# THE CASE AGAINST CARNIVORE: PREVENTING LAW ENFORCEMENT FROM DEVOURING PRIVACY

PETER J. YOUNG*

## INTRODUCTION

The use of Carnivore, the Federal Bureau of Investigation's (FBI) electronic mail surveillance system,[1] and the more sophisticated surveillance technology that is certain subsequently to be developed,[2] obliterates the already precarious balance between the government's responsibility to provide for public safety through law enforcement and individuals' right to privacy. Carnivore's emergence sparked worldwide debate regarding the legal standards to be applied to the use of such technology. Shaping the debate are intense competing public interests, namely quashing rising rates of cybercrime[3] while upholding privacy rights, at a time when the popularity of conducting personal and business transactions via the Internet is skyrocketing.[4]

The FBI is using statutes originally enacted to govern telephone wiretapping, including Title III of the Omnibus Crime Control and Safe Streets Act of 1968[5]

---

* J.D. Candidate, 2002, Indiana University School of Law—Indianapolis; B.A.A., 1993, Central Michigan University, Mount Pleasant, Michigan; M.A., 1995, Ball State University, Muncie, Indiana.

1. The Wall Street Journal broke the story of the FBI's use of its clandestine electronic surveillance system, bizarrely named "Carnivore," to monitor the electronic mail messages of suspected criminals. Neil King, Jr., *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3. The FBI chose the codename Carnivore because the diagnostic tool "chews all the data on the network, but it only actually eats the information authorized by a court order." Robert Graham, *Carnivore FAQ (Frequently Asked Questions)*, *at* http://www. robertgraham.com/pubs/carnivore-faq.html (Sept. 7, 2000). Adopting a less menacing name for its electronic surveillance system, the FBI began calling Carnivore "FS1000" in 2001. Maria Vogel-Short, *A Collision Course?: Public Safety vs. Civil Liberties*, N.J. LAW.: WKLY. NEWSPAPER, Nov. 5, 2001, at 1.

2. This more sophisticated surveillance technology is reported already to exist. Although its existence is unsubstantiated, "Echelon," the "largest technologically driven spy system ever known," is allegedly being operated by the United States, under the auspices of the National Security Agency, along with Great Britain, Canada, Australia, and New Zealand and accumulates more than three billion telephone, telegraph, radio, satellite, undersea cable, and Internet communications a day. Martin L. Haines, *The Secret Life of Echelon*, 160 N.J.L.J. 395, 395 (2000).

3. *Civil Liberties Groups Blast "Carnivore," Seek Privacy Protections*, ANDREWS EMP. LITIG. REP., Oct. 3, 2000, at 10 [hereinafter *Civil Liberties Groups Blast "Carnivore"*] (citing Kevin V. DeGregory, deputy attorney in the U.S. Justice Department, who reports that the FBI's Internet Fraud Complaint Center is receiving 1200 complaints each week).

4. In 1981, 300 computers had Internet access; in 1993, one million had access; and in January 2000, 72.4 million computers were connected to the Internet. Randall L. Sarosdy, *The Internet Revolution Continues: Responding to the Chaos*, METROPOLITAN CORP. COUNS., Sept. 2000, at 15.

5. *See generally* 18 U.S.C. §§ 2510-2522 (1968) (making wiretapping legal and currently

(Title III), the Foreign Intelligence Surveillance Act (FISA) of 1978,[6] the Electronic Communications Privacy Act (ECPA) of 1986,[7] and the Communications Assistance for Law Enforcement Act (CALEA) of 1994,[8] as justification for extending its authority under these laws to monitor electronic mail communications using Carnivore. These laws are patently inadequate when applied to the Internet medium. New comprehensive legal strategies that limit the government's authority to engage in electronic surveillance in an increasing number of ways without adequate oversight and accountability are imperative if public trust in law enforcement is to be preserved. Existing laws and court decisions on electronic surveillance seem to have been haphazardly initiated or adapted in lieu of enacting more comprehensive laws. These laws and decisions illuminate a confusing set of standards governing the various levels of protection given communications originating from diverse sources.[9]

Determining the circumstances under which Carnivore might be used is but one of many issues surrounding it; a much larger, central issue is whether this kind of electronic surveillance exceeds what the American people want the

---

being used to govern the interception of electronic mail content).

6. *See generally* 50 U.S.C. §§ 1801-1863 (1994 & Supp. V 1999) (permitting federal agents to conduct electronic surveillance where probable cause exists to believe that targeting a foreign power or a foreign power's agent will result in evidence of a crime).

7. *See generally* Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) (extending Title III's privacy protections to cover electronic mail communications and requiring that content data from communications companies be released to the government only upon the government's meeting a probable cause standard; the act further provides that before the government can obtain records of telephone calls made or Internet addresses to which mail was sent, it must demonstrate the relevance of the records to a legitimate criminal investigation).

8. *See generally* Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 and 47 U.S.C.) (giving the government authority to tap more sophisticated, digital telephone wiring and requiring telephone companies, but not ISPs, to modify their networks to accommodate wiretapping equipment).

9. For example, under current laws, the interception of an electronic mail message sent through a cable modem is more stringently protected than a telephone conversation, and significantly less demanding standards exist for capturing records of an individual's outgoing and incoming telephone and Internet communications. *Learning to Live with Big Brother*, J. REC. (Okla. City), Aug. 10, 2000, *available at* 2000 WL 14297544; *see also* 18 U.S.C. § 2515 (1994) (providing aggrieved persons a right to move for suppression of wire or oral, but not electronic communications). Whereas wire and oral communications are afforded the protection of a statutory exclusionary rule, electronic communications may only be able to be suppressed under the judicially crafted "fruit of the poisonous tree" doctrine. *See, e.g.*, United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996) (observing that 18 U.S.C. § 2515 does not apply to electronic communications). *Compare* 18 U.S.C. § 2510(12) (1994) (defining electronic communication), *with* 18 U.S.C. § 2510(1) (1994) (defining wire communication), *and* 18 U.S.C. § 2510(2) (1994) (defining oral communication). *But see, e.g.*, United States v. Smith, 978 F.2d 171, 175 (5th Cir. 1992) (applying 18 U.S.C. § 2515 to electronic communications).

capabilities of their government to be. To the FBI, the utility of Carnivore could not be more apparent—it has created a surveillance tool that undoubtedly increases its ability to effectively reach criminal suspects' communications. However, Carnivore's utility may come at too great a cost to the American people—sacrificing their right to privacy. One thing is clear—the Fourth Amendment,[10] now more than 200 years old, is showing signs of difficulty keeping up with the digital age.

Perhaps Carnivore will not prove to be the intolerable device that citizens regard as excessively offensive to their privacy rights. However, with the growing number of individuals worldwide becoming connected to the Internet every day, and the rapidly increasing technological competencies of law enforcement agencies to monitor the medium, one must constantly question how much invasion is too much.

This Note will introduce the Carnivore system and lay out the issues framing the debate around its use and potential for misuse. These issues necessitate an examination of the national and international explosion in Internet use, evidenced not only by the increased number of individuals connected to the Internet, but also in the kinds of functions in which these users are engaging. The private transactions that Internet users are conducting via the medium suggest that, contrary to some U.S. courts' characterization of Internet users as having a minimal expectation of privacy,[11] and thus expecting a lesser degree of protection from unreasonable searches and seizures, Internet users are expecting more privacy when sharing personal information with third parties online.

The Internet is a medium that transcends geographic boundaries. Therefore, although this Note will briefly detail the development of U.S. law as it relates to electronic surveillance, it will also consider the electronic surveillance practices and laws of other countries, focusing only on a few nations with recently enacted, far-reaching electronic surveillance laws.[12] Taking into account U.S. and international laws and policies, the Note will conclude with recommendations and proposals for transforming what has become an unbalanced policy, one substantially favoring law enforcements' interests, to one in which the integrity of worldwide Internet users' expectation of privacy is irrevocably secured.

---

10. The Fourth Amendment provides that persons' right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, . . . but upon probable cause." U.S. CONST. amend. IV.

11. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *5 (Tex. App. May 28, 1999).

12. For a comprehensive discussion of worldwide privacy protections and surveillance laws, see generally David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1 (1999).

## I. THE CARNIVORE ELECTRONIC MAIL SURVEILLANCE SYSTEM

### *A. Carnivore's Capabilities*

The discovery of the FBI's use of the Carnivore electronic mail surveillance system in July 2000[13] prompted numerous questions from privacy advocates and other interested citizens on the system's capabilities. The answers to those questions, provided by the few Justice Department officials who knew enough about the covert system to reply, exposed the tremendous ramifications that Carnivore can potentially have on privacy rights. The potential for abuse is palpable.

The Carnivore system, after being physically placed on Internet service providers' equipment, reads messages' address information and the subject lines describing their contents and can be programmed to capture this header information, servers and Web sites visited by a particular user, or messages' contents.[14] Despite its presence in their facilities and attachment to their computers, Internet service providers (ISPs) are not given access to the system, making the FBI exclusively knowledgeable of Carnivore's capabilities.[15] Only after the Electronic Privacy Information Center (EPIC) filed a Freedom of Information Act (FOIA) request seeking the FBI's records on the Carnivore system did the Justice Department agree to release the system's technical specifications to a group of non-FBI consultants, although it declined to suspend Carnivore's use until a thorough study could be conducted.[16] In October 2000, as a result of EPIC's FOIA request, the Justice Department released 729 pages of text documenting Carnivore's development, but of those 729 pages, 200 were completely withheld and another 400 were partially redacted.[17] The Justice Department's suppression of the information sought by EPIC led to further criticism of the FBI's seemingly unrestrained use of Carnivore.[18]

The FBI maintains that Carnivore can be programmed to garner only the specific kind of information authorized for seizure by a court order.[19] CALEA requires that before law enforcement officials engage in electronic mail searches, they secure a court order, certifying their belief that records of a suspect's electronic mail activity and other transactional data will be relevant to a

---

13. King, *supra* note 1.

14. D. Ian Hopper, *FBI Has E-Mail Sniffer but Is It a Temptation for Agency to Snoop Too Far?*, CONN. L. TRIB., Aug. 7, 2000, at 16.

15. *Id.*

16. Stefania R. Geraci, *Electronic Privacy Information Center Confronts FBI over Internet Surveillance System*, E-COMMERCE, Aug. 2000, at 10.

17. *EPIC Gets First Set of FBI's "Carnivore" Documents*, ONLINE NEWSL. ITEM00298004, Nov. 1, 2000, *available at* 2000 WL 7550696.

18. *Id.*

19. *Digital Privacy and the FBI's Carnivore Internet Surveillance Program: Hearing of the S. Judiciary Comm.*, 106th Cong. (2000) [hereinafter *Digital Privacy*] (statement of Sen. Patrick Leahy).

legitimate criminal investigation.[20] However, the ability to narrowly tailor search inquiries does not substantially diminish concerns that Carnivore will be used to capture more than that which it is authorized to catch. U.S. Senator Patrick Leahy, while acknowledging that judges may be offended by his impression, has suggested that a court order is often "designed exactly the way the government wants it to be."[21] Moreover, the protection a court order possibly provides notwithstanding, no procedural safeguard can ever exist that would prevent a rogue FBI agent from manipulating Carnivore to capture unlawfully electronic communications. Once these communications have been intercepted, this information may well end up in the FBI's files, whether or not it emanated from or was sent to the subject of a criminal investigation.

### *B. How Carnivore Works*

Understanding how Carnivore works requires a basic knowledge of how the Internet functions. Once a user has an ISP, which draws on high-powered computers and high-speed, high-volume communications channels to connect to other ISPs, the user can connect to the Internet.[22] Once a user is connected to the Internet, or "online," the user can be assigned a unique electronic mail address, usually consisting of the user's name or alias followed by the symbol "@" and the ISP's name, allowing the user to correspond over the Internet via electronic mail with other users.[23]

The information contained in electronic mail messages flows through the Internet in "packets."[24] A sender's message is broken down into multiple packets as it traverses the Internet, with each packet containing header information, identifying the sender's electronic mail address, intended recipient's electronic mail address, and subject of the message.[25] As the packets come through the ISPs' systems, Carnivore reads the header information, and if it is to or from a targeted electronic mail address or person, Carnivore will record the address information or the entire packet, according to the court order, on its hard disk.[26] Later, an FBI agent can read the recorded information.

By September 2000, the Carnivore system had been used twenty-five to thirty times.[27] The precise outcomes of these electronic surveillances, specifically regarding what information was harvested as a result of the searches, was not released because the FBI indicated that most of the cases in which Carnivore was

---

20. 47 U.S.C. § 1002(a)(2) (1994).

21. *Digital Privacy*, *supra* note 19.

22. *Communications-Technology: Decoding the Internet: An Online Primer*, INTER PRESS SERV., Apr. 23, 1996, *available* at 1996 WL 9810171.

23. *Id*.

24. James H. Johnston, *Beware of Carnivore's Voracious Appetite*, LEGAL TIMES, Sept. 4, 2000, at 29.

25. *Id*.

26. *Id*.

27. *Digital Privacy*, *supra* note 19 (statement by Donald M. Kerr, Assistant Director, FBI).

used involved issues of national security.[28] However, the FBI's unwillingness to release the results of Carnivore's quests, even in indistinct terms, engenders less public confidence that Carnivore is intercepting only that which it is authorized to intercept by a court order.

### *C. Competing Interests: Privacy v. Law Enforcement*

*1. Privacy*.—U.S. citizens immediately expressed concern about Carnivore after learning of its existence. Although the right to privacy is not mentioned in the U.S. Constitution, it is a right that U.S. citizens consider fundamental.[29] The Fourth Amendment of the United States Constitution is the primary constitutional provision from which an inferred right to privacy can be drawn, but even it does not explicitly refer to privacy.[30] Nevertheless, a right to privacy is embodied in what U.S. Supreme Court Justice Brandeis called the most inalienable of rights—"the right to be let alone."[31] In protecting that right, Brandeis believed that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[32]

Carnivore's ability to scan millions of electronic mail messages per second, making the government capable of eavesdropping on all Internet users' communications,[33] instinctively offends a sense of the right to privacy. Yet, objections to Carnivore go beyond the assertion that the system contravenes personal rights. More elemental claims are that the FBI lacks the authority to use Carnivore, that the secrecy surrounding the diagnostic tool makes it more likely that it will be abused, and that Carnivore's use detrimentally affects users' trust in the Internet medium itself and in blameless ISPs.

*a. Misusing statutes*.—Privacy advocates contend that statutes intended to govern rudimentary electronic surveillance, including those that amended earlier statutes to cover Internet surveillance, are being excessively stretched in that certain types of searches occurring via the Internet are unacceptable extensions of telephone wiretapping laws.[34] Even the most primitive electronic mail searches can yield substantive information about the subject matter contained in the body of a message and personal information about an Internet user. These

---

28. D. Ian Hopper, *Papers Contradict FBI on Carnivore*, AP ONLINE, Nov. 18, 2000, *available at* 2000 WL 29579830.

29. ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY xiii (1997).

30. *See* U.S. CONST. amend. IV; *see also* ALDERMAN & KENNEDY, *supra* note 29, at xvi (suggesting sources other than the federal Constitution in which courts have explicitly found or inferred rights to privacy: state constitutions, federal and state statutes, and judicial decisions).

31. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

32. *Id*.

33. Geraci, *supra* note 16, at 10 (taking language from a Memorandum in Support of Plaintiff's Motion for a Temporary Restraining Order, EPIC v. Dep't of Justice, No. 00-1849 JR. (D.D.C. Aug. 2, 2000) No. 00-1849 JR.).

34. Hopper, *supra* note 14.

basic electronic mail searches are far more intrusive than comparable telephone record searches, which yield only the numbers to which calls were made and from which calls were received. Yet, the standards governing law enforcement's access to the telephone and Internet records are the same.

