Harvard Journal of Law & Technology
Volume 15, Number 2 Spring 2002

IMPLICATIONS OF SELECT NEW TECHNOLOGIES FOR INDIVIDUAL RIGHTS AND PUBLIC SAFETY

*Amitai Etzioni**

TABLE OF CONTENTS

---

* In preparing this article I greatly benefited from extensive research assistance by Mackenzie Baris and from comments by Peter Swire, Orin Kerr, and Andrew Volmert.

INTRODUCTION

Are the new measures that have been introduced to protect America from terrorism too extensive, undermining our rights? Or are they not extensive enough, leaving the nation vulnerable to future attacks?[1] This Article focuses on those public safety measures pertaining to communications surveillance and, specifically, to six technologies: cellular phones, Internet communications, strong encryption, Carnivore, the Key Logger System ("KLS"), and Magic Lantern. It examines the law's effect on these technologies as well as on individual rights and the public interest.

This Article assumes that both individual rights and public safety must be protected. Given that on many occasions advancing one requires some curtailment of the other, the key question is what the proper balance between these two cardinal values is. The concept of balance is found in the Fourth Amendment. It refers to the right not to be subjected to *unreasonable* search and seizure.[2] Thus, it recognizes a category of searches that are fully compatible with the Constitution — those that are reasonable. Historically, courts have found searches to be reasonable when they serve a compelling public interest, such as public safety or public health.[3]

The debate about communications surveillance and individual rights has been characterized by strong advocacy on opposing sides. One side argues that public safety requires granting the government greater surveillance powers. These advocates warn that major calamities will strike if the government is not accorded these powers. Moreover, they claim that the best way to defend liberty is to provide the government with more authority. Dead people, they argue, are not free.[4]

---

1. After September 11, 2001, Congress introduced 158 separate provisions in the 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 (codified in scattered sections of U.S.C.) [hereinafter USA PATRIOT Act].

2. U.S. CONST. amend. IV.

3. *See, e.g.*, Vernonia School District 47J v. Acton, 515 U.S. 646, 661 (1995) (defining a compelling state interest as "an interest that appears *important enough* to justify the particular search at hand, in light of other factors that show the search to be relatively intrusive upon a genuine expectation of privacy."); United States v. Doe, 61 F.3d 107, 109-10 (1st Cir. 1995) ("[R]outine security searches at airport checkpoints pass constitutional muster because the compelling public interest in curbing air piracy generally outweighs their limited intrusiveness."); Marshall v. Horn Seed Co., 647 F.2d 96, 102 (10th Cir. 1981) (holding that "the compelling public interest in preventing or speedily abating hazardous conditions . . . demands relaxation of the traditional probable cause test for administrative inspections. . . .").

4. During the discussion of the USA PATRIOT Act on the Senate floor, Senator Hatch said, "I think of the civil liberties of those approximately 6,000 people who lost their lives, and potentially many others if we don't give law enforcement the tools they

Civil libertarians, on the other side, do not necessarily oppose making concessions to advance public safety, but they place the burden on the government to prove that such concessions are needed. They would set the bar very high for such proof, calling for an approach resembling "strict scrutiny."[5] Some have demanded a more restrictive definition of the conditions under which the new technologies can be used.[6] Others believe that the new powers are unnecessary and open the door for government abuses.[7]

Each side advocates an extreme position that prioritizes the public interest or individual rights, rather than recognizing that what is needed is a carefully crafted balance between the two. The quest for balance reflects a new or responsive communitarian position developed in the 1990s.[8] Its starting point is that there are two valid claims each society faces. First, society must advance the public interest, including not only public safety and health but also other elements of the common good, such as protection of the environment. Second, society must protect liberty, including individual rights.[9] The "turf" does not belong *a priori* to either claim. In addition, public safety and individual rights are not necessarily in conflict. In some situations, both can be advanced, such as when the police restore law and order to a crime-ridden neighborhood. However, when the public interest and rights do pose conflicting demands, criteria must be developed as to which should take priority, without assuming that one automatically trumps the other.[10] Judge Richard Posner put the same basic idea

---

need to do the job." 147 CONG. REC. S10,990-02 (daily ed. Oct. 25, 2001) (statement of Sen. Hatch).

5. Nadine Strossen, Remarks at the Communitarian Dialogue on Privacy vs. Public Safety (Nov. 26, 2001), *at* http://www.gwu.edu/~ccps/privtrans.html [hereinafter Strossen remarks].

6. *See, e.g.*, *Civil Rights and Anti-Terrorism Efforts: Hearing before the Senate Subcomm. on Constitution, Federalism and Property Rights of the Senate Comm. on the Judiciary*, 106th Cong. (2001) (statement of Jerry Berman, Executive Director, Center for Democracy and Technology).

7. *See* Letter from Laura W. Murphy, Director, ACLU Washington Office & Gregory T. Nojeim, Associate Director & Chief Legislative Counsel, ACLU, to Senate (Oct. 23, 2001) (urging rejection of the final version of the USA PATRIOT Act), http://www.aclu.org/congress/l102301k.html (last visited Mar. 26, 2002) [hereinafter Murphy letter].

8. For further detail on the responsive communitarian position, see The Responsive Communitarian Platform, *at* http://www.communitariannetwork.org/platformtext.htm (last visited Feb. 23, 2002); AMITAI ETZIONI, THE NEW GOLDEN RULE (1996) [hereinafter THE NEW GOLDEN RULE]; AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999) [hereinafter THE LIMITS OF PRIVACY]. For a critical treatment, see ELIZABETH FRAZER, THE PROBLEMS OF COMMUNITARIAN POLITICS (1999).

9. *See* THE NEW GOLDEN RULE, *supra* note 8, chs. 1–2.

10. For additional discussion of such criteria, see AMITAI ETZIONI, THE SPIRIT OF COMMUNITY 177–90 (1993) [hereinafter SPIRIT OF COMMUNITY]; THE NEW GOLDEN RULE, *supra* note 8, at 51–55; THE LIMITS OF PRIVACY, *supra* note 8, at 10–15.

in the following way: "Neither [the public-safety interest nor the liberty interest], in my view, has priority. They are both important."[11]

This general communitarian position is best understood within a historical context. Societies and polities tend to lean excessively toward the public interest or toward liberty. Corrections to such imbalances then tend to lead to over-corrections. For example, following the civil rights abuses that occurred during the years J. Edgar Hoover was the director of the FBI,[12] the Attorney General imposed severe limitations on the agency in the 1970s.[13] These limitations excessively curbed the agency's work in the following decades. The public safety measures enacted after September 11th removed many of these restrictions and granted law enforcement agencies and the military new powers. These changes arguably tilted excessively in the other direction. This over-correction was soon followed by an attempt to correct it (for example, by limiting the conditions under which military tribunals can be used and spelling out procedures not included in their preliminary authorization).[14] Historical conditions also change the point at which we find a proper balance. The 2001 assault on America and the threat of additional attacks have brought about such a change.

This Article argues that we should strive to achieve a balance by focusing on accountability. Part I introduces three technologies that have expanded individuals' liberties but have limited the ability of public authorities to conduct surveillance: cellular phones, the Internet, and strong encryption.[15] I shall refer to these technologies as *liberalizing technologies*. Part I then examines the arguments in favor of and against changing laws and regulations to enable public authorities to cope with, if not overcome, the hurdles posed by the liberalizing technologies in the post-September 11th context. Part II turns to three new technologies that help public authorities protect public safety but may curb individual rights: Carnivore, KLS, and Magic Lantern. I refer to these as *public protective technologies*. These technologies are then examined in light of new laws and regulations to discern their effect on the balance between the public interest and individual rights in the post-September 11th context. Finally, Part III discusses meas-

---

11. Richard A. Posner, *Security Versus Civil Liberties*, ATLANTIC MONTHLY, Dec. 2001, at 46.

12. For a short overview of FBI abuses during the 1970s and the responses to them, see 147 CONG. REC. S10,992–10,994 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

13. *See* THE FBI: A COMPREHENSIVE REFERENCE GUIDE 38 (Athan G. Theoharis ed., 1999) [hereinafter Theoharis].

14. *See* Katharine Q. Seelye, *Draft Rules for Tribunals Ease Worries, but Not All*, N.Y. TIMES, Dec. 29, 2001, at B7.

15. It should be noted that no attempt is made to fully describe or analyze the technologies at issue but merely to point to those features that are relevant to the issues at hand.

ures that might help increase public safety while minimizing the threat to individual rights, focusing on accountability. The proposals entail a measure of trust in the government or, at least, in some elements of it.

I. LIBERALIZING TECHNOLOGIES

A. New and Multiple Means of Communication

In 1980, the most convenient, and by far the most commonly used, way to communicate instantaneously with a person at a different location was through a wired telephone. Cellular phones existed, but they were not yet commercially viable, nor were they available in models lightweight enough to put in a pocket.[16] Fax machines had not yet come into wide use.[17] Telegraphs required, as a rule, going to a post office or Western Union location. Most people had one phone line. The Internet was still the Advanced Research Projects Agency's computer network, known as ARPANET, which mainly linked universities and research centers.[18] In 1980, communications surveillance could be carried out easily by attaching simple devices to a suspect's landline telephone.

In the following two decades, millions of people acquired several alternative modes of convenient, instantaneous communication, most significantly cellular telephones and e-mail. By July 2000, there were over 100 million cellular phone subscribers in the United States.[19] E-mail and Internet usage are similarly pervasive. Nielsen/Net Rating estimated that in January of 2002, 165.1 million people in the United States had home Internet access.[20] These technological developments greatly limited the ability of public authorities to conduct communications surveillance using traditional methods.

Before proceeding, it is necessary to define some terminology. There are two types of communications surveillance. First, public authorities may obtain "pen register" and "trap and trace" orders to gather only the numbers dialed to or from a specific telephone.[21] Alternatively, they may obtain more intrusive "full intercept" orders to

16. *See* JAMES B. MURRAY, JR., WIRELESS NATION 20 (2001).

