**Brooklyn Journal of International Law**

Volume 27
Issue 1
SYMPOSIUM:
Fourth Annual Latin American Round Table on
Competition & Trade

Article 7

2001

# Internet Communication Standards for the 21st Century: International Terrorism Must Force the U.S. to Adopt "Carnivore" and New Electronic Surveillance Standards

Seth R. Merl

# NOTES

# INTERNET COMMUNICATION STANDARDS FOR THE 21ST CENTURY:

# INTERNATIONAL TERRORISM MUST FORCE THE U.S. TO ADOPT "CARNIVORE" AND NEW ELECTRONIC SURVEILLANCE STANDARDS

## I. FOREWORD

Sitting down to write this Note in late fall 2000, the state of international terrorism was much different than that which it would become in less than a year. At the time, organized attacks on American interests were on the rise, most recently the attack on the U.S.S. Cole in Yemen. While the destructiveness of terrorist attacks had been slowly rising over the previous decade, by the time of the Cole attack it became clear to many that the organizations recruiting, planning and carrying out these deadly attacks were becoming more advanced, primarily through the use of the Internet and electronic communications.

In early September 2001, preparing to go to print, the world was much the same as it had been nine months earlier. Concern was growing, and government agencies

had stepped up their abilities to conduct electronic surveillance of the Internet. These advances were also countered by a growing concern for a protection of privacy rights, and in my view, the need for a new Internet surveillance law to properly balance the competing interests of security and fundamental rights in the new century.

September 11th changes everything, for all of us. An attack on the U.S., as I will discuss, was seen as imminent. What was never comprehended, was the destruction of the World Trade Center and attack on the Pentagon via hijacked airliners. The death toll in New York and Washington was astounding. In the aftermath, the rebuilding process has been a challenge for the entire country. Despite this dramatic change of events and ensuing war in Afghanistan to overthrow the Taliban and bring Osama bin Laden to justice, the need still exists for a 21st century approach to electronic surveillance and a new law to set standards for dealing with the internet and its capabilities. In a Postscript, I will briefly examine the proposed changes to surveillance law following September 11th, noting that the United Kingdom's Regulation of Investigatory Powers Act is still a new approach to surveillance containing provisions the U.S. may find useful in the new campaign to rid the world of terrorism.

## II. INTRODUCTION

October 12 was another clear, sun soaked afternoon in the deep-water port of Aden, Yemen. The U.S.S. Cole, a 505-foot-long Aegis guided-missile destroyer, one of the Navy's newest and most lethal, was slowly being tied up to anchor buoys in preparation for refueling.[1] Standing under the Arabian Peninsula's broiling noon-sun, her lookouts patrolled the decks, with an eye, and sidearm, on the watch for any signs of danger.[2] Scampering around the Cole were a half-dozen or so smaller vessels, hauling her huge mooring lines onto the buoys.[3]

---

1. Richard J. Newman, *A Hole in the Water Line*, U.S. NEWS AND WORLD REPORT, Oct. 23, 2000, at 26, 26.
2. *Id.*
3. *Id.*

One of those ships, with two men aboard, suddenly dropped the lines and accelerating to full speed, headed directly at the Cole's port side midsection.[4] Seconds later, an enormous explosion rocked the destroyer, tearing a forty foot hole through the ship's thick re-enforced steel.[5] The force of the blast, the result of enough C-4 plastic explosive[6] to level a building, tore into the Cole's engine room and mess hall. Crowded with sailors lined up for chow, the shear force of the blast pushed the mess hall upward, into the deck above.[7] When the smoke cleared, seventeen crewmen were dead, and thirty-nine more suffered injuries.[8] This was the latest in a growing number of terrorist attacks on American citizens and armed forces around the world.

Terrorist attacks, like the one on the Cole, seem to be a common, nearly routine occurrence over the past decade. In August 1998, American embassies in Kenya and Tanzania were bombed, killing 224.[9] These acts of violence have been attributed to the work of Osama bin Laden, the Saudi millionaire currently directing his followers from within the mountains of Afghanistan.[10] While terrorism has been a tactic of fear for hundreds of years, it is rapidly metamorphasizing amid the technological advancements of the Information Age. Through the Internet explosion and communication revolution, global terrorism stands ready to enter the new millennium. With the benefit of the Internet, electronic mail, chat rooms, instant electronic messaging, electronic banking, cell phones and satellite uplinks, terrorists are changing the way they spread fear and their ideological message via modern telecommunications.