The addresses to and from which messages are sent and received, and Web sites visited by a particular Internet user, can potentially expose considerable information about an individual. Hundreds of electronic mail messages can be sent simultaneously to other users, suggesting to someone reviewing a list of those to whom the messages were sent some connection among recipients. Similarly, reviewing a list of Web sites an individual has visited might reveal voluminous amounts of information about the person. Telephone wiretapping laws modified to apply to Internet use simply do not provide adequate privacy protections when applied to the Internet medium.[35]

*b. Shrouded in mystery*.—Another primary concern about the use of Carnivore arises from the mystery that surrounds it. Not only does the public know very little about Carnivore, but even ISPs, which are required to allow Carnivore to be attached to their equipment, are not provided access to the system.[36] Only the FBI knows how the system operates. Contrary to the procedure it follows when seeking to obtain telephone records from telecommunications companies under current law, the FBI retains full control of Carnivore, rather than allowing ISPs to provide the information in compliance with court orders.[37] This mystery prevents ISPs and their customers from knowing exactly what Carnivore does, what it reads, and its capabilities and limitations.

*c. Potential for abuse*.—Closely related to the problem of Carnivore's mysteriousness is the concern that it could be used for purposes other than those for which it is supposedly intended. Given Carnivore's ability to scan every electronic mail message that comes through an ISP's network, it is easy to

---

35. *Id*.

36. *Devouring Privacy*, CONN. L. TRIB., Aug. 21, 2000, at 22. *But see* Jason Fry, *Tech Week in Review: Web-Privacy Advocates Battle Plan*, DOW JONES NEWS SERV., July 17, 2000 (indicating that ISP EarthLink, objecting to having Carnivore installed on its equipment on various grounds, including its inability to know that for which Carnivore is seeking and what it intercepts, the legal jeopardy from its customers in which it puts itself, and the incompatibility of Carnivore with its advanced operating system, unsuccessfully challenged the FBI in court). Later, however, EarthLink struck a deal with the FBI to provide any data the FBI needs without the FBI having to install Carnivore on its network. *Id*.

37. *Id*.; *see also* Margaret Coker, *In Russia, Privacy Will Come to an End if 'You've Got Mail'; New Law Will Allow Government to Monitor Internet, Cell Phones, and Pagers*, AUSTIN AM.-STATESMAN, Sept. 10, 2000, at A17 (quoting a Russian telecommunications company executive's statements about Russia's Carnivore-like electronic surveillance system, S.O.R.M.: "We cannot see what they are doing, when they are tapping in. We can only trust that they are not working against our clients' interests."); *Learning to Live with Big Brother*, *supra* note 9 (suggesting that rather than giving the FBI unlimited access to networks, less intrusive alternatives exist, including ordering ISPs to turn over the specific material demanded by a court order).

conceive that the system could be used to monitor unpopular groups or political enemies.[38] Critics have suggested that Carnivore might be used to search electronic mail users' messages for phrases like "overthrow the government," in turn leading to the sender to becoming the subject of increased surveillance.[39]

*d. Chilling effect*.—Given its perceived potential for abuse, the very knowledge that the FBI has the ominous capabilities provided by Carnivore can have a detrimental effect on Internet users' confidence in the integrity of the medium. The use of Carnivore may increase the uncertainty of innocent citizens who are already concerned about Internet privacy.[40] Users should not have to limit their behavior out of fear that their government may be eavesdropping on them when using a medium that should be considered private.[41]

*e. Putting ISPs in a compromising position*.—Carnivore's current use forces ISPs to become unwilling parties to criminal investigations.[42] Ultimately, putting ISPs in this accessory role will undermine consumer trust. Compounding this already undesirable situation is that the telecommunications industry is caught between not wanting to spend the money to build in the Carnivore equipment (assuming it would then have control over the system) and being equally concerned about cybercrime, another important consumer-confidence issue.[43]

*2. Law Enforcement*.—Despite their extensive list of privacy concerns, even the most zealous privacy advocates recognize the importance of maintaining some of the government's electronic surveillance capabilities. To be able to meet their obligation to provide for public safety, law enforcement agencies need the appropriate tools in which to engage in sophisticated crime-fighting techniques. Accordingly, compelling arguments can be made for allowing the FBI to conduct some degree of electronic mail surveillance. These arguments include the prospect of reversing the rising rates of cybercrime, the potentiality of high-tech diagnostic tools to conduct searches that are minimally intrusive, and the general societal interest in technological advancement.

*a. Increased criminal activity*.—Electronic mail communication is increasingly used among criminals, indicative of law enforcement's need to have some manner by which to access these communications.[44] In fact, the FBI's rationale for developing the Carnivore technology centers around its observation that the nation's electronic communications networks are routinely being used by criminals in committing serious crimes, including terrorism, espionage,

---

38. *Learning to Live with Big Brother*, *supra* note 9.

39. Johnston, *supra* note 24.

40. *Digital Privacy*, *supra* note 19 (statement of Jeffrey Rosen, Professor, George Washington University Law School).

41. *Id*.

42. Elisabeth Frater, *Law Enforcement: The Carnivore Question*, NAT'L J., Sept. 2, 2000 (referring to a comment by Jeff Richards, executive director of Internet Alliance).

43. *Id*. (referring to statement by Stuart Baker, former counsel to the National Security Agency).

44. *Learning to Live with Big Brother*, *supra* note 9.

organized crime, and drug trafficking.[45] Some law enforcement officials have even characterized the surveillance of electronic communications as privacy enhancing.[46] At any rate, there can be little doubt that routine surveillance would likely curb the escalating cybercrime statistics.

*b. Narrowly-tailored use*.—Proponents of Carnivore suggest that use of the system could actually be a less-intrusive means of electronic surveillance than that currently authorized under federal law.[47] The FBI notes that unlike telephone taps that pick up all activity on a particular telephone line, the Carnivore system has the potential to be programmed to "pick up the e-mail from only one sender and a particular computer."[48] In addition to the purported ability of the system to be programmed to receive only the information authorized by a court order, the FBI argues that it is difficult to obtain an internal order to use Carnivore; an application must be signed by a high-level Justice Department official and must indicate why other investigative measures will not work.[49]

*c. Encouraging technological innovation*.—The last century has witnessed a technological revolution. As an example, telephones, once obtainable by only a select few, have become household items. Over the last decade, the explosive growth in the number of individuals owning computers suggests that it too will become as indispensable a household staple as the telephone.[50] Moreover, the telephone and computer represent only a fraction of the products that have resulted from this technology boom. Although whether the social impact of such devices has been favorable can be debated, our society is one that highly values technological progress. Arguably, the FBI's development of Carnivore represents a significant advance in electronic surveillance capabilities. With this kind of technological innovation being encouraged, the development of more sophisticated surveillance technology is a valid goal of law enforcement agencies.

---

45. Fed. Bureau of Investigation, *FBI Programs and Initiatives—Carnivore Diagnostic Tool*, *available at* http://www.fbi.gov/programs/carnivore/carnivore2.htm (last visited Jan. 15, 2001) (arguing that evidence garnered through electronic surveillance is superior to many forms because it offers juries opportunities to determine the facts of a case based on criminal defendants' own words).

46. Frater, *supra* note 42 (quoting David Green, the Justice Department's principal attorney for computer crimes: "When we're investigating the hacker who's stolen your ID, then [Carnivore is] privacy-enhancing.").

47. *See generally* 47 U.S.C. §§ 1001-1010 (1994).

48. *Learning to Live with Big Brother*, *supra* note 9.

49. Geraci, *supra* note 16, at 10; Fed. Bureau of Investigation, *supra* note 45 (offering that court orders are limited to a specified time, and judges may and often do require periodic progress reports, thus ensuring close oversight).

50. EVAN HENDRICKS ET AL., YOUR RIGHT TO PRIVACY: A BASIC GUIDE TO LEGAL RIGHTS IN AN INFORMATION SOCIETY 68 (2d ed. 1990).