17. *See* PHILIP C. W. SIH, FAX POWER 1–5 (1993).

18. *See* PETER H. SALUS, CASTING THE NET 83–84 (1995).

19. MURRAY, *supra* note 16, at 313.

20. Nielsen/NetRatings Audience Measurement Service, Average Web Usage for January 2002, *at* http://pm.netratings.com/nnpm/owa/NRpublicreports.usagemonthly (last visited Feb. 23, 2002) (on file with the Harvard Journal of Law and Technology).

21. *See* 18 U.S.C. §§ 3122–3123 (2000); *see also* United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (stating that a pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached) (Powell, J., concurring in part and dissenting in part).

listen to the content of a telephone call.[22] Law enforcement may obtain the first type of order more easily[23] because the information involved is less sensitive. The terms "pen register" and "trap and trace" refer to the devices originally used to carry out the trace orders.[24] Although the technologies they refer to have been replaced, these terms are still commonly used. In this Article, the term "pen/trap" will be used to designate the type of communications surveillance that gathers only the numbers dialed to and from a telephone or the addressing information in an e-mail message. The term "full intercept" will refer to wiretaps and other means of intercepting the full content of a communication. The term "communications surveillance" will include both pen/trap and full intercept orders.

Attempts were made to apply the old laws to new technologies, but the old laws did not fit the new technologies well. The law governing full intercepts, contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1969,[25] originally required that court orders for intercepts specify the location of the communications device to be tapped and establish probable cause that evidence of criminal conduct could be collected by tapping that particular device. Hence, under this law, if a suspect shifted from one phone to another or used multiple phones, the government could not legally tap phones other than the one originally specified without obtaining a separate court order for each.[26] Once criminals were able to obtain and dispose of multiple cellular phones like "used tissues,"[27] investigations were greatly hindered by the lengthy process of obtaining numerous full intercept authorizations from the courts.[28]

---

22. *See* 18 U.S.C. § 2518 (2000).

23. *See* Smith v. Maryland, 442 U.S. 735 (1979) (establishing that the use of a pen register to obtain the numbers dialed from a telephone does not constitute a search under the Fourth Amendment and therefore does not require a showing of probable cause).

24. "The term 'pen register' comes from the old style for tracking all of the calls originating from a single telephone. At one point, the surveillance technology for wiretapped phones was based on the fact that rotary clicks would trigger movements of a pen on a piece of paper." Peter P. Swire, *Administration Wiretap Proposal Hits the Right Issues but Goes Too Far* (Oct. 3, 2001), *in* AMERICA'S RESPONSE TO TERRORISM (The Brookings Institution, Washington, DC), *available at* http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm (last visited Apr. 1, 2002).

25. Omnibus Crime Control and Safe Streets Act of 1969, Pub. L. No. 90-351, 82 Stat. 197, 211 (1968) (codified at 18 U.S.C. §§ 2510–2521 (2000)) [hereinafter Title III].

26. 18 U.S.C. § 2518(1)(b)(ii) (2000).

27. Interview by Alan Hunt & Robert Novak, with Rep. Nancy Pelosi, 8th District of California, *Novak, Hunt & Shields* (CNN television broadcast, Oct. 27, 2001).

28. Victoria Toensing, Remarks at the Communitarian Dialogue on Privacy vs. Public Safety (Nov. 26, 2001), *at* http://www.gwu.edu/~ccps/privtrans.html [hereinafter Toensing remarks].

The rise of Internet-based communications further limited the ability of public authorities to conduct communications surveillance under the old laws. Title III did not originally mention electronic communications. Similarly, the language of the Electronic Communications Privacy Act of 1986 ("ECPA")[29] that governed pen/trap orders was not clearly applicable to e-mail.[30] To determine how to deal with this new technology, courts often attempted to draw analogies between e-mail and older forms of communication.[31] Because electronic communication used to travel largely over phone lines, courts extended laws governing intercepts or traces for telephones to electronic messages as well.[32] However, reliance by the police on such interpretations was risky because there was a possibility that a court would rule that e-mail did not fall under a pen/trap order.[33]

Extending laws that were written with telephones in mind to e-mail was an imperfect solution because e-mail messages differ from phone conversations in important ways. Unlike phone conversations, e-mails do not travel in discreet units that can be plucked out. Each e-mail is broken up into digital packets, and the packets are mixed together with those of other users.[34] This makes it difficult to intercept individual e-mails.[35] Law enforcement agents attempting to intercept or trace the e-mail of just one user may violate the privacy of other users.[36]

The decentralized nature of the Internet created additional complications in carrying out pen/trap orders. When the old legislation was enacted, a unified phone network made it easy to identify the

---

29. Pub L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 1367, 3121–3126 (2000)) [hereinafter ECPA].

30. "[T]he term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." ECPA § 301.

31. For a discussion of the various analogies applied, see Lt. Col. Joginder S. Dhillon & Lt. Col. Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques*, 50 A.F. L. REV. 135, 149 (2001).

32. *See id.*

33. *See* Swire, *supra* note 24.

34. *See* Christian D.H. Schultz, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215, 1221–23 (2001).

35. *See* Terrence Berg, *www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law*, 2000 BYU L. REV. 1305; James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997); Dhillon & Smith, *supra* note 31; Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996); Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VA. J.L. & TECH. 4 (2001).

36. *See* Swire, *supra* note 24.

source of a call.[37] E-mail, by contrast, may pass through multiple Internet service providers ("ISPs") in different locations throughout the nation on its way from sender to recipient. As a result, public authorities would have to compel information from a chain of service providers.[38] Thus, until recently, if a message went through four providers, four court orders in four different jurisdictions would be needed to find out the origin of that message.

Similarly, agents faced jurisdictional barriers when they tried to obtain search warrants for saved e-mail. Under old laws, a warrant had to be obtained from a judge in the jurisdiction where the search would take place.[39] E-mail, however, is not always stored on a personal computer but often is stored remotely on an ISP's server. This means that if a suspect in New Jersey had e-mail stored on a server located in Silicon Valley, an agent would have to travel across the country to get a warrant to seize the e-mail.[40]

In short, the introduction of both cellular phones and e-mail made it much more difficult to conduct communications surveillance, even in cases in which the court authorized such surveillance. The old laws and enforcement tools were not suited to deal with these new technologies.

Public authorities were also set back by the development of strong encryption.[41] Although ciphers have existed for thousands of years,[42] programmers have only recently developed 128-bit encryption. This level of encryption is said to be impossible to crack, even by the National Security Agency ("NSA").[43] Moreover, software that uses strong encryption is readily available to private parties at low cost. Stewart Baker, former General Counsel for the NSA, observed, "Encryption is virtually unbreakable by police today, with programs

---

37. *See id.*

38. *See* Dep't of Justice, Field Guide on the New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation § 216A, *available at* http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf (last visited Jan. 29, 2002) [hereinafter DOJ Field Guide].

39. *See* 18 U.S.C. § 2703(a) (2000) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant.").

40. *See* DOJ Field Guide, *supra* note 38, § 220.

41. *See* THE LIMITS OF PRIVACY, *supra* note 8, ch. 3.

42. *See* Deborah Russell & G.T. Gangemi, Sr., *Encryption*, *in* BUILDING IN BIG BROTHER 10, 11 (Lance Hoffman ed., 1995).

43. *See generally* DOROTHY E. DENNING & WILLIAM E. BAUGH, JR., ENCRYPTION AND EVOLVING TECHNOLOGIES AS TOOLS OF ORGANIZED CRIME AND TERRORISM (1997).

that can be bought for $15."[44] Today, manufacturers routinely prepackage these programs on computers.[45] Thus, encrypted messages are more private than any messages historically sent by mail, phone, messenger, carrier pigeon, or other means. Similarly, now data stored on one's own computer is protected much better than analogous data stored under lock and key. Despite court orders, strong encryption has frustrated the efforts of law enforcement in a growing number of cases.[46]

The impact of the development of strong encryption is qualitatively different from the impact of the other privacy-enhancing technologies. The main factor that constrained public authorities in the area of new modes of communication was the obsolescence of laws. In the case of strong encryption, on the other hand, the technology imposes its own barrier. Updating the law was sufficient to enable law enforcement to handle the challenges posed by the other new technologies. By contrast, no court order can enable strong encryption to be broken.

B. Legal Responses

These technological developments have provided all people — law-abiding citizens and criminals, non-terrorists and terrorists — greater freedom to do as they choose. In this sense, these technologies are "liberalizing." At the same time, they have significantly hampered the ability of public authorities to conduct investigations. Some cyberspace enthusiasts welcomed these developments, hoping that cyberspace would be a self-regulating, government-free space.[47] In contrast, public authorities clamored for the laws to be changed in order to enable officials to police the new "territory" as they do in the world of old-fashioned, landline telephones.[48] Such pressures led to some

---

44. Jonathan Krim, *High-Tech FBI Tactics Raise Privacy Questions*, WASH. POST, Aug. 14, 2001, at A1.

45. STEVEN LEVY, CRYPTO 310–11 (2001).

46. FBI Director Louis J. Freeh stated, "From 1995 to 1996, there was a two-fold increase (from 5 to 12) in the number of instances where the FBI's court-authorized electronic efforts were frustrated by the criminal's use of encryption that did not allow for law enforcement access." *Worldwide Threats to National Security: Hearing Before the Senate Select Comm. on Intelligence*, 105th Cong. 27 (1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) [hereinafter Freeh statement]; *see also* THE LIMITS OF PRIVACY, *supra* note 8, ch. 3.

47. *See* John Perry Barlow, Cyberspace Independence Declaration, *at* http://www.eff.org/~barlow/Declaration-Final.html (Feb. 8, 1996); *see also* Steven Levy, *The Battle of the Clipper Chip*, N.Y. TIMES MAG., June 12, 1994, at 44.