To combat these new forms, the United States has taken the lead in electronic communication surveillance. With the creation of the Federal Bureau of Investigation's

---

4. *Id.*

5. *Id.*

6. *Alleged 'Cole' Accomplices Detained,* TIMES UNION, Nov. 20, 2000, at A3.

7. Newman, *supra* note 1, at 26.

8. *Yemen's President Naming Names,* WASH. POST, Dec. 10, 2000, at B1.

9. David A. Vise & Lorraine Adams, *Bin Laden Weakened, Officials Say*, WASH. POST, March 11, 2000, at A3.

10. *Id.*

("FBI's") Carnivore Diagnostic Tool, U.S. law enforcement now possess the capability of effectively intercepting Internet communications of terrorist organizations.[11] This tool, however, is still in the testing phase. What is currently needed is a new, comprehensive surveillance law that clearly protects privacy while addressing the new international terrorist threats made possible through recent technological advancements. With higher stakes in the electronic 21st century, terrorists like bin Laden have the capacity to be more effective, with much deadlier capabilities.[12] One recent model the U.S. must follow in its synthesis of surveillance needs and privacy concerns is the United Kingdom's Regulation of Investigatory Powers Act ("RIPA")[13], a new law that takes current global developments and human rights concerns into effect while dealing with the new concerns of the Internet. This Note will argue that the fusion of internet capabilities and weapons of mass destruction in the hands of those sworn to spread terror, creates a combination that demands both the Carnivore system and a new type of U.S. electronic privacy for the 21st century's Information Age; one based on RIPA that allows updated electronic surveillance of the Internet, buffered by privacy laws that take digital threats into account.

Part III of this Note will examine acts of terrorism over the past decade, and address the advanced capabili-

---

11. *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearings Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 11 (2000) (statement by Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation) [hereinafter Kerr-House].

12. *See Countering the Changing Threat of International Terrorism: Hearings Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Comm. on the Judiciary*, 106th Cong. 29 (2000) (statement by Ambassador L. Paul Bremer III, Chairman, National Committee on Terrorism) [hereinafter Bremer]; *World Wide Threats to National Security: Hearing on Threats to U.S. National Security Before the Senate Select Comm. on Intelligence*, 105th Cong. (1998) (statement by Louis J. Freeh, Director, Federal Bureau of Investigation), *available at* 1998 WL 8991513 [hereinafter Freeh].

13. Regulation of Investigatory Powers Act, 2000, c. 29 (Eng.) [hereinafter RIPA]. The full text of RIPA is available at http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm (last visited Oct. 1, 2001).

ties of terrorists via modern communication technology. With an eye toward threats of the future, I will argue that Internet surveillance capabilities are indeed necessary, as law enforcement must keep up with the great advances of the Internet in terrorism prevention.

Part IV will address the current mix of communication, privacy, and crime laws in the U.S. Special attention will be paid to the newly operational Carnivore system, and the extent to which these older laws attempt to regulate its use.

Part V will analyze the current state of privacy in the U.K. and the European conventions that affect it. I will then closely analyze the provisions of the new surveillance act, and draw comparisons to what is needed in the U.S. to govern Carnivore.

Part VI will argue that the U.S. must adopt a similar comprehensive law based on RIPA, especially when current fears concerning Carnivore are taken into effect. We will conclude in Part VII that, facing the realities of future terrorist attacks using weapons of mass destruction, coupled with the enhanced tactical capabilities of the Internet, a Carnivore system is required in U.S., but one that will be governed by a new Internet privacy and surveillance law that follows recent international trends.

## III. THE STATE OF INTERNATIONAL TERRORISM

Traditionally, terrorism has been employed for centuries as a means of forcing change through heightened diplomatic pressure and politically consequential violence without having to bear responsibility.[14] By creating fear, it undermines the confidence of society, and radicalizes us, through resentment, to revere any counter-action.[15] At its

14. *See* W. Michael Reisman, *International Legal Responses to Terrorism,* 22 HOUS. J. INT'L L. 3, 10, 60 (1999).