## II. Increased Global Internet Use and Domestic and International Legal Responses to Electronic Surveillance and Privacy Protections

The digital age is having profound impact on the ways in which people engage in day-to-day activities. Not long after the number of personal computers in offices and homes exponentially grew, Internet connections followed the same trend. During the past twenty years, the number of computers with Internet access increased from 300 in 1981 to 72.4 million in 2000.[51] The Internet has become a dominant means for individuals to conduct business, get news and information, engage in personal and professional communications, and entertain themselves.[52] People no longer are simply using their computers as data processors or to play games. Rather, household appliances are now being wired to the Internet and many "personal thoughts and associations" are transmitted via computer.[53]

This sizable increase in the level of Internet use in the United States warrants closer attention directed to electronic mail surveillance. However, the medium is a unique one in that "[n]ational boundaries have little meaning on the Internet."[54] The Internet allows individuals on any networked computer anywhere in the world to exchange instantaneously information with one another. Electronic mail can be sent from an individual in one country to an individual in another in a matter of seconds. These extraordinary properties of the Internet necessitate both domestic and international responses.

### *A. Domestic Responses*

The U.S. Congress' good intentions are evident in the ways in which it is attempting to balance law enforcement needs with privacy protections when it comes to Internet surveillance. One way in which Congress is dealing with the issue of online privacy is through impending legislation. In Fall 2000, at least fifteen bills were pending in Congress that dealt with online privacy.[55] Given the monumental amount of recent attention being given to privacy as it relates to Internet use, these laws are presumably, at least in part, being proposed to bolster Internet users' privacy protections. Yet, despite Congress' good intentions, development in this dynamic area of the law is extremely slow, partially due to the constantly changing nature of electronic advances. However, in support of new laws being deliberated, Capital Hill hearings on the subject of Carnivore and digital privacy are being held,[56] indicative of the legislature taking steps toward

---

51. Sarosdy, *supra* note 4, at 15.

52. *Digital Privacy*, *supra* note 19 (statement of Sen. Orrin Hatch) (citing a report stating that over 40 million Americans are currently using the Internet and there are 55,000 new users every day).

53. *Learning to Live with Big Brother*, *supra* note 9.

54. *Communications-Technology*, *supra* note 22.

55. Sarosdy, *supra* note 4, at 15.

56. *See, e.g.*, *Digital Privacy*, *supra* note 19.

securing greater privacy protections.

### *B. International Responses*

*1. The United Kingdom's Regulation of Investigatory Powers Act*.—The Regulation of Investigatory Powers Act ("R.I.P."), adopted in the United Kingdom in 2000, is a comprehensive piece of legislation that explicitly provides for the interception and acquisition of electronic communications by U.K. security agencies.[57] R.I.P. requires ISPs operating in the United Kingdom to attach Carnivore-like systems to their equipment for use in assisting law enforcement officials with monitoring suspected criminals' electronic communications.[58] Unlike its statutory counterparts in the United States, R.I.P. does not mandate that a search warrant be granted by a judge to allow e-mail surveillance; rather, a "home secretary," an elected politician, can issue warrants.[59] The Act also requires ISPs to turn over decryption keys or convert messages into plain text following approval from certain officials, including senior police officers.[60]

Carnivore and R.I.P. share similarities beyond their equally threatening names. British businesses, trade unions, newspapers, and civil liberties groups have voiced significant opposition to R.I.P.[61] Some business owners have even threatened to leave Great Britain rather than accept the cost and intrusion of the R.I.P. Act's mandates.[62] R.I.P. opponents also argue that the bill breaches fundamental rights—namely privacy, liberty, expression, and association—all slated soon to be incorporated into British law according to the European Convention on Human Rights.[63] In December 2000, British politicians declined to support requests from U.K. security agencies to grant them additional powers under R.I.P. prior to Britain's impending general election.[64]

---

57. *See generally* Regulation of Investigatory Powers Act, 2000, c. 23 (Eng.).

58. *See 7 Days—No Escape from the Spooks*, COMPUTING, Aug. 24, 2000, at 16 (suggesting that if governments want to intercept electronic communications they will do it with or without legal authority, and will only go through the legal process if the information is necessary for a court proceeding).

59. Steven Semeraro, *If Only R.I.P. Bill Really Could R.I.P.*, NAT'L L.J., Aug.14, 2000, at A18.

60. *Id.*

61. *Id.*

62. *Id.*; *see also* Laura Rohde, *U.K. E-Mail Law Reaches U.S. Although Most American Companies Don't Know It Yet, the U.K.'s R.I.P. Act Has Far-Reaching Ramifications for Those Doing Business There*, INFOWORLD, Sept. 4, 2000, *at* 2000 WL 20918065 (speculating that U.S. companies worried about security breaches due to the British R.I.P. may choose not to establish business operations in the United Kingdom).

63. Semeraro, *supra* note 59.

64. Jimmy Burns & Jean Eaglesham, *Ministers Shun Call for New Snooping Powers*, FIN. TIMES (Eng.), Dec. 5, 2000, at 4.

*2. Russia's System of Operational and Investigative Measures*.—In September 2000, Russia's System of Operational and Investigative Measures (known by its Russian acronym S.O.R.M.) law was amplified, giving the Russian Intelligence Agency (formerly the K.G.B.) the legal authority to conduct relatively unbridled electronic surveillance of its citizens' (and consequently non-citizens') Internet traffic, as well as cellular telephone and pager communications, with an easily-attainable warrant, but without the user's knowledge.[65] Like the United Kingdom's implementation of R.I.P., Russian regulations will require ISPs to equip networks with surveillance devices designed to transmit information to security service headquarters.[66] Yet, the reach of S.O.R.M. is even more disturbing—it requires all Internet communications to pass through clearinghouse sites and prohibits encryption attempts.

Opposition to Russia's law parallels the opposition movement by U.S. and British objectors to Carnivore and R.I.P. Russian protesters argue that no system of checks and balances exists to prevent its federal security agency from using information for "political blackmail," commercial espionage, or any other reason.[67] The right to privacy seems especially important in Russia, a fledgling democracy, where the Internet has provided a medium for the country's citizens to criticize their government, a fundamental democratic right.[68]

*3. Additional Responses*.—In addition to the United States, Britain, and Russia, other countries have recently adopted or are considering adopting electronic surveillance laws.[69] Singapore and Malaysia have enacted laws similar to those enacted in Great Britain and Russia, allowing for electronic mail surveillance with minimal privacy protections in place.[70] Japan has also enacted electronic mail-tapping legislation.[71] Japanese legislation requires ISPs to keep a pen-register-type record of all Internet communications traveling through their networks.[72] These records must be made available to law enforcement officials when a subpoena is issued.[73] Conversely, in the Netherlands, a robust public debate is occurring over whether the government should have authority to access

---

65. Coker, *supra* note 37.

66. *Id*. *But see* Guy Chazan, *Russia Backs Down on Tapping E-Mail Traffic Without a Warrant: 'You Can Challenge Authorities and Not Only Survive But Win,'* WALL ST. J. EUR., Nov. 27, 2000, at 23 (stating that when a Russian provincial ISP challenged S.O.R.M. by filing a complaint in a Russian court after refusing to install the surveillance system on his equipment, basing his claim on a confidentiality agreement signed with his customers and a provision in his business license making disclosure of his clients' personal data a criminal offense, the government backed down, with ministers declaring that Russia needed further legislation).

67. Coker, *supra* note 37.

68. *Id*.

69. Semeraro, *supra* note 59.

70. *Id*.

71. 7 *Days—No Escape from the Spooks*, *supra* note 58.