48. FBI Director Louis J. Freeh testified:

> The looming spectre of the widespread use of robust, virtually untraceable encryption is one of the most difficult problems confronting law enforcement as the next century approaches. At stake are some of our most valuable and reliable investigative

modifications in the law before the 2001 attack on America, but the most relevant changes in the law have occurred since. The following sections examine the expansion of authorities' surveillance powers.

1. Roving Intercepts

One provision of ECPA attempted to update the laws governing communications intercepts to be more effective by providing for "roving wiretaps" in criminal investigations.[49] Roving wiretaps are full intercept orders that apply to a particular person rather than to a specific communications device. They allow law enforcement to intercept communications from any phone or computer used by a suspect without specifying in advance which facilities will be tapped.[50]

The process for obtaining a roving intercept order is more rigorous than the process for obtaining a traditional phone-specific order. The United States Attorney General's office must approve the application before it is even brought before a judge.[51] Originally, the applicant had to show that the suspect named in the application was changing phones or modems frequently with the *purpose* of thwarting interception.[52] After the Intelligence Authorization Act for Fiscal Year 1999 changed the requirement, the applicant merely had to show that the suspect was changing phones or modems frequently and that this practice "could have the effect of thwarting" the investigation.[53] Although roving intercepts have not yet been tested in the Supreme Court, several federal courts have found them to be constitutional.[54]

Prior to September 11th, the FBI could not gain authorization to use roving intercepts in gathering foreign intelligence or in investigations of terrorism. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

---

> techniques, and the public safety of our citizens. We believe that unless a balanced approach to encryption is adopted that includes a viable key management infrastructure, the ability of law enforcement to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired.

Freeh statement, *supra* note 46.

49. *See* ECPA, Pub L. 99-508, § 106(d)(3), 100 Stat. 1848, 1857 (1986) (codified as amended at 18 U.S.C. § 2518(11) (2000)).

50. *See* 18 U.S.C. § 2518(11)(b) (2000).

51. *See id.*

52. *See id.*

53. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998) (codified as amended at 18 U.S.C. § 2518(11)(b) (2000)).

54. *See, e.g.*, United States v. Petti, 973 F.2d 1441, 1444–45 (9th Cir. 1992); *see also* Bryan R. Faller, Note, *The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better*, 60 OHIO ST. L.J. 2093 (1999).

Act of 2001 ("USA PATRIOT Act")[55] amended the Foreign Intelligence Surveillance Act of 1978 ("FISA")[56] to allow roving intercept orders.[57] FISA provides the guidelines under which a federal agent can obtain authorization to conduct surveillance for foreign intelligence purposes.[58] Agents who wish to conduct surveillance under FISA submit an application first to the Attorney General's office, which must approve all requests (as with roving intercepts under ECPA). If the Attorney General's office finds the application valid, the application will be taken to one of seven federally appointed judges, who together make up the Federal Intelligence and Security Court ("FISC"), for approval. The FISC allows no spectators, keeps most proceedings secret, and hears only the government's side of a case.[59]

Initially, FISA was limited to investigations for which foreign intelligence was the sole purpose. The USA PATRIOT Act modified FISA so that foreign intelligence need be only a "significant purpose" of an investigation.[60] This change effectively allows FISA to be used as part of "multi-faceted responses to terrorism, which involve foreign intelligence and criminal investigations."[61] Because FISA was originally designed for use in gathering foreign intelligence, communications surveillance conducted under FISA differs from that conducted under Title III criminal investigations in several ways. Under normal Title III intercepts, when a law enforcement officer intercepts an individual's communication, that individual must be notified after the fact. Under FISA, the individual need not be notified unless evidence obtained through the interception will be used against him in court.[62] Furthermore, for national security reasons, defendants are not permitted access to the information the law enforcement official relied upon in his or her application to conduct the surveillance, thus increasing the difficulty of challenging the use of such evidence in court.[63]

---

55. USA PATRIOT Act (2001), Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of U.S.C.).

56. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 18 U.S.C. §§ 2511, 2518–2519 (2000), 47 U.S.C. § 605 (2000), 50 U.S.C. §§ 1801–1811 (2000)) [hereinafter FISA].

57. *See* USA PATRIOT Act § 206.

58. *See* FISA § 102.

59. *See* Tom Ricks, *A Secret U.S. Court Where One Side Always Seems to Win*, CHRISTIAN SCI. MONITOR, May 21, 1982, at 1.

60. USA PATRIOT Act § 218; *see also* 147 CONG. REC. S11,003–11,004 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

61. 147 CONG. REC. S11,055 (daily ed. Oct. 25, 2001) (Department of Justice overview of USA PATRIOT Act) [hereinafter DOJ Overview].

62. *See* FISA § 106.

63. *See* William Carlsen, *Secretive U.S. Court May Add to Power*, S.F. CHRON., Oct. 6, 2001, at A3.

2. E-mail

Although ECPA had explicitly extended full intercept orders to apply to electronic communications, it defined pen/trap orders in such a way as to exclude electronic communications. The USA PATRIOT Act included provisions to make it easier for public authorities to trace or seize e-mail. It explicitly allows pen/trap orders for computer communications.[64] Instead of requiring multiple court orders in each jurisdiction through which an electronic message has passed,[65] the Act establishes what are *de facto* nationwide pen/trap orders,[66] allowing one court order to be used on all the carriers through which a message has passed. When a law enforcement agent discovers that an e-mail message was forwarded to or from any carrier, he can serve the original court order on this carrier without getting an additional order from the court in whose jurisdiction the carrier is located. Moreover, because agents cannot know in advance which carriers will be involved, the court order need only specify the initial facility at which the pen/trap order will be carried out. The USA PATRIOT Act also allows a judge in the district with jurisdiction over the crime under investigation to grant search warrants to seize electronic communications stored on an ISP located outside that judge's jurisdiction.[67]

3. Encryption

Previous administrations attempted to pass legislation requiring that "back doors" be built into encryption software to enable public authorities to decrypt otherwise unbreakable codes when needed.[68] They also attempted to enact legislation that would require users of cryptographic software to deposit a copy of their key with third parties — referred to as "escrow" — or with public authorities, who would not be able to look at or use the key unless authorized to do so as part of an investigation.[69] A combination of civil liberties groups

64. *See* USA PATRIOT Act §§ 214, 216.

65. *See id.* § 216(a); *see also* DOJ Field Guide, *supra* note 38, § 216A.

66. The law is worded in a peculiar way, saying that a single order can be used at any carrier's facility but not explicitly establishing that the order has nationwide scope. *See* USA PATRIOT Act § 216(a).

67. *See id.* § 220; *see also* DOJ Field Guide, *supra* note 38, § 220.

68. *See* THE LIMITS OF PRIVACY, *supra* note 8, at 100. *See generally* LEVY, *supra* note 45, at 226–68.

69. *See, e.g.*, Bruce W. McConnell & Edward J. Appal, Draft Paper, Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure, *at* http://www.epic.org/crypto/key_escrow/white_paper.html (May 20, 1996); *Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Senate Subcomm. on the Constitution, Federalism, and Property Rights of the Comm. on the Judiciary*, 105th Cong. 20 (1998) (statement of Robert S. Litt, Principal Assoc. Deputy Att'y Gen.). For a fuller history of key escrow, see A. Michael Froomkin, *It*

and high-tech corporations successfully fought off both of these attempts.[70] No attempts to address this matter were included in the USA PATRIOT Act.

4. Evaluating the Changes in the Law

a. General

The adaptations of the laws governing communications surveillance and seizures of stored communications have been subject to both general and detailed debates. At the general level, these adaptations have been lumped together with other matters such as the indefinite detention of aliens,[71] surveillance of attorney-client conversations,[72] and military tribunals.[73] In the general debate, commentators have often used inflammatory rhetoric. For example, Senator Patrick Leahy stated that some of the measures are "shredding the Constitution,"[74] and Morton Halperin referred to the new legislation as "Striking Terror at Civil Liberty."[75] On the other side, Senator Hatch dismissed such misgivings as "hysterical concerns" and said the American people do not want to see Congress "quibble about whether we should provide more rights than the Constitution requires to the criminals and terrorists who are devoted to killing our people."[76] Attorney General John Ashcroft suggested that criticisms of the new

---

Came from Planet Clipper: The Battle over Cryptographic Key "Escrow," 1996 U. CHI. LEGAL F. 15 (1996).

70. *See* Jeri Clausing, *White House Yields a Bit on Encryption*, N.Y. TIMES, July 8, 1998, at D1; *see also* Lance J. Hoffman, Encryption Policy for the Global Information Infrastructure, Keynote Address to the 11th International Conference on Computer Security (May 9–12, 1995), *at* http://www.cpi.seas.gwu.edu/library/docs/ictsp-95-01.pdf (last visited Apr. 1, 2002).

71. *See* USA PATRIOT Act § 412.

72. *See* National Security; Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. 55,062 (Oct. 31, 2001) (to be codified at 28 C.F.R. pt. 500–501).

73. *See* Military Order of November 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57,833 (Nov. 16, 2001).

74. "We don't protect ourselves by bending or even shredding our Constitution. We protect ourselves by upholding our Constitution and demonstrating to the rest of the world we will defend ourselves, but we will do it by also defending our own core values." *This Week* (ABC News television broadcast, Nov. 18, 2001) (statement of Sen. Leahy).