15. *See* William Rees-Mogg, *A Devil for Our Time,* THE TIMES OF LONDON, Aug. 24, 1998, at 18. *See also* JAMES DAVIDSON & LORD WILLIAM REES-MOGG, THE SOVEREIGN INDIVIDUAL: HOW TO SURVIVE AND THRIVE DURING THE COLLAPSE OF THE WELFARE STATE (1997); 141 CONG. REC. S2502-03 (daily ed. Feb. 10, 1995) (statement of Sen. Biden) (In reference to the World Trade Center bombing, Sen. Biden stated, "the revelation that terror networks are operating in our midst undeniably has its intended effect on our national psyche - it undermines the sense of security of all Americans both at home and abroad."); Norman Dorsen, *The Need For a New Enlightenment: Lessons*

core, terrorism has three effects: An immediate effect of killing or injuring those who are deemed a prohibited target; an intermediate effect of intimidating the larger population therefore influencing their political behavior; and an aggregate effect of undermining overall public order.[16] Because international terrorism is usually a consciously adopted rather than spontaneous or impulsive strategy, the most important goals of effective response must center on arresting, deterrence and prevention.[17] For some time, the United States Congress has defined terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents;" international terrorism is defined as "terrorism involving citizens or the territory of more than one country."[18] In the last five to eight years however, terrorism has taken on new capabilities and new targets. In 1993, the World Trade Center was bombed, and further planned attacks on New York City tunnels were thwarted in their advanced stages.[19] In 1995, a plot to blow up eleven U.S. airlines was also exposed.[20] Overseas, more than 6,000 casualties were caused by a mere three attacks on American embassies in Kenya and Tanzania and an Air Force barracks in Saudi Arabia.[21] These were all done with the use of conventional weapons. Recent threats, and the stakes, have begun a dramatic evolution.[22]

Historically, in its infancy, terrorism was employed in the late 18th century revolutionary France as a means

---

*in Liberty from the Eighteenth Century, in* THE CONSTITUTION, THE LAW, AND FREEDOM OF EXPRESSION 1789-1987 22, 36 (James Brewer Stuart ed., 1987) (Dorset explained the psychological damage of terrorism as clutching us in its grip, leaving us with a loss of control. "Order unravels. Institutions lose their self-confidence. Reason itself – the belief that human problems have rational solutions – is under attack.").

16. Reisman, *supra* note 14, at 7.
17. *Id.*
18. 22 U.S.C. § 2656f(d)(1)-(2) (1994).
19. *See* Bremmer, *supra* note 12, at 32.
20. *Id.*
21. *Id.*
22. *Id.* at 30-31.

of low-level revolt fought close to home.[23] At its most basic form, the modern Western idea of terrorism is directly credited to Maximilien Robespierre and his Reign of Terror from 1793 to 1794, where he created an organization that attempted to systematize murder and lawlessness into a set of rules.[24] Adopted in Ireland to oppose English rule and occupation, its crude tactics of small-scale bombings and attacks have been used by Baske separatists in Spain, revolutionaries in Sri Lanka and throughout the Middle East, just to name a few political hot spots.[25] Recently, however, with the dawning of the new Information Age, capabilities of effecting terrorist attacks throughout the globe have been expanded, mainly due to modern communication advancements and the Internet. The United States, now more than ever, is vulnerable to this new breed of international terrorism, as modern technology has given terrorists abilities unheard of only a few years ago.[26]

*A. Dawning of the Information Age and the New Terrorist*

The Internet ("Net" or "Web") was originally developed by the Department of Defense in the early 1960's as a means of information exchange for scientists and academics.[27] Until the mid 1990's, the National Science Foundation maintained the communications medium.[28] Out of its innocent beginnings, the Net has exploded within the last ten years into a primary source of global communication. Currently, 500 million personal computers are connected to the Web worldwide.[29] In the U.S. alone, a December 1999 Harris poll found 56% of adults are now on-line, six times higher than in 1995.[30] The

23. ALBERT PARRY, TERRORISM: FROM ROBESPIERRE TO ARAFAT 39 (1976).

24. *Id.*

25. SUZANNE ROBITAILLE ONTIVEROS, GLOBAL TERRORISM (Pamela R. Byrne & Suzanne R. Ontiveros eds., 1986). *See also* WALTER LAQUEUR, THE TERRORISM READER: A HISTORICAL ANTHOLOGY (1978).

26. *See* Freeh, *supra* note 12.

27. Alan E. Wiseman, *Economic Perspectives on the Internet, at* http://www.ftc.gov/be/execsumm.htm (last visited Oct. 1, 2001).