72. Graham, *supra* note 1.

73. *Id*.

electronic mail messages at all.[74]

### *C. International Law Enforcement Telecommunications Seminar*

Recent developments in electronic surveillance activities around the world are no coincidence. The FBI has taken the lead in convening an international coordinating group responsible for harmonizing nations' schemes to make it easier to intercept information from telecommunications systems around the globe.[75] The group, called the International Law Enforcement Telecommunications Seminar (ILETS), has secretly met annually for the past seven years.[76] The Seminar's plans to compel ISPs all over the world to install Carnivore-like "black boxes" on their servers surfaced in 1999, unveiling the FBI's intent that countries all over the globe work in concert to conduct the kind of electronic mail surveillance that Carnivore and its successors make possible.[77]

As the ILETS devised its cooperative worldwide electronic surveillance strategy, it excluded from its discussions lawyers and industry experts who could have provided advice on protecting privacy.[78] In fact, the formation of the global communications' interception alliance was "without parliamentary or public discussion or awareness" all together.[79]

## III. BALANCING PRIVACY PROTECTIONS WITH LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE NEEDS

### *A. U.S. Case Law: The Fourth Amendment*

In its first consideration of whether warrantless wiretapping of a criminal suspect's telephone violated the Fourth Amendment, the Supreme Court determined that where surveillance did not include physical intrusion on the defendant's property and no material objects were seized, no constitutional violation existed.[80] Nearly forty years later, the Court reversed its position on

---

74. *Learning to Live with Big Brother*, *supra* note 9.

75. Duncan Campbell, *Many Governments Tapping E-Mails*, CANBERRA TIMES (Austl.), Aug. 21, 2000, at 16.

76. *Id*.

77. *Id*.

78. Duncan Campbell, *The Spy in Your Server: There Is No Hiding Place on the Net as Governments Around the World Chase Your Data*, GUARDIAN (U.K.), Aug. 10, 2000, *at* 2000 WL 25045488 (suggesting that as a result of the exclusion of these individuals, laws based on the ILETS's arrangements have led to worldwide controversies).

79. *Connected: How the NSA Has Spread Its Web over the Globe*, DAILY TELEGRAPH (Eng.), Feb. 17, 2000, *at* 2000 WL 12384227.

80. Olmstead v. United States, 277 U.S. 438, 466-67 (1928). *But see id*. at 474 (Brandeis, J., dissenting) (predicting that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court . . . ," invading individual security).

wiretapping, holding in two cases decided within a few months of one another that the Fourth Amendment protects people and not places.[81] In one of the two cases, *Katz v. United States*, the government's electronic surveillance, listening to and recording a criminal suspect's words while he was having a phone conversation in a telephone booth, was deemed to have invaded the privacy upon which the defendant had relied.[82] The Court determined that the law enforcement officers' actions constituted an unreasonable search and seizure without a warrant under the Fourth Amendment.[83] The Court found it insignificant that the surveillance device used by the government did not penetrate the walls of the booth. The *Katz* analysis shifted the focus from the means of communication to the communication itself as the source of a constitutional right.[84] Following *Katz*, which remains sound precedent for limits on Fourth Amendment wiretapping, the Court held in subsequent cases that application of the Fourth Amendment depends on whether a claimant can invoke a "legitimate" or "reasonable" expectation of privacy.[85]

In 1979, in *Smith v. Maryland*,[86] the Court considered whether police violated a criminal suspect's Fourth Amendment rights when the police installed a pen register on the suspect's telephone line without a warrant to record the numbers dialed from the phone. Using the standard established in earlier cases in which telephone wiretapping was deemed to be a search under the Fourth Amendment,[87] the Court required the claimant to establish that he held a subjective expectation that the numbers dialed were a matter of privacy and that this expectation was one society recognizes as reasonable.[88] Because the pen register was installed on the phone company's property, the petitioner could not claim invasion of a constitutionally protected area, and instead rested his claim on an expectation of privacy.[89] The Court rejected the privacy argument, determining that because pen registers do not acquire the contents of communications, but only the numbers dialed, and all numbers dialed go through phone companies that customers know make records, no expectation of privacy can reasonably exist.[90] Therefore, the Court determined that information gathered by the pen registers are not Fourth Amendment "searches" and hence do not require warrants.[91]

Today, law enforcement requests for pen-register and trap-and-trace records

---

81. Katz v. United States, 389 U.S. 347, 351 (1967); Berger v. New York, 388 U.S. 41, 51 (1967).

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

83. *Id*.

84. *See Digital Privacy*, note 19 (statement of Michael O'Neill, Professor, George Mason University Law School).

85. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 (1978); Terry v. Ohio, 392 U.S. 1, 9 (1968).

86. 442 U.S. 735 (1979).

87. *See Katz*, 389 U.S. at 352-53; Berger v. New York, 388 U.S. 41, 51 (1967).

88. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

89. *Smith*, 442 U.S. at 741.

90. *Id*.

91. *Id*. at 745-46.

are granted "without question" by federal courts.[92] Pen-register and trap-and-trace records in the electronic communications context are records of "to-and-from e-mail addresses" and Web site visit histories.[93]

### *B. U.S. Statutory Law*

Immediately after the Supreme Court issued the opinion in which it identified the requisite showing a claimant must make to prove an unreasonable search under the Fourth Amendment, Congress passed Title III.[94] Title III requires the government to obtain a court order before tapping wire communications or eavesdropping on an oral conversation in which parties have an expectation of privacy.[95] In order to obtain a warrant, the government has to demonstrate probable cause, define the surveillance parameters, and explain why other investigative techniques will not work.[96] Although the Act requires that minimal notice be given to parties targeted by wiretapping, the provision is considered by many to be too vague, and no notice is required to be given to non-targets who are part of the conversations.[97]

Recognizing that Title III applied only to the expectation of privacy in conversations that could be heard, Congress sought to modify the law covering computer technology where the question of whether an expectation of privacy exists is blurred.[98] The Electronic Communications Privacy Act (ECPA) was the first federal statute to specifically address the surveillance of electronic communications.[99] The ECPA extended protections afforded aural communications to non-aural communications, thereby safeguarding unwarranted interceptions of the content of electronic mail.[100]

In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA).[101] CALEA makes it possible for the government to tap more modern digital telephone wiring and requires telephone companies to modify their equipment to accommodate wiretapping devices.[102] As it pertains to electronic mail, CALEA requires a court order, but not probable cause, for the government to obtain electronic mail addresses and other transactional data.[103]

---

92. *Learning to Live with Big Brother*, *supra* note 9.

93. *Civil Liberties Groups Blast "Carnivore," supra* note 3.

94. *See generally* 18 U.S.C. §§ 2510-2522 (1994) (incorporating basis for Title III).

95. *Id*.

96. HENDRICKS ET AL., *supra* note 50, at 69.

97. *Id*.

98. *Id*. at 70-71.

99. *See generally* Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

100. HENDRICKS ET AL., *supra* note 50, at 71.

101. *See generally* Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 and 47 U.S.C.).

102. *Id*.

103. *See* 47 U.S.C. § 1002(a) (1994).

However, CALEA does not require ISPs to modify their equipment to accommodate interception.[104]

Privacy advocates contend that in the FBI's battle to get CALEA passed, it explicitly stated that it did not want more surveillance capacity than it already had, but rather simply wanted to conduct surveillance in new ways made possible by new technologies.[105] Yet, ultimately, the FBI's authority under CALEA seemed to include dictating wiretapping technical standards while telecommunications systems were still in an explosive period of development.[106]

### *C. Expectation of Privacy*

Some World Wide Web users would be surprised to learn that site administrators can detect their e-mail address, sites they have previously visited, and other information to be used for marketing purposes.[107] Electronic mail users may also be surprised to find out that copies of their messages may remain on ISPs' servers long after recipients have deleted them.[108]

As a result of third parties' ability to access electronic mail messages sent and Web sites addresses visited, courts have determined that electronic communicators have a reduced expectation of privacy in their communications, and thus reduced protection from unreasonable searches. However, such an assumption may be dangerous and unwarranted when Internet activity is rapidly increasing and more private transactions are conducted via Internet, its result being a downward spiral in the level of protection provided to electronic communications.[109] It is difficult to argue that no expectation exists of online privacy when activities like banking and investing, unquestionably regarded as both personal and confidential, are being conducted through the medium.[110] Technology is swiftly moving our society toward a personal computer-less Internet world, one in which "much of our lives will be in the hands of third parties."[111]

In light of these many technological, societal, and legal developments, the time has come for courts to redefine their standard for determining whether the kind of electronic surveillance made possible by Carnivore violates the Fourth

---

104. *See id.* § 1002(b)(2).