75. Morton H. Halperin, *Less Secure Less Free; Striking Terror at Civil Liberty*, AM. PROSPECT, Nov. 19, 2001, at 10.

76. *DOJ Oversight: Preserving Our Freedoms While Defending Against Terrorism: Hearing before the Senate Comm. on the Judiciary*, 107th Cong. (2001) (statement of Sen. Hatch).

powers requested by the executive branch serve only to "aid terrorists" and "erode our national unity and diminish our resolve."[77]

b. Fourth Amendment

There has been some debate in the courts and among legal scholars about the application of the Fourth Amendment to the new technologies and to the new legislation governing these technologies. Before 1967, the Supreme Court interpreted the Fourth Amendment in a literal way to apply only to physical searches. In *Olmstead v. United States*,[78] the Court ruled that telephone wiretaps did not constitute a search unless public authorities entered a home to install the device.[79] The Court held that the Fourth Amendment does not protect a person unless "there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house . . . ."[80]

In 1967, the Court replaced this interpretation of the Fourth Amendment with the view that the Amendment "protects people, not places."[81] In *Katz v. United States*,[82] the Court established that an individual's "reasonable expectation of privacy" would determine the scope of his Fourth Amendment protection.[83] Justice Harlan, in his concurring opinion, set out a two-part test: the individual must have shown a subjective expectation of privacy, and society must recognize that expectation as reasonable.[84]

Although legal scholars have criticized this test,[85] *Katz* still represents the state of the law. However, the emergence of new technologies requires a reexamination of what constitutes a reasonable expec-

---

77. Attorney General Ashcroft told Congress that tactics of attempting to scare citizens with "phantoms of lost liberty . . . only aid terrorists [and] give ammunition to America's enemies . . . ." *Anti-Terrorism Policy Review: Hearing before the Senate Comm. on the Judiciary*, 107th Cong. (2001) (statement of John Ashcroft, Attorney General of the United States).

78. 277 U.S. 438 (1927).

79. *See id.* at 466.

80. *Id.*

81. Katz v. United States, 389 U.S. 347, 351 (1967).

82. *Id.*

83. *Id.*

84. *See id.* at 361 (Harlan, J., concurring).

85. *See, e.g.*, State v. Reeves, 427 So. 2d 403, 425 (La. 1982) (Dennis, J., dissenting); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384–85 (1974); Jonathan Todd Laba, *If You Can't Stand the Heat, Get Out of the Drug Business: Thermal Imagers, Emerging Technologies, and the Fourth Amendment*, 84 CAL. L. REV. 1437, 1470–75 (1996); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751 (1994); Richard S. Julie, Note, *High-tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127, 131–33 (2000).

tation of privacy. In *United States v. Maxwell*,[86] the court determined that there was a reasonable expectation of privacy for e-mail stored on America Online's "centralized and privately-owned computer bank."[87] However, the court in *United States v. Charbonneau*,[88] relying on *Maxwell*, held that an individual does not have a reasonable expectation in statements made in an Internet chat room.[89]

Lieutenant Colonel Joginder Dhillon and Lieutenant Colonel Robert Smith argue that individuals may not have a reasonable expectation of privacy in e-mail.[90] They point out that e-mail resides on numerous servers between the sender and recipient, and on some networks, the system administrator keeps copies of all e-mails.[91] For similar reasons, the Supreme Court found in *Smith v. Maryland*[92] that there is no reasonable expectation of privacy in the telephone numbers that one dials because those numbers must be conveyed to the phone company.[93] Dhillon and Smith conclude that, at the very least, *Smith v. Maryland* means that recording e-mail addressing information does not require a full intercept order.[94]

Additionally, there is some question as to whether roving intercepts are constitutional. The Fourth Amendment states, "[N]o 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."[95] Because roving intercepts cannot name the location to be tapped, they may violate the particularity requirement of the Fourth Amendment.

The argument in favor of their constitutionality is that the particularity of the *person* to be searched is substituted for the particularity of the *place* to be searched. In *United States v. Petti*,[96] the Ninth Circuit Court of Appeals upheld the use of roving intercepts. It explained that the purpose of the "particularity requirement was to prevent general searches."[97] As long as a warrant or court order provides "sufficient

86. 45 M.J. 406 (C.A.A.F. 1996)

87. *Id.* at 417.

88. 979 F. Supp. 1177 (S.D. Ohio 1997).

89. *See id.* at 1185.

90. *See* Dhillon & Smith, *supra* note 31, at 150.

91. *See id.*

92. 442 U.S. 735 (1979)

93. *See id.* at 744; *see also* COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2001) (discussing the implications of *Smith* for seizure of electronic communications), *available at* http://www.usdoj.gov/criminal/cybercrime/searchmanual.wpd (last visited Apr. 1, 2002).

94. Dhillon & Smith, *supra* note 31, at 150.

95. U.S. CONST. amend. IV (emphasis added).

96. 973 F.2d 1441 (9th Cir. 1992).

97. *Id.* at 1444 (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)).

particularity to enable the executing officer to locate and identify the premises with reasonable effort," and there is no "reasonable probability that another premise might be mistakenly searched," it does not violate the Fourth Amendment.[98] In other words, a court order to tap all phones used by a specific person *does* describe particular places but in an unconventional way. Public authorities cannot use the order to tap any location they wish. They can only tap a set of specific locations, namely those used by a specific person.[99]

Not everyone agrees that this substitution of particularity of person for particularity of place is sufficient to satisfy the Fourth Amendment. Tracey Maclin argues that search warrants that specify only the target of the search and not the locations to be searched are constitutionally flawed.[100] To support her argument, she cites *Steagald v. United States*,[101] in which the Supreme Court concluded that law enforcement officers may not search a private place not specified in a search warrant even in pursuit of a person who was named in the warrant. Furthermore, argues Maclin, roving warrants do not effectively limit a search to a single individual. Once public authorities decide to "tap" a telephone or computer, everyone using that telephone or computer will be subject to surveillance. Therefore, there is no true particularity of person maintained.[102]

In contrast, Clifford Fishman finds that there are strong arguments in favor of the constitutionality of roving intercepts. He contends that roving intercept orders "describe the 'place' to be searched in a somewhat untraditional but still sufficiently particular way."[103] Furthermore, he argues that "[i]f the Fourth Amendment is flexible enough to protect privacy against technological developments far beyond the contemplation of the founding fathers, as it should be, then it also must be flexible enough to permit investigators to preserve the basic mandate of the amendment's particularity requirement in novel ways."[104]

---

98. *Id.* (quoting United States v. Turner, 770 F.2d 1508, 1510 (9th Cir. 1985)).

99. *See* 18 U.S.C. § 2518(11)(b)(iv) (2000) (specifying that in the case of a roving intercept, "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted"); 18 U.S.C. § 2518(12) (2000) (requiring that the interception "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order").

100. Tracey Maclin, *Another Grave Threat to Liberty*, NAT'L L.J., Nov. 12, 2001, at A20.

101. 451 U.S. 204 (1981).

102. Maclin, *supra* note 100, at A20.

103. Clifford S. Fishman, *Interception of Communication in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1, 65–66 (1987).

104. *Id.* at 68–69.

Additional questions may arise regarding differential application of the laws to various classes of people. Should non-citizens be treated the same as citizens? Terrorists the same as other criminals? International terrorists the same as domestic terrorists? These are significant issues that go to the heart of the debate about the rights of non-citizens. These issues raise potential problems, such as how to define terrorism and whether that definition should extend to citizens, as well as the danger that a loose definition might allow ordinary criminals to be encompassed by terrorism laws. These issues go beyond the scope of this Article and are not addressed here, but it is worth noting that they have implications for the issues at hand.

c. Policy Critiques

Proponents of roving intercepts argue that, without the intercepts, authorities will see a "whole operation frustrated because a terrorist throws away a telephone and picks up another phone and then moves on."[105] Critics argue that the new law will ensnarl many innocent people unrelated to investigations. Civil libertarians such as Nadine Strossen argue that the new law relating to roving intercepts "goes far beyond" facilitating investigations based on individual suspicion.[106] She argues that it would allow the government to intercept communications of individuals who are not under suspicion. For example, if the FBI taps a public library computer from which a suspected terrorist sends e-mail, any of the other users, who have no connection to the suspect, will also have their communications intercepted.

Other critics contend that issuing nationwide warrants allows law enforcement agents to "shop for friendly judges."[107] Senator Hatch counters that these provisions and others merely fix parts of the criminal code that formerly treated terrorists "with kid gloves."[108]

Although the American Civil Liberties Union ("ACLU") has criticized the new measures overall, it has hinted that it is somewhat less troubled by the changes in the laws governing roving intercepts than many of the other measures.[109] Even Alan Dershowitz, a long-

105. Interview by Larry King with Ted Olsen, United States Solicitor General, *Larry King Live* (CNN television broadcast, Oct. 24, 2001).

106. Interview by Monita Rajpal with Nadine Strossen, President, ACLU, *Has the War on Terror Created a New Threat Against Civil Liberties?* (CNN International broadcast, Oct. 30, 2001).

107. Bart Kosko, *Your Privacy Is a Disappearing Act*, L.A. TIMES, Dec. 2, 2001, at M5.

108. Adam Clymer, *Antiterrorism Bill Passes, U.S. Gets Expanded Powers*, N.Y. TIMES, Oct. 26, 2001, at A1 (quoting Sen. Hatch).

109. *See* Strossen remarks, *supra* note 5.

time defender of civil liberties, has stated that roving intercepts are "a very good idea."[110]

The ACLU also criticizes changes in FISA, which allow authorities to "by-pass normal criminal procedures that protect privacy and take checks and balances out of the law."[111] I shall defer my own assessment of the effect of the legal adaptations to liberalizing technologies on the balance between individual rights and public safety and health until Part III.[112]

II. PUBLIC PROTECTIVE TECHNOLOGIES

The discussion now turns to three technologies with opposite characteristics of those discussed so far. The liberalizing technologies that I have already addressed enhance individuals' liberties and hinder public authorities. The following technologies are public protective technologies, which enhance the capabilities of government authorities and can curtail individual rights.

