hereinafter *Carnivore FOIA Litigation*], *at* http://www.epic.org/privacy/carnivore (last visited Apr. 6, 2002). Although Robert Corn-Revere provided testimony regarding Carnivore in April of 2000, it was not until mid-July 2000 that the press picked up the story. *Biting Into Carnivore*, *supra* note 13, at E3. In fact, according to the Washington Post, even White House Chief of Staff John D. Podesta was "unaware" that the FBI was in the process of developing the Carnivore system until he read reports in the news media. John F. Harris & David A. Vice, *With Freeh, Mistrust Was Mutual; Relations Soured Over FBI's Role: For or Against Administration?*, WASH. POST, Jan. 10, 2001, at A1.

197. *Carnivore FOIA Litigation*, *supra* note 196; *see also* Nick Wingfield, *ACLU Asks Details on FBI's New Plan to Monitor the Web*, WALL ST. J., July 17, 2000, at B7 (stating that the ACLU also filed a FOIA request, yet, unlike the situation with the EPIC, no lawsuit ensued). It was not until the FOIA Amendments were passed in 1974 that FBI files became accessible to the public. Despite the increased accessibility, however, the FBI was subject to a number of exceptions and, therefore, was not required to produce "classified information, information that might reveal FBI sources or methods, and information that might violate the privacy rights of individuals referenced in FBI records." FBI REFERENCE GUIDE, *supra* note 32, at ix.

198. *See* Timothy W. Maier & Michael Rust, *FBI Unleashes Carnivore To Spy on American's E-Mail*, 16 INSIGHT MAG., Aug. 14, 2000, at 6.

199. *Carnivore FOIA Litigation*, *supra* note 196.

these disclosures were ultimately made,[200] a large number of documents were produced in completely redacted form.[201]

Since the initial disclosure of documents by the FBI in 2000, the parties have continued to argue over whether the FBI conducted an adequate search for responsive documents.[202] In response to numerous motions by both parties, on March 25, 2002, the court ordered the FBI to conduct an additional search of their records.[203]

In addition to the concern exhibited by privacy groups, news of Carnivore's capabilities also worried members of Congress.[204] As a result, FBI officials were called to Capitol Hill to explain the system to congressional leaders.[205] Yet, despite the FBI's assurances that surveillance would be conducted within legal limits, many members of Congress remained skeptical, finding it hard to accept the FBI's assurances without definitive proof.[206]

The most significant concern of privacy groups and Congress is that Carnivore invades the privacy rights of innocent Internet users by allowing "excessive monitoring of online communications."[207] Critics of Carnivore argue that in order for Carnivore to intercept the targeted individual's electronic messages, the system must analyze and filter *all* email transmitted over the ISP network.[208] Un-

200. The FBI disclosed approximately 1665 pages worth of documents. Elec. Privacy Info. Ctr. v. Dep't of Justice, No. 00-1849 (D.D.C. Mar. 25, 2002).

201. EPIC October Press Release, *supra* note 195. The FBI has opposed the public disclosure of Carnivore's operating system for arguably legitimate reasons. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at xiv. According to the report issued by the Illinois Institute of Technology, exposing Carnivore's technical limitations could compromise the system, allowing criminals to circumvent its surveillance capabilities. *Id.*; *see also* Ted Bridis, *Carnivore Review Still Doesn't Ease Privacy Concerns*, WALL ST. J., Dec. 5, 2000, at B6.

202. *Biting Into Carnivore*, *supra* note 13; *Carnivore FOIA Litigation*, *supra* note 196.

203. *Elec. Privacy Info. Ctr. v. Dep't of Justice*, No. 00-1849 (D.D.C. Mar. 25, 2002) (agreeing with the EPIC that the FBI did not conduct an adequate search for responsive documents); *Biting Into Carnivore*, *supra* note 13 (noting that the ordered search must be completed by May 24, 2002); *Carnivore FOIA Litigation*, *supra* note 196.

204. Joel Cohen, *How Far Will Computer Monitoring Go?*, N.Y. L.J., Dec. 28, 2001, at 1 (noting that even Republican conservatives such as Dick Armey, the House Majority leader, disapproved of Carnivore when its use was first made public); *see also* Letter from John Collingwood, Assistant Director, FBI Office of Public and Congressional Affairs, to Members of Congress on Carnivore Diagnostic Tool (Aug. 16, 2000), *at* http://www.fbi.gov/congress/congress00/collingwood081600.html (responding to inquiries made to the FBI's offices).

205. *See* Elisabeth Frater, *Law Enforcement: The Carnivore Question*, NAT'L L.J., Sept. 2, 2000, at Technology.