28. *Id.*

29. *Id.*

30. *Fourth Amendment and the Internet: Hearings Before the Sub-*

Internet has blossomed into a major source of commerce, or "E-commerce" with billions of dollars in sales transactions occurring every year.[31] It has allowed for instantaneous communication via electronic mail, chat rooms where anyone can log onto a Web page and join an open discussion and hundreds of thousands of Web sites overflowing with all types of information imaginable. Nationwide, telephone lines are being upgraded to integrate telephone, television and Internet capabilities to allow for faster downloading speeds. Yet, along with this new electronic lifestyle of immediate communication, high efficiency and instant gratification, there is great vulnerability. Over the last five years in particular, we have witnessed a continuing steady growth of criminal and terrorist elements employing these new capabilities.[32]

Recent reliance on and advancements in computers and communication technology have freed organizations and individuals from the constraints of specific locations.[33] The result is the inadvertent creation of a new breed of international terrorist with far greater capabilities of wreaking havoc than ever before, and exploiting vulnerabilities from anywhere in the world.[34] With the Internet explosion, the most notable benefactor of the communication revolution has been Osama bin Laden. The Saudi born millionaire, whose anti-American terrorist network *al Queda* has a presence in twenty-four countries, including the U.S., and is believed to control forces of over 3,000 men, is dedicated to forcing American influence out of the Middle East.[35] Bin Laden had ties to Ramzi Yousef, convicted mastermind of the World Trade Center bombing in February 1993, and was accused of being the brains behind the August 1998 bombings of American embassies in

---

*comm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 22 (2000) (testimony of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology) [hereinafter Dempsey].

31. Wiseman, *supra* note 27.

32. *See* Kerr-House, *supra* note 11, at 14.

33. *See* Rees-Mogg, *supra* note 15, at 18.

34. Freeh, *supra* note 12.

35. Kevin Whitelaw, *The Ball Goes Up, But What Comes Down? Assessing Terrorists' Plans for the Millennium,* U.S. NEWS AND WORLD REPORT, Dec. 27, 1999, at 20, 20.

Africa.[36] Living in hiding deep within the mountains of Afghanistan, the Net has allowed bin Laden to serve as planner, communication center and bank roller for attacks such as these.[37]

*B. Terrorism Advances via Modern Communication*

In its current form, the Internet can be harnessed by terrorists and hate groups primarily in four ways: Planning attacks, recruiting followers, financing their campaigns and carrying out acts of "cyber-terrorism."[38] All three give them a great edge in achieving their goals of spreading fear through violence. One documented case of trans-Atlantic planning surfaced in October 1996, when Israeli Defense Forces asserted that activists of the fundamental Islamic terrorist group *Hamas*, living in the United States, were planning attacks via Internet chat rooms and e-mail in coordinating activities across Gaza, Lebanon and the West Bank.[39] In his statement on the worldwide threat in the year 2000, Director of Central Intelligence George Tenet testified that such groups, including *Hezbollah, Abu Nidal* and *al Queda*, were found to have widely adapted information technology, relying on the Web, e-mail and electronic bulletin boards to allow members to exchange information without running a high risk of being captured by U.S. counter-terrorism forces.[40] On the cutting edge, they even employ laptops, palmtops, cell phones and satellite phones to communicate.[41] With only satellites and the Internet, bin Laden has continued

36. Tim Weiner, *Dossier of Terror: Osama bin Laden,* AUSTIN AMERICAN-STATESMAN, Aug. 21, 1998, at A1.

37. *See* Rees-Mogg, *supra* note 15, at 18.

38. *See* Anthony Forster, *Hi-Tech Terrorists Turn to Cyber Warfare,* JANE'S INTELLIGENCE REV., Sep. 1999, at 46, 46-48.

39. *Id.* at 46.

40. *Carnivore Diagnostic Tool: Testimony Before the Senate Comm. on the Judiciary,* 106th Cong. (2000) (testimony of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation), *available at* http://www.fbi.gov/pressrm/congress/congress00/kerr090600.htm (last visited Oct. 1, 2001) [hereinafter Kerr-Senate].

41. *See* Kavita Kaur, *Terrorists on the Net: Dynamiting the Peace Domain,* COMPUTERS TODAY, Aug. 15, 1999, at 78.

to plan and direct successful terrorist attacks without being hindered by counteractions from the West.[42]

Terrorist organizations have also been successful in employing the Net for recruiting purposes, creating new independent cells around the world as old ones are used up or captured.[43] Recent studies have shown this to be both cheap and incredibly effective.[44] Through Web sites, mass e-mailings and chat rooms, with little effort leaders such as bin Laden can easily reach out into any country and find recruits ready to give their lives for his cause. Terrorists and hate groups can also use the Web to disseminate their beliefs and information quickly and directly to the public, bypassing traditional news media avenues altogether.[45] In 1995, the Anti-Defamation League reported that numerous U.S. based right-wing groups were using the Net for recruitment, including the Neo-Nazi National Alliance, anti-Semitic "Identity" churches and a variety of Ku Klux Klan organizations.[46]