A. Carnivore

Carnivore, a computer program unveiled by the FBI in July of 2000, can capture a suspect's e-mail messages or trace messages sent to and from his account.[113] To do so, it sorts through a stream of many millions of messages, including those of many other users.[114] Carnivore has a filter that can be set to scan various digital packets for specific text strings or to target messages from a specific computer or e-

110. Interview by Monita Rajpal with Alan Dershowitz, Professor of Law, Harvard Law School, *Has the War on Terror Created a New Threat Against Civil Liberties?* (CNN International broadcast, Oct. 30, 2001).

111. ACLU, *USA PATRIOT Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances*, *at* http://www.aclu.org/congress/l110101a.html (Nov. 1, 2001).

112. It should be noted that this Article does not deal with the general legitimacy of FISA or the USA PATRIOT Act but only with those elements of the laws that relate to communication surveillance. To the extent that criticism of these laws touches upon other matters, such as military tribunals and indefinite detention of suspects, analysis of that criticism is beyond the scope of this Article.

113. *See Internet and Data Interception Capabilities Developed by FBI: Hearing Before the House Subcomm. on the Constitution of the House Comm. on the Judiciary*, 105th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, FBI), *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm (last visited Apr. 1, 2002) [hereinafter July 2000 Kerr statement].

114. Some ISPs have the capability of doing this sorting themselves and will simply pass the appropriate information to agents after a warrant or court order is presented. The FBI uses Carnivore only if an ISP is not capable of doing this sorting. *See* Letter from Assistant Director John Collingwood to Members of Congress on Carnivore Diagnostic Tool, *at* http://www.fbi.gov/congress/congress00/collingwood 081600.htm (Aug. 16, 2000).

mail address.[115] The program can operate in two different modes: "pen" or "full." In pen mode, it will capture only the addressing information, which includes the e-mail addresses of the sender and recipient as well as the subject line. In full mode, it will capture the entire content of a message.[116] Carnivore is designed to copy and store only information caught by the filter, thus keeping agents from looking at any information not covered by the court order.[117] (Note that there are different "editions" of Carnivore, and these statements may not apply equally to all of them.)[118]

Carnivore's pen mode is valuable to public authorities even if the messages' contents cannot be read due to encryption because the government may benefit from an analysis of the addresses. For instance, the FBI can use pen/trap orders to trace to whom a group of suspects address their e-mail. When the program is used in pen mode, it would make more sense to call Carnivore — which, despite its name, hardly devours the messages — a communications traffic analyzer.

Carnivore has only been used in a limited number of circumstances. As of the fall of 2000, the FBI said that it had used Carnivore "approximately 25 times in the last two years."[119] In addition, it is stored in an FBI laboratory and is only brought out when needed to fulfill a specific court order. After the court order has expired, the program is returned to the laboratory.[120]

B. The Key Logger System and Magic Lantern

Despite the introduction of Carnivore, the government has been greatly hobbled by its inability to decrypt a rapidly growing proportion of messages.[121] To overcome this limitation, the FBI has devel-

---

115. *See* ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, INDEPENDENT REVIEW OF CARNIVORE SYSTEM — FINAL REPORT §§ 3.4.4.1.1, 3.4.4.1.4, 3.4.4.1.6, http://www.epic.org/privacy/carnivore/carniv_final.pdf (Dec. 8, 2000) [hereinafter IITRI Report].

116. *See id.* § 3.4.4.1.3.

117. *See* July 2000 Kerr Statement, *supra* note 113, at 7.

118. Interview with Peter Swire, Visiting Professor of Law, George Washington University, in Washington, D.C. (Mar. 19, 2002).

119. *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary,* 106th Cong. (statement of Donald M. Kerr, Assistant Director, Laboratory Division, FBI), http://www.fbi.gov/congress/congress00/kerr090600.htm (last visited Apr. 1, 2002) [hereinafter Sept. 2000 Kerr statement].

120. *See* July 2000 Kerr statement, *supra* note 113, at 14.

121. *See* 1999 Budget Request: Hearing Before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies of the House Appropriations Comm., 105th Cong. (1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress98/hac35.htm (last visited Mar. 26, 2002); *see also* Freeh Statement, *supra* note 46.

oped two new technologies to obtain a suspect's password: the Key Logger System ("KLS") and Magic Lantern. The password allows law enforcement to decrypt messages protected by sophisticated encryption schemes that are virtually impossible to decode.[122]

Once agents discover that they have seized encrypted information, they can seek a warrant to install and retrieve KLS.[123] In the case of Nicodemo Scarfo, a suspected racketeer, agents had to show both probable cause that Scarfo was involved in crime and probable cause that evidence of criminal activity was encrypted on his computer before installing KLS.[124] As in other warrants, the FBI had to specify the exact location of the computer on which KLS would be installed.[125]

Once installed, KLS uses a "keystroke capture" device to record keystrokes as they are entered into a computer. It is not capable of searching or recording fixed data stored on the computer. Moreover, KLS is designed so that it is unable to record keystrokes while a computer's modem is in operation[126] because intercepting electronic communications would require an intercept order that is more difficult to get than a warrant.[127]

In November 2001, the FBI revealed that it has developed but not yet implemented a less invasive technology called Magic Lantern.[128] Because KLS must be manually installed on a suspect's computer, it requires breaking and entering into a suspect's home.[129] In contrast,

---

122. The public encryption key is usually a long string of computer data that the user cannot simply memorize. Instead, the user has a pass phrase that enables him to decrypt his files. When the pass phrase is entered into a dialog box, the program then decrypts the key and uses it to decrypt the file. *See* Affidavit of Randall S. Murch at 3–4, United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) (No. 00-404), *available at* http://www.epic.org/crypto/scarfo/murch_aff.pdf (Oct. 4, 2001) [hereinafter Murch Affidavit].

123. *See Judge Orders Government to Explain How "Key Logger System" Works*, ANDREWS COMPUTER & ONLINE INDUS. LITIG. REP., Aug. 14, 2001, at 3.

124. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 577 (D.N.J. 2001).

125. *See In re* Application of the United States of America for an Order Authorizing the Surreptitious Entry into the Premises of Merchant Services of Essex County, Located at 149 Little Street, Belleville, New Jersey, for the Purpose of Conducting a Search for Evidence of Violations of Title 18, U.S.C. §§ 371, 892–894, 1955 and 1962, at 1–4, *Scarfo* (No. 00-404), *available at* http://www2.epic.org/crypto/scarfo/order_5_99.pdf (May 8, 1999) [hereinafter Scarfo warrant].

126. *See* Murch Affidavit, *supra* note 122, at 6–7. The component that records the keystrokes can be set to evaluate each keystroke individually before recording it. When a keystroke is entered, KLS checks the status of the computer's communication ports. The component will only record a keystroke if all the communications ports are inactive. *See id.*

127. *See* 18 U.S.C. §§ 3122–3123, 2516 (2000).

128. Ted Bridis, *FBI Is Building "Magic Lantern"; Software Would Allow Agency to Monitor Computer Use*, WASH. POST, Nov. 23, 2001, at A15.

129. KLS is arguably more invasive than "back doors" and key escrow, which were never adopted due to opposition by civil libertarians and high-tech businesses. *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

Magic Lantern allows the FBI to put software on a computer to record keystrokes without installing any physical device.[130] Like KLS, Magic Lantern cannot decrypt e-mail by itself but can retrieve the suspect's password. The details of how it does this have not been released.[131] It is said to install itself on the suspect's computer in a way similar to a Trojan horse computer virus.[132] It disguises itself as an ordinary, harmless message, then inserts itself onto a computer. For example, when someone connects to the Internet, a pop-up box could appear, stating "Click here to win!" When the user clicks on the box, the virus will enter the computer.[133]

C. Evaluating the New Technologies

Just as laws were put in place both before and after September 11th to limit the concerns that new liberalizing technologies posed for public safety, measures have also been introduced that limit the use of new protective technologies and address the concerns they pose for individual rights. Most of the limitations on the use of Carnivore and KLS were put in place as these technologies developed and before they were used, though there have also been "additions" to the checks placed on them. The shift from KLS to Magic Lantern can be considered an improvement from a rights viewpoint because Magic Lantern will not require covert breaking and entering by a law enforcement agent to install it on a suspect's office or home computer.

Groups like the Electronic Privacy Information Center ("EPIC") and the Center for Democracy and Technology ("CDT") have raised multiple arguments for why Carnivore should not be used at all. They are skeptical that Carnivore operates as the FBI claims and are troubled by the degree of secrecy the FBI maintains about the way it works.[134] Furthermore, they argue that separating addressing information from content is more difficult for Internet communications than for phone calls.[135] Therefore, Carnivore, they say, will not allow the

---

130. Bridis, *supra* note 128.

131. Bob Port, *Spy Software Helps FBI Crack Encrypted Mail*, DAILY NEWS, Dec. 9, 2001, at 8.

132. *See id.*

133. *See* Lou Dolinar, *Upping the Pressure: With New Tools and Laws, Authorities Can Target Suspects' Computers with Accuracy*, NEWSDAY, Dec. 12, 2001, at C8.

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

135. *Carnivore's Challenge to Privacy and Security Online: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 107th Cong. (2001) (statement of Alan Davidson, Staff Counsel, Center for Democracy and Technology), *available at* http://www.cdt.org/testimony/000724davidson.shtml ("Finding the addressee of an email or the name of a web site being visited — if that is what law enforcement is seeking — will often require analysis of the content of packets, not just the header information.") [hereinafter Davidson statement].