105. Frater, *supra* note 42.

106. *Id*. *But see* United States Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000) (holding that call waiting and call forwarding records are outside of the scope of what is attainable under wiretap orders and suggesting that CALEA would not permit the government to use a lower legal standard engaging in electronic mail surveillance).

107. Joe Borders, *Finding Security Online: You're Not Being Paranoid; Someone Really Is Watching You*, TEX. LAW., July 31, 2000, at 27.

108. *Id*. (noting that there are companies that sell encryption devices so that an Internet user may engage in anonymous browsing).

109. *Devouring Privacy*, *supra* note 36.

110. *Digital Privacy*, *supra* note 19 (statement of Michael O'Neill).

111. *Id.*

Amendment. Currently, in order for a claimant to prevail on privacy grounds in cases alleging unreasonable searches, one must show a subjective expectation of privacy and that this expectation is one society recognizes as reasonable.[112] As applied to Internet communications, it seems likely that most claimants, given the nature of the personal business conducted via the medium, could make strong arguments supporting these subjective expectations of privacy. Therefore, only the question of whether a societal expectation of online privacy is reasonable needs to be considered. Based on the evidence surrounding Internet use, this question could likely be answered in the affirmative.

## IV. RESOLUTION REQUIRES NATIONAL AND INTERNATIONAL CONSIDERATION

### *A. The United States*

Resolving the issues surrounding the use of Carnivore and its international cousins calls for a multifaceted intervention. Ultimately, a combination of actions is likely required. Existing laws should be strengthened to ensure greater privacy protections, coupled with proper and regular oversight of government electronic surveillance networks. Likewise, comprehensive, forward-thinking legislation should be passed, rather than piecemeal statutes that result in applicable laws lagging behind electronic surveillance practices. Together, these actions will aid in quieting controversy over this form of electronic surveillance. Therefore, the following recommendations, although some dependent upon others, are offered to be considered as parts of a larger scheme, or in some cases, as alternatives to one another.

*1. Addressing Constitutional Concerns*.—When Carnivore is used specifically to seize the contents of electronic mail messages of suspected criminals in cases in which probable cause warrants have been issued, the search appears not to contravene the Fourth Amendment. However, there are three ways in which the FBI's use of Carnivore may controvert the Fourth Amendment. First, Carnivore's ability to search all electronic mail, even when its operation attempts to limit the search to the communications of suspected criminals, invariably means that the communications of innocent parties from whom mail is received and to whom mail is sent by a suspected criminal is searched in the process. Searches of innocent parties' electronic mail messages, for which no proper judicial authorization exists, might violate the Fourth Amendment.[113]

Along these same lines, the relative ease with which people can forge electronic mail messages (sending messages from another person's account), suggests that even under an ostensibly proper warrant, a Carnivore search could

---

112. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

113. To find that these searches violate the Fourth Amendment would require the Supreme Court to articulate a clear standard of what constitutes a reasonable search related to electronic mail communications. Currently, the Court likely views these communications as unprotected by the Fourth Amendment due to a misperception that electronic mail users have a decreased expectation of privacy. *See supra* Part III.A.

mistakenly focus on an innocent party, capturing that individual's genuine messages along with the forged ones. An ISP or computer specialist may easily be able to detect this information, but Carnivore may not possess the same capacities. If so, this type of search may also violate the Fourth Amendment.

Second, under existing laws, acquiring pen-register and trap-and-trace electronic mail records has not been held to trigger Fourth Amendment protections. Courts should distinguish Internet searches from the less intrusive corresponding telephone pen-register and trap-and-trace searches, and hence recognize the need that these searches be subject to the limitations imposed by the Fourth Amendment. Requiring the government to meet a "probable cause" standard whenever it seeks to intercept electronic mail, header information, or contents, would provide the level of privacy protection to Internet communications contemplated by the Fourth Amendment and called for by Internet users.

Finally, Carnivore is configured to perform sweeping searches. These searches seem to parallel the kinds of broad searches courts have held to be unconstitutional in other contexts, such as those in which passers-by are indiscriminately stopped and searched in an attempt to uncover criminal activity.[114] These constitutional questions are threshold issues requiring ultimate resolution before Carnivore can legitimately be used at all by the FBI, at least in its current form.

*2. Obtain Access to Carnivore*.—In a country built upon a system in which each branch of government guards against abuses of power by the others, Carnivore is currently operating without a watchdog. Making the Carnivore software available to ISPs would be a substantial first step in implementing a system of checks and balances, while at the same time allowing the FBI to use Carnivore for its intended purpose.[115] If ISPs know how Carnivore works and are able to configure inquiries themselves, they can set the limits ordered by courts. In so doing, the configured search would mirror the methods used when law enforcement officials seek telephone records in that telephone companies provide records based on the parameters set in the court order. Furthermore, ISPs' role in the searches would allow them to assure their customers that the integrity of their systems will remain intact, even when the ISPs are required to turn over information to law enforcement agencies in fulfillment of a court order.

In addition to requiring that ISPs have access to the system, Congress should obtain detailed briefings, perhaps classified if necessary, in order to understand Carnivore's design, fallibility, potential for abuse, and whether encryption software could easily defeat its objective. The regular oversight by Congress, coupled with the transfer of control from the FBI to the ISPs, would provide a

---

114. *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1968); *see also* City of Indianapolis v. Edmond, 531 U.S. 32 (2000) (holding that the city's drug interdiction checkpoints violated the Fourth Amendment).

115. *Digital Privacy*, *supra* note 19 (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

buffer between the ISPs' customers and the FBI.[116]

In order to further ease the concerns of its critics and to make Carnivore understandable to Internet users and others, the system should undergo an independent review.[117] The Justice Department agreed to have such an external review conducted in Fall 2000, but the manner by which it went about the process drew additional criticism.[118] Elite academic computer departments, including the Massachusetts Institute of Technology and Purdue University, withdrew themselves from consideration of Carnivore's review, objecting to the acute limitations imposed on it by the Justice Department.[119] When the Illinois Institute of Technology's Research Institute was finally selected to conduct the review, the Justice Department was again sharply criticized for choosing a team that included a former policy advisor to President Clinton, a former Justice Department official, and other members with backgrounds in the National Security Agency (NSA), the Department of Defense, and the Department of the Treasury.[120] The preliminary report of the research institute, released by the Justice Department in November 2000, unsurprisingly gave Carnivore a relatively clean bill of health, recommending only slight tweaking to the system to prevent unlawful interceptions.[121] However, the report's seemingly biased origins instill little confidence that the concerns over Carnivore's potential for misuse are unjustified.

The FBI articulates what it doubtlessly regards as legitimate reasons to oppose the release of Carnivore's operating code, as it could potentially be used as a source from which hackers could develop ways to defeat the system. However, since the technological knowledge that provided for Carnivore's construction was available to the government, it seems highly likely that knowledge to circumvent the system is available to skilled hackers. Subjecting Carnivore to peer review might illuminate ways of solidifying the code against potential attacks by individuals seeking to undermine the system.

Assuming arguendo that the FBI should not reveal Carnivore's source code, it should at least conduct a laboratory test of the system, the complete results of which could be made public. Such an overt testing of each of Carnivore's

---

116. *Id*. (statement of Michael O'Neill); *see also* Frater, *supra* note 42 (quoting Rep. John Conyers Jr.'s statement made during a hearing on Carnivore with the FBI: "So should we now be comfortable with a 'trust us we're the government' approach? I don't think anybody on the [congressional oversight] committee has that view.").

117. D. Ian Hopper, *Critics Denounce Carnivore Review*, AP ONLINE, Oct. 4, 2000, *at* 2000 WL 27902983 (discussing the Justice Department's choice of alleged "government insiders" to conduct an "independent review" of the Carnivore system released in November 2000).

118. *Id*.

119. *Id*.

120. *EPIC Gets First Set of FBI's "Carnivore" Documents*, *supra* note 17.