206. *See id.*

207. Wingfield & Clark, *supra* note 191.

208. *See* King & Bridis, *supra* note 8; Maier & Rust, *supra* note 198.

willing to rely on the FBI's assurances, privacy groups have expressed a great concern over the breadth of Carnivore's capabilities.[209] This is especially true in light of the disclosure of an internal FBI memorandum obtained by way of the EPIC's FOIA request.[210] According to this document, tests conducted on Carnivore prove that it can "reliably capture and archive *all* traffic through an Internet service provider."[211] This suggests that, in addition to targeting the communications of a specific individual, the FBI could intercept the communications of innocent Internet users. Furthermore, privacy groups are concerned about the apparent lack of accountability associated with Carnivore,[212] and argue that law enforcement should be required to meet much tougher, uniform standards to conduct such surveillance.[213]

According to the FBI, Carnivore does not pose a threat to individual privacy.[214] Rather, Carnivore actually enhances privacy rights by allowing law enforcement to apprehend cyber criminals who pose a threat to the security of all.[215] The FBI maintains that Carnivore only gives law enforcement the ability to intercept and collect electronic communications from individuals being investigated subject to a court order.[216] Specifically, the FBI asserts that Carnivore has the "surgical ability to intercept and collect the communications which are the subject of [a] lawful [court] order while ignoring those communications which they are not authorized to

209. *See* Wingfield & Clark, *supra* note 191.

210. Schwartz, *supra* note 188.

211. *Id.* (quoting the FBI memorandum) (emphasis added); *see also* Dan Eggen & David A. Vise, *More Questions Surface About FBI Software; Wiretap Program Can Archive All Internet Communications*, WASH. POST, Nov. 18, 2000, at A03 (reporting test results concluding that Carnivore can "retrieve all communications passing through an Internet provider, not just those connected to a criminal suspect"). The publication of this memo has led many privacy advocates to accuse the FBI of misleading the public. *Id.*

212. *See infra* text accompanying notes 228-230, 232 and accompanying text.

213. *See* Frater, *supra* note 205. According to Barry Steinhardt, Associate Director of the ACLU, one way in which law enforcement implements Carnivore is through a pen register or trap-and-trace order, which requires a much lower standard. *The Fourth Amendment and Carnivore: Statement Before the H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 2 (July 24, 2000) (statement of Barry Steinhardt, Associate Director, ACLU). For a discussion of the required standard for implementing a pen register or trap-and-trace devise, see *supra* notes 127-135 and accompanying text.

214. *See* Frater, *supra* note 205.

215. *Id.*

216. *Earthlink, FBI Agree to Drop Internet Surveillance Device*, FLA. TIMES-UNION, July 15, 2000, at B2.

intercept."[217] The FBI also claims that, similar to a pen register or trap-and-trace device, Carnivore only intercepts the identifying information of electronic communications, without scanning the content or even the subject line of the email.[218] This assertion has allowed the FBI to implement Carnivore under the less-restrictive rules of the ECPA, rather than through compliance with the more stringent Title III standard of probable cause.[219] Furthermore, in addition to being authorized only through a strict court order, the FBI maintains that Carnivore's use is limited, having been used in only twenty-five investigations in the past eighteen months.[220]

Amid the growing controversy in the summer of 2000, former Attorney General Janet Reno announced plans to disclose the technical specifications of Carnivore. Such disclosures would be made to a select "group of experts" who would conduct an independent review to determine the exact capabilities of the system, while at the same time dispel public concern.[221] This review was conducted by the Illinois Institute of Technology's Research Institute, which issued its initial report on November 17, 2000.

According to the report, Carnivore functions in a way that is consistent with the FBI's initial explanation.[222] The report concludes that the installation and operation of Carnivore pose no op-

---

217. *Carnivore: Diagnostic Tool*, *supra* note 9.

218. *See* Frater, *supra* note 205; Schwartz, *supra* note 11.

219. Schwartz, *supra* note 11. According to the independent report, Carnivore can be implemented either under Title III (when the FBI seeks to capture content) or under the ECPA rules for pen register or trap-and-trace devices. Officials at the Department of Justice admitted, however, that "the system has been used, in most cases, under the less-restrictive [ECPA] rules." *Id.* It is important to note that The USA Patriot Act, (*see* discussion *infra* Part II.C.), now specifically authorizes the implementation of Carnivore under the less-restrictive standards commonly used for pen registers and trap-and-trace devices. This standard is less restrictive because it does not require a showing of probable cause; rather, law enforcement must certify that the information is "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2) (2000). For a comparison of the legal requirements necessary to implement Title III and ECPA devices, see discussion *supra* notes 88-106, 127-142.

220. Bridis & King, *supra* note 192. In fact, current FBI Director Robert Mueller recently stated that the use of Carnivore has "diminished substantially" because ISPs have developed more sophisticated technology to independently monitor their customers' online activities. Ted Bridis, *FBI Still Stuck on the Source of Anthrax*, AP ONLINE NEWS SERV., Mar. 1, 2002.

221. Press Release, Electronic Privacy Information Center, Lawsuit Seeks Immediate Release of FBI Carnivore Documents (Aug. 2, 2000), *at* http://www.epic.org. Many, however, question the independence of the review panel, complaining that it is pro-law enforcement. Eggen & Vise, *supra* note 211, at A03.