While the dissemination of information is not only used to recruit, it should be mentioned that the Internet is now being harnessed to spread the capabilities of achieving bloodshed to anyone with access to a computer. Many believe that the recent increase in terrorist bombings over the last few years is to a large extent, attributable to the amount of readily available information on the Web teaching how to create highly effective explosives.[47] In the case of the Oklahoma City bombing, only hours after Timothy McVeigh blew up the Alfred P. Murrah Federal Building in 1994, killing 168 people, an anonymous source posted detailed instructions, including a diagram, on how to construct a similar fertilizer bomb.[48] Another

---

42. *See* Tom Regan, *When Terrorists Turn to the Internet: Seemingly Unconnected Events May Have a More Sinister Source: Coordinated, Cyber-Hacker Attacks,* CHRISTIAN SCIENCE MONITOR, July 1, 1999, at B7. *See* Vise & Adams, *supra* note 9, at A3.

44. Kaur, *supra* note 41, at 78 (citing Mike Caldrick, a bomb technician and anti-terrorist expert at Scotland Yard).

45. *See* ANTI-DEFAMATION LEAGUE, TERRORIST ACTIVITIES ON THE INTERNET (1998), *available at* http://www.adl.org/Terror/focus/16_focus_a.html (last visited Oct. 1, 2001).

46. Forster, *supra* note 38, at 47.

47. *See* Kaur, *supra* note 40, at 78-79.

48. *Id.*

site discussed how the McVeigh bomb could have been improved and more devastating.[49] Recent searches on the Web have come up with bomb making information on everything from "calcium carbide bomb[s]" to "chemical fire bottle[s]."[50] In this regard, terrorism has been transforming. No longer are we dealing with a war of people, but information war, where the Internet plays a key role in making everything from detailed on-line maps to information on sarin gas easily available.[51]

The Internet has also greatly improved the financing capabilities of terrorist organizations, primarily in the realm of money transfers and on-line banking via the Internet.[52] With electronic, instant transfers, terrorist groups can gain financial support from any source. From a central command post and laptop, leaders like bin Laden have the ability to fund individual terrorist cells from his own inherited wealth,[53] and from private or state donations made to his account. Independent cells can now receive the funds they need to carry out terrorist attacks almost instantly, leaving little time for law enforcement to follow a "money trail."

Combining the previous three advancements, recent Net capabilities have further created a new type of terrorism that has yet to be effectively countered – "cyberterrorism." [54] Due to its ease of coordination, extreme effectiveness and anonymity, cyber-terrorism has become an attractive alternative to traditional action over the past few years, as it inflicts great damage with little harm to the attacker.[55] So extreme is this threat, that cyberterrorism has become one of the two top post-Cold War problems facing the world today, second only to organized crime.[56] The Pentagon alone receives 2,500,000 hacking

---

49. *Id.*

50. *Id.*

51. *Id.*

52. *See id.* at 79.

53. He received part of a $5 billion inheritance from his father, a Saudi construction and oil magnate. Weiner, *supra* note 36, at A1.

54. It is defined as any person or group that "alters, destructs or acquires on line information with the intent to cause harm to the public." Kaur, *supra* note 41, at 80.

55. *See* Regan, *supra* note 42, at 17.

56. Kaur, *supra* note 41, at 80.

attempts each year.[57] Due to "[o]ur growing dependence on computer networks and telecommunications" the U.S. has become "increasingly vulnerable to possible cyber attacks against such targets as military war rooms, power plants, telephone networks, air traffic control centers and banks."[58]

The Internet is now being used not just as a means of creating a terrorist strike, but as a launch weapon itself.[59] Targets of the future are more likely to be corporate information structures as opposed to governmental, as evidenced in the recent cyber attack on Yahoo. Internet worms like "Worm.Explore Zip" created havoc in computer e-mail systems around the world, but particularly at corporations like Microsoft, Intel and NBC.[60] From a small apartment in the Philippines, the "I Love You" virus caused millions of dollars in damage worldwide by invading hard drives via Internet e-mail.[61] The FBI estimates such electronic intrusions to cause roughly $10 billion in damages every year within the United States alone.[62] As more and more companies take advantage of the information superhighway and modernize their communications systems, such targets become increasingly attractive. While technology and communication advances can increase corporate profits and establish better defense, they also assist potential enemies in improving their capabilities to attack.[63]

---

57. *Id.*

58. Freeh, *supra* note 12. *See also* Kerr-Senate, *supra* note 40 (Cyber attacks to shut down critical national infrastructure such as energy, telecommunications, transportation or government operations for the purpose of coercing or intimidating a government or civilian population is emerging as a very real threat.).