121. 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 A02. *See generally* Ill. Inst. of Tech. Research Inst., *Independent Review of the Carnivore System Draft Report*, (Nov. 17, 2000), *available at* http://www.usdoj.gov/jmd/publications/carniv_entry.htm.

capabilities, indicating the evidence gathered as a result of the searches, may increase public trust in the government's legitimate use of the system for certain purposes.

*3. Determine Statutory Authorization*.—Based on the FBI's current stretch of existing statutory laws to justify its authority to develop and use Carnivore, Congress should articulate whether such a statutory basis is reasonable. There are at least two ways in which the use of Carnivore seems to exceed the government's allowable use and employment of electronic surveillance laws.

First, the sheer fact that the laws upon which the FBI relies as its mandate to use Carnivore were initially passed to make lawful the interception of electronic communications that by today's standards seem archaic makes the claimed authority questionable.[122] Neither the public nor Congress should simply acquiesce in the use of Carnivore because the FBI says the system is necessary. To do so would perhaps encourage the FBI to conduct electronic surveillance in a manner in which U.S. citizens never intended to tolerate.

Admittedly, among the problems inherent in enacting legislation affecting technology is the patent difficulty posed in keeping up with technological advances. Therefore, Congress must enact laws comprehensive and resilient enough to accommodate such growth or constantly have its fingers on the pulse of developing technology so as to regularly engender laws responsive to current technological trends. Obviously, such constant oversight cannot be accomplished by the entire Congress, but could be performed by legislative committee or an external group held accountable to Congress. The challenging issues presented by advances in the ability of the government to spy on its citizens using increasingly sophisticated technology is a dynamic area of the law that warrants such attention. Perhaps the best solution is found in combining both propositions—enacting comprehensive legislation and providing regular oversight.

A second issue requiring resolution is whether the government has the authority to compel ISPs to participate in the interception of the electronic mail of its customers and those with whom they correspond. CALEA makes it clear that ISPs do not have to modify their equipment to accommodate the government's interception of electronic mail.[123] Yet, arguably, the attachment of Carnivore represents a substantial modification, whether or not the ISP itself affixes the system. A recent attachment of Carnivore by the FBI to one ISP's equipment exposed Carnivore's incompatibility with the ISP's operating system, causing the ISP to have to install an old version of its operating system.[124] The

---

122. *See, e.g.*, 18 U.S.C. § 3127(3) (1994) (defining a pen-register device as one that records or decodes electronic impulses and identifies numbers transmitted on a telephone line to which the device is attached). Under this definition, Carnivore clearly fails to qualify as a pen-register device. Yet, the FBI cites ECPA as granting it the authority to acquire e-mail addresses.

123. *Id.* § 1002(b)(2).

124. Nick Wingfield et al., *Companies: FBI's New Surveillance Device Refused by U.S. Web Provider*, WALL ST. J. EUR., July 14, 2000, *available at* 2000 WL-WSJE 21066306.

system crashed and disrupted service to a number of its customers.[125] Whether the ISP was "compelled" to modify its equipment to accommodate the FBI's interception of targeted electronic mail is certainly open to question, but assuming that it did not welcome the opportunity to downgrade its operating system illustrates that the FBI may not be adhering to CALEA's unambiguous provisions, or at the very least its spirit. Therefore, it is imperative that Congress determine if any statutory authority exists to permit the FBI to require ISPs to either install the system or have the system installed on their equipment.[126]

*4. Modify Existing Laws and Enact Comprehensive Legislation*.—If Congress does not pass comprehensive legislation, the risk of individual states enacting their own laws to bolster privacy protections of the Internet using citizenry looms largely. Such a reaction from states could worsen the current nationwide situation, leading to multifarious laws and policies governing Internet use and surveillance being enacted because the federal laws do not provide adequate protection. With the landscape of federal electronic surveillance laws as difficult to traverse as it is, states independently enacting legislation would lead to increased uncertainty and imbalanced protections that should be uniformly provided.

Electronic surveillance laws, specifically Title III and the ECPA, are inadequate in their current form when applied to the FBI's use of Carnivore. The modification of these laws, coupled with new laws, should define exactly the circumstances under which Carnivore can be used and the extent of that use. Most obviously lacking from current law is any unequivocal requirement that law enforcement officials try or at least consider the least intrusive means of investigation before engaging in interception.[127] This procedural safeguard would provide those concerned about their privacy with some assurance that a judge has heard compelling evidence substantiating law enforcement officials' need to make use of Carnivore to monitor a suspected criminal's electronic mail. In other words, using Carnivore should be law enforcement's act of last resort. Enacting such a law would serve to codify what the FBI purports in its policies already to be doing before using Carnivore.[128]

Taking into account the extraordinary burden imposed on privacy by electronic mail searches, laws should require a heightened uniform standard for court orders that requires ISPs to assemble and produce any Internet communications information. Orders should be granted only after a judge finds that reasonable cause exists to believe that a target has committed or is about to commit a crime. Making orders more difficult to obtain would add an additional safeguard ensuring that law enforcement officials would only use Carnivore in the most extremely necessary situations. As the laws currently exist, it is likely that if the FBI suspects a person of a crime for which electronic mail is being used, it will first attempt to get a court order to access the full contents of the

---

125. *Id*.

126. *Digital Privacy*, *supra* note 19 (statement of Michael O'Neill).

127. *Learning to Live with Big Brother*, *supra* note 9.

128. Fed. Bureau of Investigation, *supra* note 45.

mail. Only after such an attempt fails will the FBI settle for a court order that will provide less information.

In compelling a higher standard for court orders, laws should take into account the unique nature of information yielded by even the most rudimentary searches of electronic mail. Carnivore can be used as a content wiretap, trap-and-trace device, or pen register.[129] Internet queries, even those that ascertain only addressing information, subject lines, and web sites visited, provide far more information than what is accessed from pen-register or trap-and-trace telephone records.[130] A subject line has the potential of revealing the entire heart of the message's content.[131] Yet, authorization for obtaining such information from telephone or Internet users is acquired in the same way—from lower-level judges without a probable cause warrant.

In addition to reinforcing the required showing the government must make for court orders to be granted, and as part of an overall approach to Internet mail and other online activities produced as courtroom evidence, laws should require notice and an opportunity for defendants to object when civil subpoenas seek personal information regarding Internet activities.[132] Providing this kind of protection to individuals' right to privacy may have positive implications for future lawmaking and provide a firm foundation for the development of an increased societal expectation of privacy in Internet communications.

Finally, laws governing the use of Carnivore should bring an end to the ambiguity surrounding what information the government can and does gather. Public distrust of the FBI's unfettered use of Carnivore would dissipate if people knew exactly what the law enforcement agencies are permitted to obtain. Requiring the executive branch to provide Internet consumers with notice when the government obtains information regarding their Internet transactions would lead to increased public trust.[133] In addition, requiring specific statistic reports for pen-register and trap-and-trace orders for Internet communications, similar to those reports required under existing legislation for telephone pen-register and trap-and-trace records, would also bolster support for the use of surveillance systems.[134]

Enacting comprehensive laws will serve to disentangle the confusing mixed bag that federal electronic surveillance legislation has become. In doing so, it is imperative to note that Internet users do not have a minimum expectation of

---

129. A content wiretap captures all electronic mail and network traffic to and from a specific account. A trap-and-trace device captures the electronic mail addresses from which a user receives mail; a pen register captures the electronic mail addresses to which a person sends messages and those servers and web pages the person accesses.

130. *Learning to Live with Big Brother*, *supra* note 9.

131. For example, a subject line reading "The Case Against Carnivore" would lead viewers well informed in electronic surveillance equipment being used by the FBI to conclude that the message contains arguments against the use of the diagnostic tool.

132. *Digital Privacy*, *supra* note 19 (statement of Michael O'Neill).

133. *Id.*

134. *Id.*

privacy in their use of electronic mail and the World Wide Web as primary sources of personal and professional communications and information.