222. Schwartz, *supra* note 188.

erational or security risks to an ISP's network.[223] The report also concludes that Carnivore's technology can be a more effective means of privacy protection and lawful surveillance, and that there is an appropriate system of checks and balances in place.[224] In addition, the report states that Carnivore does not monitor the online activities and downloading preferences of every ISP customer.[225]

Despite these conclusions, critics of the system are still not satisfied.[226] Citing the report's acknowledgement of Carnivore's deficiencies, critics interpret the report as a confirmation of the system's threat to privacy.[227] Specifically, critics point to the report's conclusion that, although Carnivore's operational procedures appear sound, the system "does not provide protections, especially audit functions, commensurate with the level of the risks."[228] Moreover, Carnivore is deficient in its ability to protect the integrity of the data it collects,[229] and the system cannot eliminate the risk of unauthorized acquisition, both intentional and unintentional, of electronic communications by law enforcement agents.[230] In addition, the report validates the concerns of privacy groups, noting that the system is capable of conducting broad searches that would allow the FBI to "record any traffic it monitors."[231] The report also offers proposals for how the system could be improved, suggesting that more could be done to better

223. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at xii. Yet, this assertion remains uncertain, considering the technical difficulties experienced by Earthlink after Carnivore was installed on its network. *See infra* notes 237-238 and accompanying text.

224. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at xii-xiii.

225. *Id.* at xiii.

226. Groups such as the ACLU and EPIC emphasize that the review failed to provide the necessary public discourse about Carnivore, a system which poses a "serious threat to individual liberties." Press Release, ACLU, ACLU and EPIC Say Further Study of Carnivore Review Proves "Beast Must Be Tamed" (Dec. 1, 2000), *at* http://www.aclu.org/news/2000/n120100.html.

227. *Evidence of FBI Evasions*, *supra* note 185.

228. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at xii. In fact, computer security experts who analyzed the independent report concluded that "[s]erious technical questions remain about the ability of Carnivore to satisfy its requirements for security, safety and soundness." Schwartz, *supra* note 11.

229. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at xiii; *see also* David A. Vise & Dan Eggen, *Study: FBI Tool Needs Honing; Panel Says 'Carnivore' Software Can Be Altered To Protect Rights*, WASH. POST, Nov. 22, 2000, at A2.

230. INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at xi.

231. *Id.* at xiii. Although the report notes that the system records only the packet segments that fall within certain specifications, it states that Carnivore is a "tool used to examine all Internet Protocol packets on an Ethernet." *Id.*

safeguard privacy from flaws in "human and organizational controls."[232]

Accordingly, critics cite the report as proof that: (1) the FBI misled the public with respect to the assurances they made about Carnivore; and (2) Carnivore's "supposed" safeguards are impossible to enforce.[233] In addition, critics argue that Carnivore may not be as useful as it had originally been portrayed, considering the increasing availability of encryption software to would-be criminals.[234]

In light of the independent review and the lingering controversy, Carnivore's fate is seemingly unclear. To date, there have only been a handful of legal challenges by ISPs resisting the installation of Carnivore, and because of the secrecy of the related investigations, these decisions have remained under seal.[235] One such case involved the ISP Earthlink. Earlier this year, Earthlink challenged a court order requiring it to install Carnivore.[236] Despite the company's concerns over the privacy and security of its network, a federal magistrate judge ruled against Earthlink, compelling the company to install the surveillance device.[237] Because Carnivore was not compatible with Earthlink's software, the company was forced to operate from an older version, thus causing its network to crash.[238] As a result, Earthlink refused to make any further installations, ultimately reaching an agreement with the FBI where, in the future, the company would use its own software to collect data.[239]

B. The Decline of a Legitimate Expectation of Privacy in the Internet Age

An important consideration in the growing debate over privacy versus protection is whether individuals actually have a legitimate expectation of privacy with respect to Internet use and communica-

232. Schwartz, *supra* note 188.

233. *Evidence of FBI Evasions*, *supra* note 185. The article points out that it is impossible to subject employees who misuse Carnivore to criminal prosecution, because all Carnivore users share the same logon code. *Id.*

234. *Id.* (noting the ITT report's revelation that encryption software can "foil" Carnivore's system).

235. King & Bridis, *supra* note 8.

236. *See id.*

237. *Id.*

238. Nick Wingfield et al., *Earthlink Says It Won't Install Device For FBI*, WALL ST. J., July 14, 2000, at A16.

239. *Earthlink, FBI Agree to Drop Internet Surveillance Device*, *supra* note 216.

tions.[240] Without such expectations, there is far less validity in the arguments that the Fourth Amendment is being violated or that privacy rights are being infringed.[241] According to Robert Corn-Revere, "The Internet revolution has altered the calculus for what may be considered a reasonable expectation of privacy."[242] This statement is an accurate reflection of the Internet's influence on privacy rights, and supports the argument that privacy expectations have eroded with increased Internet use. This argument is based on many Internet users' suspicions that their computer transactions may not be secure.[243]

Recognizing the technological capabilities associated with the proliferation of Internet use, it is unrealistic to believe that an individual's expectation of online privacy exceeds or even equals their expectation of privacy within their own home. Rather, the framework of the Internet poses unique security issues. Not only are Internet users reminded throughout the course of their online session that they are utilizing an unsecured connection, but they are often asked whether they are willing to continue their transaction under these circumstances. A user's willingness to proceed, over what are clearly unsecured lines, signals an affirmative recognition of the privacy risks associated with online use.