59. *See* Regan, *supra* note 42, at 18 (citing "Countering the New Terrorism" survey by the Rand Corp.); John Arquilla & David Rondfeldt, *Cyberwar is Coming! in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 23, 49 (1997).

60. Regan, *supra* note 42, at 18.

61. George Cole, *'I Love You' Can Really Hurt,* THE TIMES EDUCATIONAL SUPP. June 9, 2000, at 6, *available at* http://www.tes.co.uk/search/search_display.asp?section=Archive&sub_section=Online+Education&id=335588&Type=0 (last visited Oct. 1, 2001).

62. Vernon J. Ehlers, *Information Warfare and International Security,* OFFICER, Sep. 1, 1999, at 30.

63. *See id.*

*C. The Stakes Have Changed – A Need for Action in Internet Surveillance*

A heightened capability through instantaneous Internet connections is not the only problem facing U.S. and global security in the new century; in fact, it is merely half the equation. What must be realized are the lethal capabilities of modern international terrorist organizations, when recent technological advances in communication are linked with weapons of mass destruction. Once an issue only debated, many in law enforcement, intelligence and the armed forces now treat as fact the expectation that a terrorist group will use either a nuclear, chemical or biological weapon against the United States in the near future.[64]

The recent trend in terrorism has been directed toward more large-scale incidents designed for maximum destruction, terror and media impact, putting more Americans at risk than ever before.[65] In the last five years, the U.S. has seen a dramatic increase in the number of validated threats to use such agents.[66] In particular, the FBI has seen an increase in interest for biological agents by white supremacist and other domestic terrorist groups.[67] In 1997 for example, conspirators in a white supremacist organization pled guilty to planning to explode tanks containing hydrogen sulfide, a deadly industrial chemical, as a diversion to their armored car robbery.[68] Recently, authorities foiled a terrorist plot in the Southern U.S., uncovering a group planning to blow up power transmission facilities to be downloading off the Web information concerning Ricin, the third most deadly toxin in the world.[69] To better demonstrate the grave effects of even a limited chemical attack, one must only examine the 1995 nerve gas attack launched by the Japanese cult

64. *See* Freeh, *supra* note 12.
65. *Id.*
66. *See* Bremmer, *supra* note 12, at 29-30.
67. *See* Freeh, *supra* note 12.
68. *Id.*
69. *See* Kerr-Senate, *supra* note 40.

*Aum Shrinrikyo* upon the Tokyo subway system, killing twelve and sickening 5,000.[70]

Primarily, these new threats are due to the ease of acquiring weapons of mass destruction.[71] Nuclear proliferation has not only spread such weapons around the world, but some economically devastated countries such as Russia, with 30,000 war heads scattered across 100 sites, have questionable means of preventing their theft.[72] With a mentality that "everything is for sale," none of the key facilities in the former Soviet Union that hold weapons-usable nuclear material has adequate safeguards and security.[73] Chemical and biological weapons can also be easily manufactured or obtained, even within the United States.[74]

As terrorist cells diffuse from a central command post, weapons are assembled from different regions and routes of attack into the United States come from anywhere, the U.S. must take action in developing Internet surveillance capabilities. There can be little disagreement that an attack using weapons of mass destruction, planned, controlled and even executed through the benefits of the advancing Internet and communication technology could be devastating. We must be able to do a better job identifying terrorists and their plans, possess better intelligence collection techniques and have the ability to share and disseminate information on potential threats.[75] As technology has advanced greatly over the past decade to benefit all our lives, so must our capabilities of dealing with the evolving effects of those advancements.[76] As the Internet honeymoon period is over, the electronic 21st century must witness the combination of updated counter-terrorism devices and new communication standards, in an attempt to safeguard privacy, while

---

70. *See* Nicholas D. Kristof, *At Trial in Tokyo, Guru Says Aim was to Give 'Ultimate Joy,'* N.Y. TIMES, Apr. 25, 1996, at A11.

71. *See* Freeh, *supra* note 12.

72. Graham Allison, *Nuclear Dangers: Fear Increases of Terrorists Getting Hands on 'Loose' Warheads as Security Slips,* BOSTON GLOBE, Oct. 19, 1997, at C1.

73. *Id.*

74. *See* Freeh, *supra* note 12.