FBI to do a pen/trap without seizing more information than authorized. Privacy advocates also worry that Carnivore violates the Fourth Amendment because it scans through "tens of millions of e-mails and other communications from innocent Internet users as well as the targeted suspect."[136] The ACLU compares a Carnivore search to the FBI sending agents into a post office to "rip open each and every mail bag and search for one person's letters."[137]

Officials at the FBI respond that when used properly, Carnivore will capture only the targeted e-mails. Additionally, Carnivore's use is subject to strict internal review and requires the cooperation of technical specialists and ISP personnel, thus limiting the opportunities an unscrupulous agent might have to abuse it.[138]

A review of Carnivore conducted by the Illinois Institute of Technology concluded that although it does not completely eliminate the risk of capturing unauthorized information, Carnivore is better than any existing alternatives because it can be configured to comply with the limitations of a court order.[139] However, the report also determined that failure to include audit trails makes the FBI's internal review process deficient.[140] Specifically, the operator implementing a Carnivore search selects either pen or full mode by clicking a box on a computer screen,[141] and the program does not keep track of what kind of search has been run.[142] Therefore, it is difficult, if not impossible, to determine if an operator has used the program only as specified in the court order. Furthermore, it is impossible to trace actions to specific individuals because everyone uses the same user ID.[143] The head of the review panel commented, "Even if you conclude that the software is flawless and it will do what you set it to do and nothing more, you still have to make sure that the legal, human, and organizational controls are adequate."[144] This focus on accountability will be explored below.

There is a tendency to assign human attributes to computers. For example, commentators often talk or write about computers as if they "sniff" and "snoop."[145] However, a computer does not ogle, snicker

136. ACLU, Urge Congress to Stop the FBI's Use of Privacy-Invading Software, *at* http://www.aclu.org/action/carnivore107.html (last modified Feb. 5, 2002).

137. *Id.*

138. *See* July 2000 Kerr statement, *supra* note 113.

139. *See* IITRI Report, *supra* note 115, §§ ES.5–ES.6.

140. *See id.* § ES.5.

141. *See id.* §§ ES.5–ES.6.

142. *See id.* §§ ES.4–ES.5.

143. *Id.* § 4.2.4.

144. John Schwartz, *Wiretapping System Works on Internet, Review Finds*, N.Y. TIMES, Nov. 22, 2000, at A19 (quoting Henry Perritt Jr.) (internal quotation marks omitted).

145. *See, e.g.*, Charles Pillar, *"Lies" Propagates One Truth: No One Can Get a Lock on Net Security*, L.A. TIMES, Oct. 30, 2000, at C3 ("[T]he FBI's 'Carnivore'

at, or get aroused by a picture of a nude person. It does not "see" because its "mind" processes only ones and zeros. Thus, if millions of messages pass through a computer monitored by Carnivore, none of them is "read" *unless* it is caught by the filter and passed on to a human observer. Computers do not "read" or "scan" messages any more than phones "listen" to messages left in their voice mail box. Ultimately, what matters is what humans do.

Critics have also voiced concerns about KLS and Magic Lantern. In *United States v. Scarfo*,[146] the defendant challenged the legality of KLS. In that case, the FBI had used KLS to decrypt records implicating Scarfo in racketeering.[147] Scarfo's counsel argued that KLS recorded keystrokes sent over a modem and, therefore, should have required a Title III order rather than an easier-to-obtain search warrant.[148] Although the FBI claimed that KLS cannot record keystrokes while a modem is in operation, thus protecting against the capture of electronic communications, Scarfo and the privacy advocates interested in the case were skeptical. During the trial, Scarfo was shown a hard copy of all of the keystrokes intercepted but was unable to pick out anything that he recognized as being part of an electronic communication.[149] The court found that KLS did not operate while the computer's modem was activated and thus did not violate Title III by intercepting communications without the proper court order.[150]

The defendant also argued that KLS violated the particularity requirement of the Fourth Amendment and constituted a general search because a search warrant authorizing the use of KLS could not describe specifically what was to be searched and seized.[151] The warrant in *Scarfo* was issued to get one password, but KLS recorded every keystroke typed.[152] David Sobel of EPIC observed, "It's as if the government had a warrant to seize one book in your house, but was allowed to haul out everything that's in there."[153]

---

technology, which sniffs millions of supposedly private e-mail messages."); Bart Kosko, *supra* note 107, at M5 ("Carnivore snoops through the millions of e-mail and Web site bit packets . . . .").

146. 180 F. Supp. 2d 572 (D.N.J. 2001).

147. *Id.*

148. Motion to Suppress Evidence Seized by the Government Through the Use of a Keystroke Logger, at 3, *Scarfo* (No. 00-404), http://www2.epic.org/crypto/scarfo/def_supp_mot.pdf (last visited Mar. 4 , 2002) [hereinafter Scarfo motion].

149. Brief of the United States in Opposition to Defendant Scarfo's Pretrial Motions at 25, *Scarfo* (No. 00-404), http://www2.epic.org/crypto/scarfo/gov_brief.pdf (July 17, 2001)) [hereinafter Scarfo brief].

150. *Scarfo*, 180 F. Supp. 2d at 581.

151. Scarfo motion, *supra* note 148, at 3.

152. *Id.*

153. Richard Willing, *FBI Technology Raises Privacy Issues*, USA TODAY, July 31, 2001, at 3A.

The government responded that KLS is similar to any other search. For example, if public authorities have a warrant to get a suspect's account book from his office, they may have to look through many drawers and shelves before finding it.[154] The court agreed and ruled that the use of KLS did not constitute a general search.[155]

Moreover, encryption has made counter-encryption necessary. As the *Boston Globe*'s technology reporter commented, "[t]echnolibertarians rightly howled when the feds tried to bar access to encryption software; now we must live with the consequences. The bad guys have encryption. The good guys must have counter-encryption tools."[156]

III. ACCOUNTABILITY

A. The Second Balance

This Article opened by calling attention to the need for balance between individual rights and public safety and health. When the polity tilts too far toward either safety or rights, the imbalance should be corrected. Accordingly, we must determine how the balance is affected by new technologies. Liberalizing technologies have greatly hindered the work of public authorities in the area of communications surveillance. On the other hand, new protective technologies have offset these difficulties to some extent. New legislation that adapted old laws to the new technologies has further lessened these obstacles. Finally, the September 11th attack on America changed the point or zone[157] of balance by posing a new, credible threat to public safety and health. The question remains whether the new technological and legal measures enhance public safety to the extent needed or excessively intrude into individual rights.

In turn, this raises the question of how to determine whether the polity is in the zone of balance. It would take volumes to begin to do justice to this issue, but I have dedicated some text to it elsewhere.[158] Briefly, I concluded that the course of a nation's laws should not be

154. *See* Scarfo brief, *supra* note 149, at 38.

155. *Scarfo*, 180 F. Supp. 2d at 578 ("Just like searches for incriminating documents in a closet or filing cabinet, it is true that during a search for a passphrase 'some innocuous [items] will be at least cursorily perused in order to determine whether they are among those [items] to be seized.'" (quoting United States v. Conley, 4 F.3d 1200, 1208 (3d Cir. 1993)).

156. Hiawatha Bray, *Military-Tech Complex*, BOSTON GLOBE, Nov. 29, 2001, at C1.

157. I refer to a zone because I do not claim that there is a precise point of balance that one can identify at which the government tilts clearly too far in one direction or the other.

158. *See* SPIRIT OF COMMUNITY, *supra* note 10; NEW GOLDEN RULE, *supra* note 8, at 3–57.

corrected unless (1) there is a compelling reason, a concept akin to "clear and present danger" although not necessarily as strict; (2) the matter cannot be addressed by non-legal, voluntary means; and (3) one can make the intrusion small and the gain — either in safety or in rights — considerable. These criteria can be applied to the issues discussed here. For example, after September 11th, the government should have greater powers to decrypt e-mail because (1) terrorism does pose a major threat; (2) voluntary means to fight encrypted terrorist messages have not sufficed; and (3) decrypting e-mail messages is not more intrusive than tapping a phone. Some other new measures, such as roving wiretaps, may also pass the same test.[159]

To judge whether a new measure that enhances the powers of public authorities is called for, I suggest *a second, perhaps more decisive, form of balancing*. Its concern is not whether the government should be accorded new powers, but *how closely it is held accountable regarding the ways it uses these powers*. From this viewpoint, the key issue is not whether certain powers, like the ability to decrypt e-mail, should be available to public authorities, but whether these powers are used legitimately and whether mechanisms are in place to ensure proper usage. This is similar to passing over the question of whether there is too much money in a vault in favor of asking how strong the locks are.

Although the two forms of balance have some similarities and points of overlap, they are quite distinct. The cyber-libertarians' argument that the government should not be able to decrypt encoded messages is different from recognizing that such powers are justified *as long as they are properly circumscribed and their use is duly supervised.* The balance sought here is not between the public interest and rights, but between the supervised and the supervisors. Deficient accountability opens the door to government abuses of power, and excessively tight controls make agents reluctant to act. Thus, a case can be made that under most of Hoover's reign, the FBI was insufficiently accountable. One could also argue that under the new rules adopted following the Church Commission report, the FBI was excessively limited in its ability to conduct communications surveillance. Agents, fearing reprimands and damage to their careers, may have been too reluctant to act.

It is difficult to sustain the argument that the government should be unable to decrypt any messages or be unable to gain the authority

159. Other public safety measures that do not concern communications surveillance, such as requiring protestors to remove their disguises, are not addressed in this article and may not meet the criteria listed. *See, e.g., Anti-terrorism Measures: And Throw Away the Key*, ECONOMIST, Nov. 17, 2001, at 54 (reporting that the United Kingdom's anti-terrorism bill introduced on November 13 includes a provision that would obligate protestors to remove disguises).

to do so. After the first bombing of the World Trade Center in 1993, one of its principal masterminds used encryption to protect files on his laptop computer, even as he plotted to blow up commercial airlines.[160] Encrypted files were found on a computer used by Osama bin Laden's lieutenants in the Afghan capital.[161] Few would argue that public authorities should be unable to decrypt such files, even after obtaining a warrant based on probable cause that the files included important information.