Another indicator of the decline in privacy expectations associated with the advent and proliferation of the Internet is the wide array of tracking software available to companies and individual citizens. For example, through the use of devices known as "cookies," advertisers and marketing companies can target the individual

240. *See supra* note 132 and accompanying text; *see also infra* text accompanying notes 249-255.

241. *See supra* notes 51 & 132 and *infra* notes 248-51 and accompanying text. Although the FBI, in its defense of Carnivore, has yet to argue that Internet users have no legitimate expectation of privacy, this expectation has been a factor in the Supreme Court's consideration of how far to extend Fourth Amendment protection. *See supra* text accompanying note 132. Therefore, because the use of Carnivore has ignited a fierce debate about privacy rights that may ultimately be decided by the courts, it is important to examine case precedent on privacy expectations involving Internet use.

242. *Electronic Privacy: Statement Before the H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 2 (Sept. 6, 2000) (statement of Robert Corn-Revere, Esq., Hogan & Hartson, LLP).

243. *See* Cohen, *supra* note 204 (noting that most corporate employees are aware of the probability that their email communications and visits to Internet sites are monitored and stored). The realization that the communications sent over a computer network may be less secure is especially apparent in the wake of the terrorist attacks on September 11, 2001. In response to the attacks, Congress has made it easier for law enforcement to conduct such electronic surveillance. *See infra* Part II.D.

preferences of Internet users by tracking their activity while online.[244] Also, email users can now purchase software that provides notification when the messages they have sent are opened by the intended recipient, or even forwarded to a third party.[245] In addition, many employers have installed software called "Superscout" on their networks, which enables them to track an employee's email and Internet activities.[246] Through the use of this software, companies are now starting to fire employees for surfing the net on company time, in what has been dubbed "cyber-loafing."[247]

Unfortunately for employees concerned with their privacy rights, the courts have sided with employers, holding that "office practices, procedures, or regulations may reduce legitimate privacy expectations."[248] According to the Fourth Circuit in *United States v. Simons*, to establish a Fourth Amendment violation, a petitioner has the burden[249] of proving that he has "a legitimate expectation of privacy in the place searched or the item seized."[250] In doing so, a petitioner must show that this "subjective expectation of privacy is one that society is prepared to accept as objectively reasonable."[251]

Courts have also used this standard of "subjective expectation" to determine what protection to afford the personal information that customers voluntarily turn over to their ISPs.[252] For example, in *United States v. Hambrick*, the Western District of Virginia found that the petitioner could not seek Fourth Amendment protection despite the fact that law enforcement relied on an invalid warrant to obtain personal information from his ISP.[253] Pointing out that individuals have no legitimate expectation of privacy with

244. Amy Harmon, *Software That Tracks E-Mail Is Raising Privacy Concerns*, N.Y. TIMES, Nov. 22, 2000, at A1.

245. *Id.*

246. Maier & Rust, *supra* note 198.

247. *Id.*

248. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000), *cert. denied*, 122 S. Ct. 292 (2001). The court concluded that the warrantless search and seizure of Simons' computer files did not constitute a Fourth Amendment violation because, based on his employer's policy, he lacked a legitimate expectation of privacy. *Id.*

249. *Id.* at 400.

250. *Id.* at 398 (citing Rakas v. Illinois, 439 U.S. 128, 143 (1978)).

251. *Id.* (citing California v. Greenwood, 486 U.S. 35, 39 (1988)).

252. *See* United States v. Hambrick, 55 F. Supp. 504, 506 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

253. *Id.* at 506-09.

regard to information voluntarily turned over to third parties,[254] the court refused to suppress the evidence obtained.[255]

C. Recent Litigation and Shifting Partisan Policies Send a Positive Signal to Privacy Advocates Prior to September 11, 2001

Recent decisions have reinforced the limitations of Fourth Amendment protection by holding that individuals must prove a legitimate expectation of privacy to have a valid claim. Nevertheless, the courts have signaled a willingness to control the authority of law enforcement by making it more accountable for its surveillance activities. For example, the District Court for the District of Columbia granted the EPIC's initial document request under the FIA.[256] The court rejected the FBI's efforts to delay the production of documents relating to Carnivore, instead requiring them to set a schedule for immediate disclosure.[257] Furthermore, the district court recently granted a renewed request for responsive documents by the EPIC, holding that the FBI's initial production did not represent an adequate search.[258]

Another illustration of the courts' willingness to control law enforcement's authority, with respect to electronic surveillance technology, is *United States Telecom Association v. FCC.* In this case, the Court of Appeals for the District of Columbia criticized the FCC's inclusion of four of the "punch list items" proposed by the FBI, finding the FCC's decision defective.[259] This decision effectively limited the FBI's control over the telecommunications industry.