75. *See* Bremmer, *supra* note 12, at 29-31.

76. *See* Forster, *supra* note 38, at 48.

gaining equal footing with terrorists who have raised the stakes through weaponry and communication capabilities.

## IV. THE CURRENT MERGER OF U.S. LAW AND CARNIVORE

A balance must be struck between countering the increase in widespread multi-organizational terrorist networks, who are keenly adept at using advanced technology for both communications as well as munitions, and the grave danger that that response may be used to restrict the ambit of privacy and personal liberty that is at the very center of liberal societies. After all, it is that type of society that is the real target of the international terrorism. While it is often the case that unsettled times may tempt government officials to sacrifice individual rights in the name of national security,[77] the current situation of international terrorism we are now facing shows no sign of remaining only for a short while, a sudden flash in the pan that reactionaries jump at, but more of a new fact of life facing the new century. In the fight to achieve a comfortable medium against this steadily growing threat, the U.S. is currently attempting to fit Carnivore into a web of differing laws.

### *A. U.S. Law Addressing Terrorism, Surveillance and Privacy*

The recent trend in the U.S. has been to address the new level of Internet threats head on. The need for striking a balance between the Bill of Rights and national security, however, dates back to the earliest days of the new republic.[78] The Alien and Sedition Acts were designed in many ways to deal with the 18th century version of

77. *See, e.g.*, Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting) ("History teaches that grave threats to liberty often come in times or urgency, when constitutional rights seem too extravagant to endure."); RODNEY A. SMOLLA, FREE SPEECH IN AN OPEN SOCIETY 4 (1992) ("[I]t is a natural reflex to penalize speech perceived as inimical to national security, social order, or public civility.").

78. *See* The Alien Act of June 25, 1798, 1 Stat. 570; The Alien Act of July 6, 1798, 1 Stat. 577; The Sedition Act of July 14, 1789, 1 Stat. 596.

modern day terrorism facing the fledgling nation.[79] The second attempt by Congress, as a reaction to the world-wide turmoil leading up to World War I, came in 1917 with the Espionage Act.[80] Under this Act, jail sentences would now be assessed for participation in a conspiracy,[81] violently interfering with foreign commerce[82] and counterfeiting.[83] Despite the many First Amendment challenges to the Act, the Supreme Court interpreted the internal benefits to be of greater value than free speech concerns.[84]

The next attempt came in 1978 with the Foreign Intelligence Surveillance Act ("FISA").[85] The law provides regularized procedures for obtaining electronic surveillance warrants for foreign intelligence investigations for national security purposes.[86] For the first time, specifically included as "foreign powers" are groups engaged in international terrorism.[87] Under FISA, the government must obtain a court order before electronic surveillance can proceed against a U.S. person within the country's borders. With approval of the Attorney General, application is made to the Foreign Intelligence Surveillance Court.[88] If probable cause exists that the target of the surveillance is a foreign power, the warrant will be issued. In reviewing the application, the government must outline its minimization procedures which "limit acquisition, retention and dissemination of information concerning U.S. persons which is not publicly available."[89] Under judicial review, the courts have ruled that FISA's issuance of a warrant authorizing electronic surveillance complied with

---

79. *See* Thomas C. Martin, *The Comprehensive Terrorism Prevention Act of 1995,* 20 SETON HALL LEGIS. J. 201, 207 (1996).

80. Espionage Act of June 15, 1917, Pub. L. No. 24, ch. 30, 40 Stat. 217 (1917).

81. *Id.* tit. I, § 4.

82. *Id.* tit. IV, § 1.

83. *Id.* tit. V, § 2.

84. *See, e.g.,* Frohwerk v. United States, 249 U.S. 204 (1918); Schenk v. United States, 250 U.S. 47 (1919); and Abrams et al. v. United States, 250 U.S. 616 (1919).

85. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-29 (1994).

86. *Id.* §§ 1801-11.

87. *Id.* § 1801(a).

88. *Id.* § 1804.