### *B. The International Community*

As the lines between governments' intelligence agencies and law enforcement agencies converge, increased attention must be given to electronic surveillance practices abroad. No matter what choices the United States makes about its domestic use of Carnivore, the reality of electronic communications surveillance as a global issue demands ethical and responsive leadership on an international level. The United States should promote worldwide adoption of privacy protections as it encourages countries to develop surveillance policies congruent with its own. This policy promotion must be carried out in a systematic manner, at all times taking into account developments in technology.

In practice, achieving congruence in international electronic surveillance policies presents countless challenges. No single country or group of countries can implement electronic surveillance laws without unavoidably interfering with the electronic mail use of other countries' nationals. For example, the European Union is considering approving an international cybercrime treaty that purports to define how countries should handle cybercrimes committed outside their borders.[135] The treaty, which was finalized by committee in June 2001, makes it a crime to access one's computer without the owner's authorization, but parties to the treaty can interpret what constitutes such "authorization" differently.[136]

The potential negative effects of the European Union treaty are easily recognizable. The European Union represents only a handful of the countries of the world. If this small group of countries establishes multiple interpretations of the parameters of "authorization," the consequence in the global community would be the proliferation of increased incompatibility in the way countries treat these concepts. Time is of the essence. If each country of the world implements its own laws, independent from one another, and those laws are challenged in each country's courts as they undoubtedly would be, the result would be a series of mutated statutes governing a global medium, making it all the more difficult to eventually implement what can be nothing other than an international regulatory scheme.

Although there is already at least one international agency charged with setting policy for the Internet,[137] the nature of privacy expectations and the needs

---

135. Lisa Porteus, *Achieving Privacy Balance Is More Difficult, Panel Says*, NAT'L L.J.'S TECH. DAILY, Jan. 11, 2001.

136. *Id.*; *Cyber Security: Committee Approves Cyber-Crime Treaty*, NAT'L L.J.'S TECH. DAILY, June 25, 2001; *Digital Privacy*, *supra* note 19 (referring to a statement by Stewart Baker, former general counsel at the U.S. National Security Agency). John Ryan, vice president and associate general counsel for America Online, contends the treaty will open the door to other content-related issues, raising a fundamental issue for resolution—whether an ISP in one country must comply with the content laws in another. *See id*.

137. Semeraro, *supra* note 59.

of law enforcement to have ways in which to engage in surveillance of electronic communications necessitate greater attention devoted to these manifestly international issues. The worldwide controversies that flowed from the ILETS' plans to make countries' telecommunications equipment interception-friendly can now be parlayed into the promulgation of an organization with a much nobler mission—promoting balanced polices and procedures.

This new organization, which could be formed by international treaty or otherwise, should serve not only as a policy-making body, but also as a conduit for the accumulation of worldwide input on electronic privacy concerns. Following appropriate administrative procedures, this agency could provide opportunities for privacy advocates, law enforcement officials, and other interested parties to engage in rigorous debate on how to balance privacy protections with the need to provide for public safety via surveillance. Negotiation among representatives of the compound interests involved, albeit time consuming, could produce desirable regulations acceptable to all stakeholders.

Part of this international organization's undertaking could be to stipulate that nations' law enforcement agencies engaging in Internet-activity surveillance routinely provide statistics for legislative oversight.[138] Review of the use of electronic mail search devices and countries' practices could be a priority for the agency. Among the important outcomes of these records would be the notice it would provide suspected criminals of the attention being paid by the world community to electronic surveillance and the consolation it would provide citizens of the world that their privacy is of paramount importance.

Every citizen of the world engaging in electronic mail communications has a significant stake in seeing to it that all states' governments recognize privacy protection as a remedial aim of electronic surveillance. Whether sending a message to a friend across town, to a family member in another part of the country, or to a business counterpart overseas, Internet users need to be confident that their messages will not be intercepted by their or anyone else's government. Given the technical capabilities of Carnivore in the United States and Carnivore-like systems in other countries, as well as the broad interpretations of laws by those using them, citizens worldwide using the Internet as their primary means of communication currently lack such assurance.

## CONCLUSION

At the close of the year 2000, the Denver-based, non-profit Privacy Foundation put the FBI's use of Carnivore on its short list of the most important privacy issues of the year.[139] Given the potential of Carnivore to affect adversely

---

138. *Digital Privacy*, *supra* note 19 (statement of Michael O'Neill) (referring to U.S. Congress, but seemingly applicable to other countries' governments as well).

139. Robert Trigaux, *Technology Endangers Privacy Like Never Before*, ST. PETERSBURG TIMES, Jan. 3, 2001, at 1E. The other privacy issues on the list were: workplace surveillance, patient privacy rules, DoubleClick's profiling of Internet surfers, the rise of chief privacy officers,

every sender and receiver of electronic mail, Carnivore's placement on the list is not unexpected. Arguably, the greatest of Carnivore's grave flaws is the impact its use will have on individuals' personal, not to mention professional, lives.

As an illustration, consider its impact on one aspect of the practice of law. Legal technology experts predict that one outcome of the Carnivore furor will be an increased interest among lawyers and their clients in electronic mail security.[140] An electronic mail message sent from an attorney to a client or sent from a client to his or her attorney could be a target of Carnivore's probe. Without either the sender or receiver being aware of it, the message could be intercepted by the FBI and used against the client in court, destroying the client-attorney privilege that might otherwise have protected the communication from its use against the client.

The FBI chose to implement its use of Carnivore without considering what U.S. citizens would accept when it comes to giving up a measure of their precious privacy rights. Carnivore's capabilities, coupled with the FBI's unwatched use of the diagnostic tool, are an affront to those privacy rights. In short, the government is telling U.S. citizens to leave their front doors open so that officials may walk through their homes when looking for the suspects they are pursuing. As it stands, the order is unendurable.

If Carnivore, or its successors, is to be tolerated by U.S. citizens and pass constitutional muster, extensive national and international work must be accomplished to alleviate privacy concerns. In the United States, the question of whether Carnivore is constitutionally permissible must be answered. In its current configuration, the answer is most likely no. Obtaining access to the precise nature of Carnivore's aims, exactly how it is used and its potential for abuse, will help provide the answers to further uncertainties about the investigative tool. Adopting comprehensive legislation, including the modification of existing laws to strengthen Internet users' privacy protections, could lead to a legislative scheme acceptable to both law enforcement agencies and those concerned about privacy. Internationally, the United States has to take the lead in convening countries' representatives to fashion solutions to what is a major global concern. Among those strategies employed by the group must be the adoption of worldwide policies that allow governments access to the electronic communications they need to engage in crime prevention while protecting worldwide Internet users' expectation of privacy. Contribution to these policies must be sought from a wide range of interested parties.

Conceptually, the ability of law enforcement agencies to be able to access the communications of criminals is benign. Most people would probably be willing to give up a certain degree of privacy in furtherance of the state's interest and

---

inconsistent privacy policies, merging personal financial data, wireless privacy battles, Microsoft cookie-blocking software, and electronic mail and World Wide Web activity sought in legal cases. *Id.*

140. Dennis Kennedy, *Changes to Come: Legal Technology Predictions for 2001*, IND. LAW., Jan. 3, 2001, at 9 (writing about statement of Jerry Lawson, lawyer and Internet expert).

responsibility in curtailing the growing number of crimes being conducted using the Internet as a means of communication. Most objectionable, however, about the government's approach to advanced electronic surveillance is the secrecy with which it has pursued its objectives. Without releasing the details of the Carnivore operating system and the precise agenda of the ILETS, the U.S. government could have nonetheless subjected itself to following basic procedures of formal rulemaking in administrative law—an opportunity for notice and comment. Notice would serve a dual purpose. First, it would provide forewarning to criminals that should they choose to engage in criminal conduct using the Internet, law enforcement agencies may have access to those communications. Second, it would provide those interested stakeholders with an assurance that the government values their input, whether that input were eventually to influence law enforcement agencies' policies. A period for comment would provide a means by which those interested parties could participate in the development of policy that affects one of their perceived indispensable rights. This democratic exercise could serve as a model to the broader international community working collectively with the United States toward achieving vital compatible goals—crime prevention and the preservation of individuals' right to privacy.