However, *United States Telecom Association v. FCC* is also significant because, in its opinion, the court clearly stated, "CALEA does not cover 'information services' such as email and [I]nternet

254. *Id.* at 508 (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979)). The court also pointed out that there is no reason to believe that the ECPA intended for there to be a reasonable expectation of privacy with regard to a person's "name, address, social security number, credit card number, and proof of Internet connection." *Id.*

255. *Id.* at 509.

256. *Carnivore FOIA Litigation*, *supra* note 196. For additional discussion, see *supra* text accompanying notes 197-199.

257. *Carnivore FOIA Litigation*, *supra* note 196. *See supra* text accompanying note 199.

258. *Carnivore FOIA Litigation*, *supra* note 196. *See supra* text accompanying notes 202-203.

259. United States Telecom Ass'n v. FCC, 227 F.3d 450, 461 (D.C. Cir. 2000). *See supra* note 162 and accompanying text.

access."[260] This statement suggests that, unlike telecommunications companies, ISPs may not have to make their systems compliant with the surveillance technology of law enforcement agencies. Also, the recent Earthlink litigation[261] proves that it may not even be necessary to install Carnivore on the networks of ISPs, since most ISPs have their own surveillance capabilities.[262] These factors, along with independent study results that cast doubt on Carnivore's ability to safeguard privacy,[263] may ultimately make it easier for ISPs to challenge court orders mandating the installation of Carnivore on their networks. ISPs can argue that CALEA was never intended to require compliance by online communications networks, therefore the installation of Carnivore is not necessary. They can also argue that the privacy expectations of their customers require law enforcement to meet higher standards to justify the installation of surveillance devices on their networks.

In addition to the above factors suggesting the courts may favor a more limited scope for Carnivore, it also seems likely that had the events of September 11 never happened, our government's priorities would continue to reflect a balance between privacy and protection, rather than an uncompromising focus on security at any cost.[264] In fact, prior to September 2001, it seemed likely that both Congress and the Bush Administration were willing to consider a legislative solution to privacy concerns.[265] Specifically, observers note that Attorney General John Ashcroft, at one time, may have supported legislation restricting law enforcement's power of surveillance in favor of increased privacy rights for individuals and businesses.[266] During his time in the Senate, Mr. Ashcroft supported efforts by businesses to encrypt their communications as well as efforts by privacy groups seeking to curb the government's

260. *United States Telecom Ass'n*, 227 F.3d at 455 (quoting 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A) 2000). The court pointed out that in enacting CALEA, Congress intended on "preserv[ing] the status quo" by giving law enforcement "no more and no less access to information than it had in the past." *Id.* at 455 (quoting H.R. REP. No. 103-827, pt.1, at 22 (1994)).

261. *See supra* notes 237-239 and accompanying text.

262. Bridis, *supra* note 220 (quoting FBI Director Robert Mueller).

263. *See* text accompanying notes 226-232.

264. *See infra* Part II.D.

265. For a discussion of the privacy concerns of both members of Congress and members of the Bush Administration, see *supra* notes 204-206 and *infra* notes 266-268.

266. Cloud, *supra* note 187. Although prior to September 2001, Attorney General Ashcroft had never criticized Carnivore specifically, his record in the Senate was critical of privacy intrusions by the government. Schwartz, *supra* note 18.

power to conduct wiretaps on the Internet.[267] The Republican leadership in Congress also displayed strong resistance to Carnivore when the news reports surfaced last summer, suggesting that Carnivore should be shut down until the privacy concerns were addressed.[268]

D. Changing Priorities in the Wake of a National Tragedy: The Introduction of the USA Patriot Act

Despite the continued concerns of many privacy advocates and members of Congress over surveillance tools such as Carnivore,[269] the events of September 11, 2001 have dramatically changed the nation's priorities.[270] Specifically, just six months after the terrorist attacks, "high-tech tools that once were considered too intrusive are becoming part of everyday life in America."[271] Rather than worrying about a potential intrusion on their civil liberties, many American citizens are more concerned with feeling "a sense of safety."[272]

In response to these shifting priorities, the Bush Administration quickly devised numerous antiterrorism measures to strengthen the power of federal law enforcement and bolster the confidence of the American public.[273] Specifically, within days of the terrorist attacks, Attorney General John Ashcroft began pressuring Congress to adopt legislation that would expand the surveillance power of law enforcement.[274] By October 26, 2001, the Bush Administration had signed into law a new antiterrorism bill entitled, "Uniting and Strengthening America by Providing Appropriate Tools Required

267. Cloud, *supra* note 187.

268. Schwartz, *supra* note 18. Republican leaders are concerned that the invasive nature of the technology allows government to infringe on basic constitutional rights. *Id.*; Cohen, *supra* note 204.

269. *See* discussion *infra* notes 279-287, 290 and accompanying text.