For encryption, the issue should be which messages can be decrypted, who will verify that these limits are observed, and by what means. Similarly, regarding roving intercepts, the issue should not be whether the government can monitor the same suspect over different instruments of communication, but how we will ensure that it does not collect information about third parties who use the same devices as the suspect. More generally, the issue is not whether communications in cyberspace should be exempted from the same type of public scrutiny to which mail and phone calls have historically been subjected, as cyber-idealists had hoped,[162] but whether proper controls are in place to protect against abuse.

In assessing whether the American polity is excessively attentive to public safety or rights in matters concerning communications surveillance, the next step is to determine to what extent accountability has been built into the new powers granted to the government in response to new technologies and September 11th.

B. Layers of Accountability

1. Limitations Built into the Law

Limitations on the use of new powers are written into the laws governing them and limitations on protective technologies are often built into the technologies themselves. Roving and other types of intercepts are not granted without limits. Title III lays out a requirement for "minimization." It states that "[e]very order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."[163]

---

160. Freeh statement, *supra* note 46, at 27.

161. *See* Alan Cullison & Andrew Higgins, *How al Qaeda Agents Scouted Attack Sites In Israel and Egypt*, WALL ST. J., Jan. 16, 2002, at A1.

162. *See* LEVY, *supra* note 45, at 212 (quoting a "cypherpunk manifesto" written by one such cyber-idealist).

163. 18 U.S.C. § 2518(5) (2000).

Such built-in guidelines are intended to limit the ability of public authorities to gather and use information not directly related to their investigations.[164] Practically, this means that agents are not allowed to record conversations unrelated to the subject of the investigation and should stop listening when irrelevant matters are being discussed. If agents are unsure whether a seemingly innocent conversation might touch on a relevant subject at some point, agents are to conduct "spot-monitoring," in which they tune in every few minutes to check but only begin to record when appropriate.[165]

In *Scott v. United States*,[166] the Supreme Court found that an agent's implementation of minimization guidelines must be evaluated under a "standard of objective reasonableness," so that if circumstances make minimization difficult, an agent's failure to attempt it does not constitute an illegal violation.[167] In addition, if investigators have reason to suspect a conspiracy involving a large number of people, they are justified in recording and listening to all conversations until they are certain who is innocent and who is not.[168] Many critics point out that under any circumstances, minimization is voluntary and we must rely on our trust in law enforcement officers to do it properly,[169] highlighting the importance of further layers of accountability, such as the exclusionary rule.[170]

Although telephone wiretaps require human judgment to implement minimization, new public protective technologies, if properly used, carry out much of the minimization function automatically. Carnivore's filters, if set properly, act as a built-in minimization process, intercepting only what is appropriate. Although it might be capable of collecting all content that passes through it, it can and should be set to capture only data sent to and from a specific user in compliance with court orders.[171] As mentioned before, data that does not fit the filter settings merely passes through without being saved by Carnivore and is not seen by public authorities.[172]

---

164. *Id.*

165. *See, e.g.*, United States v. Clerkley, 556 F.2d 709 (4th Cir. 1977); United States v. Losing, 539 F.2d 1174, 1180 (8th Cir. 1976); United States v. Costello, 610 F. Supp. 1450, 1477 (N.D. Ill. 1985); United States v. Clemente, 482 F. Supp. 102, 108–10 (S.D.N.Y. 1979).

166. 436 U.S. 128 (1978).

167. *Id.* at 137–39.

168. *See id.* at 142.

169. *See* Rep. Bob Barr, *A Tyrant's Toolbox: Technology and Privacy in America*, 26 J. LEGIS. 71, 74 (2000).

170. *See id.* at 85.

171. *See* IITRI Report, *supra* note 115, at §§ ES.5, 3.4.4.1.6.

172. *See id.* § 3.4.4.1.3.

2. Supervision Within Executive Agencies

Numerous accountability mechanisms are built into the executive agencies of the government. Of course, numerous FBI guidelines exist, and supervisors are to ensure that field agents abide by these guidelines.[173] Moreover, when agents cross the line, they face internal reviews. In addition, the Attorney General's office supervises the FBI to some extent. For instance, as already mentioned, requests by the FBI to conduct communications surveillance under FISA must be approved by the Attorney General's office before they are submitted to the FISC. In some cases, court order or warrant requests never get past internal FBI approval procedures. For example, before September 11th, Zacarias Moussaoui, the possible "20th hijacker," was arrested on immigration charges, and field agents wanted to search his computer, but their request never made it past FBI attorneys, who found insufficient evidence to justify it.[174]

3. Courts

Once surveillance technology makes it possible to scan e-mail or decrypt messages and once it is established in principle that the government will have access to such technology, the question for both sides becomes: under what conditions should the government be allowed to use it? The contest on this second-level issue often centers on the issuance of warrants and court orders.

Civil libertarians contend that courts issue search orders too liberally, without due scrutiny.[175] In fact, around 10,000 intercept orders have been granted under FISA since its creation in 1979,[176] amounting to under 1,000 per year. Civil libertarians point to the fact that the FISC has only denied one request for surveillance in its entire history[177] as evidence that the standards for receiving a FISA intercept order are lower than for receiving a Title III order.[178] Though applications for intercept orders are rarely turned down by the FISC, public safety advocates point out that it is embarrassing and damaging to agents' records and careers to be turned down by the FISC, and as a result, they are reluctant to request warrants even when they seem

173. *See id.* §§ 3.2–3.3; *see also* Orin Kerr, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001) (on file with Computer Crime and Intellectual Property Section, United States Dep't of Justice).

174. *See* Dan Eggen & Brook A. Masters, *U.S. Indicts Suspect in September 11 Attacks*, WASH. POST, Dec. 12, 2001, at A1.

175. *See* Carlsen, *supra* note 63, at A3.

176. *See id.*

177. *See id.*

178. *See* Davidson statement, *supra* note 135.

justified.[179] Moreover, if the FISC finds insufficient justification, it tends to return the request, and attorneys either submit further documentation or abandon the application before receiving an official rejection, which accounts for there being next to no outright refusals.[180] Furthermore, some requests never get past the Attorney General's office.[181] Lastly, FISA applications need to meet preset guidelines and must include a statement of the means by which the surveillance will be conducted as well as a statement of proposed minimization procedures.[182]

Although civil libertarians typically prefer courts to administrative agencies,[183] they fear that judges might be unable or disinclined to curb law enforcement agents.[184] First, judges are either elected or politically appointed, making them subject to the influence of public opinion.[185] In addition, they might be less cautious in granting warrants and court orders that apply to other jurisdictions, which the USA PATRIOT Act allows. Judge Meskill, in his concurrence in *United States v. Rodriguez*,[186] warned:

> [J]udges may be more hesitant to authorize excessive interceptions within their territorial jurisdiction, in their own back yard so to speak, than in some distant, perhaps unfamiliar, part of the country. Congress determined that the best method of administering wiretap authorizations included territorial limitation on the power of judges to make such authorizations.[187]

As a result, courts would be a relatively weak accountability mechanism for nationwide warrants.

---

179. Interview with Orin Kerr, Associate Professor of Law, George Washington University, and former trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division at the U.S. Dept. of Justice, in Washington, D.C. (Dec. 14, 2001).

180. *See* Toensing remarks, *supra* note 28.

181. *See* Carlsen, *supra* note 63.

182. *See* 50 U.S.C. § 1804(a) (2000).

183. *See* ACLU, *supra* note 111.

184. *See* ACLU, *More Detail on ACLU Objections to Selected Provisions of Proposed Anti-Terrorism Legislation* (2001) ("Law enforcement, rather than a Court, will decide what is 'content' and systems like Carnivore will be used without any real judicial supervision."), *at* http://www.aclu.org/congress/Patriot_Links.html (last visited Mar. 4, 2002).

185. *See* William Mishler & Reginald S. Sheehan, *Public Opinion, the Attitudinal Model, and Supreme Court Decision Making: A Micro-Analytic Perspective*, 58 J. POL. 169, 169–200 (1996); Beverly B. Cook, *Public Opinion and Federal Judicial Policy*, 21 AM. J. POL. SCI. 567, 567–600 (1977).

186. 968 F.2d 130 (2d Cir. 1992).

187. *Id.* at 135.

In addition to the requirements that must be met to get a warrant or court order in the first place, courts ensure that law enforcement agents act within the limits of their power by suppressing illegally collected evidence. The exclusionary rule, established in *Boyd v. United States*[188] and re-affirmed in *Weeks v. United States*,[189] states that evidence collected in violation of the Fourth Amendment must be excluded in a trial against the suspect.[190] This serves not only to protect the suspect after a violation occurs but also to deter inappropriate searches because agents know that if they do not follow the correct procedures, the culprits might go free.

4. Congress

Under our system of checks and balances, Congress is supposed to oversee the work of the executive branch and its agencies. It has many instruments for doing so. It can require heads of agencies and other high-ranking officials to respond to written questions, testify before congressional committees, and turn over documents. It may order the General Accounting Office to perform a study. In addition, Congress can conduct committee hearings in which interested parties can voice their concerns.

Civil libertarians argue that many of the measures included in the USA PATRIOT Act were enacted in a great rush without the usual hearings and deliberations.[191] Supporters of the public authorities

---

188. 116 U.S. 616 (1886).

189. 232 U.S. 383 (1914).