270. Pogue, *supra* note 6 (noting the general change in priorities among many Americans, and suggesting that, in the aftermath of September 11, 2001, Americans may be more willing to sacrifice their privacy rights in exchange for greater security).

271. Balint, *supra* note 6 (comparing Americans' attitudes towards electronic surveillance today with those they held prior to September 11, 2001).

272. *Id.* While many Americans were "increasingly wary of privacy invasions by companies or by the government" prior to September 11, 2001, security concerns are now paramount. Guernsey, *supra* note 7. The author compares the events of September 11, 2001 to national crises of the past, noting that Americans have often been willing to "sacrifice some privacy in the name of security." *Id.*

273. *Id.*

274. *Id.*; Pogue, *supra* note 6.

to Intercept and Obstruct Terrorism Act of 2001" ("The USA Patriot Act").[275]

The USA Patriot Act has made it easier for law enforcement to monitor the activities and communications of Internet users.[276] The USA Patriot Act specifically authorizes the monitoring of electronic communications under the less-stringent standards of the ECPA.[277] Specifically, The USA Patriot Act allows Internet-based communications to be intercepted using the same implementation procedures as a pen register or trap-and-trace device.[278] As a result, the use of tools such as Carnivore will only require the government showing "that the information likely to be obtained is relevant to an ongoing criminal investigation."[279]

Although the Bush Administration claims that the expansion of electronic surveillance capabilities under the USA Patriot Act is a necessary tool in the war against terrorism, there are many Americans who disagree.[280] For example, many critics argue that the Bush Administration's antiterrorism legislation was enacted too expeditiously and without regard to proper procedure.[281] According to media reports, it took the Senate a mere thirty minutes to expand federal wiretap laws in the wake of September 11.[282] Avoiding the usual procedures of debate and amendment, Congress essentially accepted the legislation on a mandate from the executive branch, leaving many privacy advocates wary that the

275. The USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); Robinson, *supra* note 4.

276. Balint, *supra* note 6.

277. Guernsey, *supra* note 7 (stating that Ashcroft had proposed that the words "electronic communications" be added to existing telephone surveillance laws); Anna Kandra, *National Security vs. Online Privacy: The New Anti-Terrorism Law Steps Up Electronic Surveillance of the Internet*, PC WORLD, Jan. 1, 2002. The existing telephone surveillance laws, namely pen registers and trap-and-trace devices, are currently authorized under the ECPA. *See supra* text accompanying notes 118-124 for the necessary implementation requirements.

278. Kandra, *supra* note 277.

279. 18 U.S.C. § 3122(b)(2) (2001); *see also supra* notes 133-135 and accompanying text.

280. Robinson, *supra* note 4 (noting how the debate over privacy versus protection has been revived since September 11, 2001); *see also* Kara Swisher, *Boom Town: Will the Hunt for Terrorists Target Privacy?*, WALL ST. J., Sept. 24, 2001, at B1 (noting the policy efforts being made by privacy advocates to ensure the civil liberties of online users in the wake of new antiterrorism legislation).

281. Robinson, *supra* note 4 ("[I]n the race to protect the public from terrorist activity, essential values such as freedom of expression and the right to communicate without fear of eavesdropping are being ignored.").

282. Swisher, *supra* note 280.

constitutional safeguard of checks and balances had been disregarded.[283]

Many privacy advocates also criticize The USA Patriot Act because it implicitly authorizes the use of surveillance tools such as Carnivore to intercept electronic communications, yet conditions the implementation on a less stringent standard.[284] Privacy advocates from the American Civil Liberties Union are quick to point out that they do not necessarily oppose the idea that law enforcement should have access to such information. They do believe, however, that law enforcement should have to meet higher standards to access that information.[285]

Questions have also surfaced about how effective increased electronic surveillance will be in preventing crime and future terrorist attacks.[286] Specifically, some critics argue that electronic surveillance is only effective if there are enough law enforcement agents to sift through it for analysis.[287] In addition, many security experts agree that electronic surveillance should not become a substitute for hands-on intelligence gathering by live agents working in the field.[288]

III. PUTTING THE LEASH ON LAW ENFORCEMENT: CARNIVORE SHOULD BE SUBJECT TO TITLE III SCRUTINY

A. Congress Must Reevaluate the Law and Extend Title III Protections

The proliferation in communications technology has not only changed the way people conduct their daily lives, but it has also changed the way that law enforcement investigates criminal activity. These technological advancements pose great challenges to the competing interests of privacy advocates and law enforcement, as the existing legal rules are being stretched beyond their limits.

---

283. Cohen, *supra* note 204.

284. The USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). *See supra* notes 277-279 and accompanying text.

285. Guernsey, *supra* note 7 (asserting that Carnivore is capable of intercepting the content of communications, and therefore, the stricter standards of Title III should apply).

286. Ted Bridis & Gary Fields, *Fight Over Civil Liberties*, WALL ST. J., Sept. 26, 2001, at A1 ("[E]xpanding surveillance authority doesn't necessarily lead to more effective law enforcement."); Guernsey, *supra* note 7 (suggesting that there is such a thing as "too much surveillance").

287. Bridis & Fields, *supra* note 286.

288. Guernsey, *supra* note 7.

The concern over electronic surveillance, and specifically Carnivore, is not limited to privacy advocates and concerned citizens. Rather, the drafting of House Bill 5018 and the hearings on Carnivore, before the House Subcommittee on the Constitution, signal Congress's concern as well.[289] Specifically, members of Congress are concerned that Carnivore allows the government to infringe upon Americans' "basic constitutional protection against unwarranted search and seizure."[290] Even though the debate in Congress has stalled since September 11, and The USA Patriot Act passed with overwhelming support, some members of Congress have not been deterred from expressing their continued concern.[291]

Considering the strong debate sparked by the introduction of Carnivore, Congress should respond by repealing portions of The USA Patriot Act and amending existing wiretap laws. While Congress cannot and should not ignore the fact that electronic surveillance is a necessary means of crime prevention, it must not sacrifice fundamental civil liberties. Congress must recognize that current implementation procedures for Carnivore are effectively allowing law enforcement to evade the very safeguards that federal wiretap legislation was designed to ensure.[292] While the FBI has always had the ability to intercept communications that fall outside the scope of its warrants, the exclusionary rule and disciplinary measures under Title III have served as a deterrent from law enforcement officials engaging in unauthorized activity.[293] More importantly, these safeguards have served as a protection mechanism against governmental abuse.[294] By not extending these safeguards to cover electronic communications,[295] the government is asking individuals to trust the FBI and other government intelligence agencies, without providing any protection in return. In ef-

289. *See* Congressional Statements, FBI Press Room, *at* http://www.fbi.gov (last visited Apr. 15, 2002); *supra* Part II.A.

290. Schwartz, *supra* note 18.

291. *See EPIC Alert*, Electronic Privacy Communication Center, *at* http://www.epic.org (Vol. 8.20 dated Oct. 12, 2001) (referring to unsuccessful protests mounted by various senators prior to the passage of The USA Patriot Act); *see also* Madanmohan Rao, *Technology: Creating a Smart and Secure Cyberspace*, INTER PRESS SERV., Mar. 25, 2002 (quoting United States Congressman Bob Barr who still feels that "effective oversight mechanisms" are necessary particularly with respect to Carnivore).

292. *See supra* Part I.B.

293. *See supra* notes 102-104 and accompanying text.

294. *See supra* notes 105-106 and accompanying text.

295. *See supra* text accompanying notes 136-142.

fect, the government is asking Americans to put their faith in a system with a history of corruption.[296]

Accordingly, as it has done so many times in the past, Congress must reevaluate the delicate balance between the privacy interests of the public and law enforcement, and recognize that the wiretap laws, as currently written, no longer provide adequate safeguards for privacy. Congress must adopt stricter and more uniform standards with regard to electronic surveillance to ensure that the protection of privacy rights remains a national priority.

Carnivore should not be treated as a mere pen register.[297] Despite the FBI's claims that Carnivore only intercepts the identifying information of a particular person's incoming or outgoing email, both the FBI's own internal document and an independent report contradict this assertion.[298] Carnivore goes beyond the traditional scope of what pen register devices were developed to intercept,[299] as it can search the actual contents of communications on an ISP's network, rather than just the mere identifying information associated with a criminal suspect's email address. Some have argued that Carnivore cannot be compared to a pen register because knowledge of a suspect's email address is much more intrusive and may reveal more about a person's identity than a phone number can.[300] Because the breadth of Carnivore's capabilities far exceeds that of a pen register, Carnivore should neither be compared to such a limited device, nor authorized under a pen register's weakened standard.[301]

In short, Congress must require that the authorization procedure for the use of Carnivore conform to the strict requirements of Title III.[302] For example, any new legislation should make it clear that for law enforcement agents to use devices like Carnivore, they must comply with the particularity and minimization requirements set forth in Title III.[303] Any interceptions that fall outside of the targeted communications must be considered unauthorized, and

296. *See supra* text accompanying notes 79-84.

297. *See supra* notes 277-278 and accompanying text.

298. *See supra* text accompanying notes 210-211, 229-231.

299. Specifically, pen registers and trap-and-trace devices were intended to intercept mere identifying information, namely telephone numbers being dialed into and out of a particular telephone receiver. *See supra* text accompanying notes 128-129.

300. Ted Bridis, *FBI's E-mail Suggests Divisions on Legality of Web Surveillance*, WALL ST. J., Dec. 7, 2000, at B9. These attorneys argue, as a result, that email addresses should be afforded more privacy protections than telephone numbers. *Id.*

301. For a discussion on this standard, see *supra* notes 133-135.

302. *See supra* notes 85-106 and accompanying text.