190. Although the rule has been diluted somewhat, it is still controlling law. *See, e.g.*, United States v. Leon, 468 U.S. 897 (1984) (establishing a "good faith" exception to the exclusionary rule); Nix v. Williams, 467 U.S. 431, 444 (1984) (creating the "inevitable discovery" exception to the exclusionary rule); Massachusetts v. Sheppard, 468 U.S. 981 (1984) (upholding the "good faith" exception); United States v. Calandra, 414 U.S. 338, 348 (1974) (establishing that the exclusionary rule does not proscribe use of *all* illegally obtained evidence). For further discussion, see Leslie-Ann Marshall & Shelby Webb, Jr., *Constitutional Law — The Burger Court's Warm Embrace of an Impermissibly Designed Interference with the Sixth Amendment Right to the Assistance of Counsel — The Adoption of the Inevitable Discovery Exception to the Exclusionary Rule: Nix v. Williams*, 28 HOW. L.J. 945 (1985); Christopher A. Harkins, *The Pinocchio Defense Witness Impeachment Exception to the Exclusionary Rule: Combating a Defendant's Right to Use with Impunity the Perjurious Testimony of Defense Witnesses*, 1990 U. ILL. L. REV. 375, 389–412 (1990).

191. Representatives of the ACLU have stated:

> The process that brought you this bill is terribly flawed. After bypassing a Judiciary Committee mark-up, a few Senators and their staffs met behind closed doors, on October 12, 2001 to craft a bill. The full Senate was presented with anti-terrorism legislation in a take-it-or-leave-it fashion with little opportunity for input or review. No conference committee met to reconcile the differences between the House and Senate versions of the bill. We find it deeply disturbing that once again the full Senate will be forced to

point out that after September 11th it was assumed that there were other "sleeper" terrorist agents in the United States and that other attacks were imminent, which justified the rush. Indeed, they held that expanded powers should have been given well before September 11th.[192] Moreover, Congress had begun to address these issues before September 11th by holding hearings on Carnivore.[193]

5. The Public

The ultimate source of oversight is the citizenry, informed and alerted by a free press and by civil liberties advocates and briefed by public authorities. To be fully effective in overseeing the issues at hand, civil libertarians argue that the public must be informed about the inner workings of the protective technologies, while public authorities claim that such disclosures would inform terrorists and other criminals about how to circumvent the technologies, thus rendering them useless. Specifically, since the existence of Carnivore was made public, numerous parties have demanded access to information about how it works. The ACLU filed a Freedom of Information Act

---

> vote on legislation that it has not had the opportunity to read. Senate offices are closed and staff cannot even access their papers to fully prepare you for this important vote. Regular order is being rejected and it is an offense to the thoughtful legislative procedures necessary to protect the Constitution and Bill of Rights at a time when the rights of so many Americans are being jeopardized.

Murphy letter, *supra* note 7.

192. Senator Hatch remarked:

> We can never know whether these tools would have prevented the attack on America, but, as the Attorney General has said, it is certain that without these tools we did not stop the vicious acts of last month. I personally believe that if these tools had been in law — and we have been trying to get them there for years — we would have caught those terrorists. If these tools could help us now to track down the perpetrators — if they will help us in our continued pursuit of terrorists — then we should not hesitate to enact these measures into law. God willing, the legislation we pass today will enhance our abilities to protect and prevent the American people from ever again being violated as we were on September 11.

147 Cong. Rec. S10,990 (2001) (statement of Sen. Hatch).

193. *See, e.g.*, *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution, House Comm. on the Judiciary*, 106th Cong. (2000), *available at* http://www.house.gov/judiciary/con07241.htm (last visited Mar. 4, 2002); *The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong., *available at* http://www.senate.gov/~judiciary/oldsite/wl96200f.htm (last visited Mar. 4, 2002).

("FOIA") request to get its source code,[194] which reveals the technical commands and internal structure of a program. EPIC filed a FOIA request to gain a copy of *all* documents relating to Carnivore.[195] In addition, numerous ISPs who might be asked to cooperate in installing Carnivore have called for guarantees that the program works as claimed and that there are sufficient controls to keep law enforcement agents from capturing more than what is covered by a court order.[196]

In *Scarfo*, the judge joined civil liberties groups in demanding that the FBI release information on how KLS works, stating that he could not rule on whether its use was legal without knowing how the technology worked. The judge said he would review the technology secretly.[197] This solution satisfied neither the civil libertarians nor the FBI. David Sobel of EPIC said the matter raised "very basic questions of accountability. The suggestion that the use of high-tech law enforcement investigative techniques should result in a departure from our tradition of open judicial proceedings is very troubling."[198] Donald Kerr, Director of the FBI's Laboratory Division, stated that the disclosure of certain information about KLS would "compromise the use of this technology . . . and jeopardize the safety of law enforcement personnel."[199]

Secrecy also remains one of the key objections to the use of roving intercepts under FISA. FISA was established in the mid-1970s after the public was alarmed to learn of the activities of President Nixon and the NSA's illegal interception of telegraph and telephone calls.[200] A congressional committee was created to investigate and found that nearly every president had authorized warrantless communications surveillance, often for political purposes.[201] Essentially, agencies such as the FBI, CIA, and NSA were able to conduct surveillance without going through normal criminal procedures. The Department of Justice launched its own in-house investigation, resulting in new guidelines for both domestic and foreign intelligence investi-

194. *See* Press Release, ACLU, In Unique Tactic, ACLU Seeks FBI Computer Code On "Carnivore" and Other Cybersnoop Programs (July 14, 2000), http://www.aclu.org/news/2000/n071400a.html (last visited Mar. 4, 2002).

195. *See* Press Release, EPIC, Lawsuit Seeks Immediate Release of FBI Carnivore Documents (Aug. 2, 2000), http://www.epic.org/privacy/carnivore/8_02_release.html (last visited Mar. 4, 2002).

196. *See* Nick Wingfield & Don Clark, *Internet Companies Decry FBI's E-mail Wiretap Plan*, WALL ST. J., July 12, 2000, at B11A.

197. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 575 (D.N.J. 2001).

198. John Schwartz, *U.S. Refuses to Disclose PC Tracking*, N.Y. TIMES, Aug. 25, 2001, at C1.

199. Krim, *supra* note 44.

200. *See* Jim McGee, *The Rise of the FBI*, WASH. POST MAG., July 20, 1997, at W10.

201. *See FBI's "Political Abuses,"* U.S. NEWS & WORLD REP., Dec. 15, 1975, at 61.

gations.[202] To prevent future abuses, Congress passed FISA in 1978 to spell out what intelligence agencies could and could not do.[203] The NSA had insisted that its activities — especially regarding its methods and technologies — would be severely compromised if discussed in open court. In response, FISA authorized the formation of a special federal court whose proceedings could be completely secret.[204] In short, while the public cannot be informed about all the workings of all the protective technologies, such as Carnivore, because this would impair the usefulness of the technologies, the public can act as the ultimate enforcer of accountability. Ultimately, this is a question of whom we trust.

C. Trust

Accountability is ultimately a matter of trust. Plato is said to have raised the issue in asking *quis custodiet ipsos custodes*, or who will guard the guardians?[205] Others attribute the question to the Roman satirist Juvenal, who wrote around 2000 years ago.[206] The issue, though, is very much with us today. If we do not trust the cops on the beat, we may ask their captains to keep them under closer supervision. If we do not trust the captains, we may call on the mayor to scrutinize the police. We may call on the other branches of government, especially the courts, to serve as checks and balances. However, if we believe that the mayors are corrupt and the judges cannot be trusted, we have little to fall back on other than the press. Yet the media, too, is often distrusted.[207]

The question, then, is whom we should distrust and how much. If no authority or media figure is trustworthy and "The System" is corrupt, we face a much larger problem than if, in a few instances, public authorities intercept more e-mail than they are supposed to or tap phones they should not. If someone believes the entire system is untrustworthy, she should either move to another country or fight for an entirely new political system.

---

202. *See* Theoharis, *supra* note 13.

203. *See* McGee, *supra* note 200.

204. 50 U.S.C. § 1803(c) (2000).

205. *See* Robert O. Keohane, *Governance in a Partially Globalized World*, 95 AM. POL. SCI. REV. 1 (2001).

206. *See* Martin Edmonds, *Politics, Law, Economics and Social*, 62 INT'L AFFAIRS 290 (1986) (reviewing MILITARY INTERVENTION IN DEMOCRATIC SOCIETIES (Peter J. Rowe & Christopher J. Whelan eds., 1985)).

207. *See generally* SEYMOUR MARTIN LIPSET & WILLIAM SCHNEIDER, THE CONFIDENCE GAP: BUSINESS, LABOR, & GOVERNMENT IN THE PUBLIC MIND (rev. ed., Johns Hopkins U. Press 1987) (1983) (studying trends, causes, and consequences of public confidence in U.S. institutions).

However, if the problem is only some individuals in positions of authority, we have good reason to watch out for those individuals but not to doubt the entire political system. We ought, then, to work to improve the various layers of accountability but also realize that the fact that critics can always come up with some horror stories does not necessarily mean that those stories are typical of the system.

CONCLUSION

Determining whether a specific public policy measure is legitimate entails more than establishing whether it significantly enhances public safety and minimally intrudes on individual rights. It also requires assessing whether those granted new powers are sufficiently accountable to the various overseers — ultimately to the citizenry. Some powers are inappropriate no matter what oversight is provided. However, others are appropriate given sufficient accountability. *If accountability is deficient, the remedy is to adjust accountability, not to deny the measure altogether.*[208]

Whether the specific powers given to the government sustain or undermine the balance between rights and safety depends on how strong each layer of accountability is, whether higher layers enforce lower ones, and whether there are enough layers of accountability. I suggest that we should ignore both public authorities' claims that no strengthening of accountability is needed and the shrillest civil libertarian outcries that no one is to be trusted. Instead, we should promote reforms that will enhance accountability rather than deny public authorities the tools they need to do their work. This does not necessarily mean granting them all the powers they request, but in a world where new technologies have made the government's duties more difficult and in which the threat to public safety has vastly increased, we should focus more on accountability before denying powers to law enforcement.

208. It is true that accountability can be excessive and that law enforcement agents can be reluctant to act due to fear that they will be penalized by superiors, courts, or Congress, or be skewered by the press. However, there have been no signs of this since September 11th.