303. *See supra* notes 89-93, 100-101 and accompanying text.

therefore off-limits for use in a criminal prosecution.[304] Also, in order to provide for more accountability, the exclusionary rules under Title III must be extended to cover *all* forms of electronic communication, and law enforcement agents should be required to obtain the approval of senior Justice Department officials before applying for a court order to install Carnivore.[305] In addition, the standards for seizing stored communications must be heightened to require, at minimum, a showing of probable cause.[306]

If Congress is not willing to subject Carnivore to complete Title III scrutiny, it should at least introduce new legislation explicitly stating that pen register and trap-and-trace orders served on ISPs do not authorize access to the content of communications, including the subject lines of electronic mail. If law enforcement agents violate this restriction, they should be subject to the same disciplinary penalties and evidentiary exclusions provided under Title III.[307]

CONCLUSION

As our world continues to advance technologically, scholars predict that the Internet will "begin to seem less separate from our daily lives."[308] As the distinctions between the virtual world and the real world begin to fade, it appears likely that individuals will increasingly demand and legitimately expect the same privacy protection online that they expect in their own homes. As a result, Congress must take affirmative steps to ensure that all means of electronic surveillance comply with the Fourth Amendment and that the implementation of certain devices complies with the strict standards of Title III.

Despite the outcome of the study conducted on Carnivore and the events of September 11, 2001, public outrage over Carnivore's existence and use clearly has not subsided. In fact, the concerns over Carnivore, while originally based on speculation regarding the system's capabilities, may be justified now more than ever.[309] Although the study conducted by the Illinois Institute of Technology's

304. *See supra* note 102 and accompanying text.

305. *See supra* notes 86-87 and accompanying text.

306. *Compare supra* text accompanying notes 120-126, *with* supra text accompanying notes 97-99.

307. *See supra* notes 102-104 and accompanying text.

308. *Communities*, *supra* note 169, at 1596 (citation omitted).

309. Public disclosure of information concerning Carnivore is especially important in the aftermath of September 11, because such investigative techniques are likely to increase in use. *See* Balint, *supra* note 6 ("By all indications, law enforcement agen-

Research Institute concluded that Carnivore performs in many ways as advertised by the FBI, privacy advocates argue that the report's conclusions and recommended improvements[310] demonstrate system deficiencies that undermine privacy protection. Furthermore, it is clear that suspicions will continue to mount until Congress passes legislation that specifically delineates the specific categories of information that devices such as Carnivore may intercept.

Even if the controversy over Carnivore eventually subsides, the legal debate over electronic surveillance will undoubtedly continue for some time. As technological advancements continue to revolutionize the way in which criminals communicate, law enforcement will be forced to develop even more sophisticated means of surveillance.[311] The FBI will no longer be satisfied with the interception of mere identifying information, and will use Carnivore and other devices to intercept the content of electronic communications. This expanded capability will likely draw new criticism from privacy advocates, claiming, once again, that law enforcement has overstepped its authority.

Rather than overburden the courts with continuous litigation seeking to determine whether law enforcement officials have acted within their legal authority, Congress must take the initiative and develop consistent and detailed standards under which electronic surveillance may be conducted. Congress must amend portions of the ECPA to adhere to the more stringent standards of Title III and the Fourth Amendment, and it must extend Title III protection to cover the use of invasive devices such Carnivore. In addition,

---

cies are stepping up their use of technology that can record Internet use, from e-mails to Web surfing to online chats.").

310. *See supra* text accompanying notes 228-232.

311. In fact, the FBI is already in the process of updating Carnivore, a process that will undoubtedly enhance the system's surveillance capabilities. *See* INDEPENDENT REVIEW OF CARNIVORE, *supra* note 189, at vii. Also, in November 2001, the FBI acknowledged the existence of another technologically advanced surveillance system known as "Magic Lantern." Kim Zetter, *New Technologies, Laws Threaten Privacy: The FBI's 'Magic Lantern' Keystroke Logger Could Help Catch Terrorists, But at What Cost to Your Fundamental Rights?*, PC WORLD, Mar. 1, 2002. Although it has not yet been deployed, Magic Lantern is a "virus-like program" that will allow federal agents to capture electronic communications before a user's encryption software kicks in. *Id.* Through manual installation or a simple email, Magic Lantern invades a user's computer and, after activation, allows agents to record the user's keystrokes. Elizabeth Clark, *Illuminating Magic Lantern*, NETWORK MAG., Feb. 1, 2002. In effect, Magic Lantern acts as an enhancement to Carnivore, since the Carnivore system fails when confronted with encrypted files. Robinson, *supra* note 4.

Congress must hold law enforcement accountable for compliance with these standards.

Although the advent and proliferation of the Internet has dramatically altered the traditional privacy expectations of individuals with respect to their online activity, online users should not be penalized for embracing this emerging technology. In choosing to access the information superhighway, to take advantage of the convenience of electronic communication, Internet users should not have to forfeit the most basic principles of the Fourth Amendment. Instead, Congress must take the necessary steps to put an end to this controversy. To reflect our changing times, Congress must adopt detailed laws that will put the privacy concerns of citizens to rest, as well as provide the courts with much needed guidance.