89. *Id.* § 1801(h).

the procedural safeguards required by the Fourth Amendment to the Constitution, protecting individuals from unreasonable searches and seizures in criminal investigations.[90] The standards under FISA for the issuance of court orders were also found reasonable.[91]

Dangers of the Internet and the heightened threat of terrorism on American soil began to enter the mix in 1995. Following the World Trade Center and Oklahoma City bombings, the Senate passed the Comprehensive Terrorist Prevention Act.[92] Sponsored by Senate Majority Leader Robert Dole (R-Kans.), it created the new federal crime of international terrorism, broadened the federal jurisdiction over terrorist offenses, authorized "roving wiretaps" that could follow a suspect over numerous phone lines, simplified deportation of aliens linked to terrorism, prohibited donations to terrorist organizations, increased FBI access to credit reports and enhanced the pre-emptive striking power of law enforcement to stop terrorist violence before it occurred.[93] Most importantly however, for the first time Congress began to recognize the role, albeit a fledgling one in 1995, of the Internet in effecting terrorist attacks. During debate on the bill, Senator Barbara Feinstein (D-Cal.) proposed amendment number 1209 that would make it unlawful to intentionally distribute information by any means, pertaining to the manufacture of explosives, to someone who is going to use it to commit a federal offense.[94] In illustrating the need for such an amendment, the Senator read several passages from the *Terrorist Handbook*, an "invaluable guide to having a good time" in using chemical products to

---

90. United States v. Falvey, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982). *See also* United States v. Duggan, 743 F.2d 59, 69 (2nd Cir. 1984) (Members of the Provisional Irish Republican Army fell within FISA's foreign power definition as a group engaged in international terrorism).

91. *See Falvey*, 540 F. Supp. at 1313.

92. Comprehensive Terrorist Prevention Act of 1995, S. 735, 104th Cong. (1995) [hereinafter CTPA]. The bill passed on June 7, 1995 by a vote of 91-8. 141 CONG. REC. S7880 (daily ed. June 7, 1995).

93. Holly Idelson, *Details of Anti-Terrorism Proposals*, 53 CONG. Q. 1178 (Apr. 29, 1995).

94. *See* 141 CONG. REC. S7684 (daily ed. June 5, 1995) (statement of Sen. Feinstein). The amendment was based in part on 18 U.S.C. § 231(a)(1) making it a federal offense to knowingly or intentionally teach or demonstrate the use, application or making of an explosive that will be unlawfully employed for use in or in furtherance of a civil disorder. *Id.*

blow up buildings, which she downloaded from the Internet.[95] After only mild debate,[96] the amendment, geared to the content and source of the message, was passed as part of the bill.[97]

Unfortunately, only the House version of the bill, the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA") ever passed both houses and became law.[98] AEDPA enhanced the ability of the U.S. government to respond to terrorist threats. Section 302 authorizes the Secretary of State, in conjunction with the Attorney General and Secretary of the Treasury, to designate as foreign terrorist organizations those groups that meet certain specific criteria.[99] Once this designation is applied, financial contributions are illegal.[100] Such a provision has been received within the law enforcement community as becoming an "invaluable tool" in disrupting the fundraising capabilities of international terrorist groups.[101] A watered down version of its Senate counterpart, the AEDPA could still have gone much further in taking effective steps towards eliminating terrorist threats from abroad.[102]

---

95. 141 CONG. REC. S7682 (daily ed. June 5, 1995) (statement of Sen. Feinstein).

96. *See* 141 CONG. REC. S7686 (daily ed. June 5, 1995) (statement of Sen. Hatch).

97. *See* CTPA tit. IX, § 901.

98. *See* 142 CONG. REC. H3618 (daily ed. Apr. 18, 1996) (passed in the House by a vote of 293-133); 142 CONG. REC. S3477 (daily ed. Apr. 17, 1996) (passed the Senate by a vote of 91-8).

99. Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, sec. 302(a), § 1189, 110 Stat. 1248.

100. *Id* sec. 303(a), § 2339B, 110 Stat. 1250 ("Whoever . . . knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title, imprisoned not more than 10 years, or both.").

101. Freeh, *supra* note 12.

102. Proposals to expand law enforcement powers in gaining credit reports and information on a suspect's business records were not included. Additionally, the original bill would have added terrorism-related offenses to the list the FBI may obtain approval to intercept wire or oral communications. *See Blown Away? The Bill of Rights After Oklahoma City*, 109 HARV. L. REV. 2074, 2084-87 (1996).

*B. Carnivore and its Application*

Within the FBI and law enforcement community, the realization was made in the mid-1990's that, on the intergovernmental plane, we must project and plan to forestall or respond adequately to possible terrorist disasters that while not necessarily assigned a high probability of occurrence, are expected.[103] For if they were to occur, the degree of injury would be deemed unacceptable either because it is irreparable or because of its projected political, social or economic costs. Due to the ever-growing dependence on high-tech industry and science-based systems, we must develop our capacities for "proacting" or "prosponding" to the dangers of international terrorism, rather than merely "reacting" or "responding."[104]

The classic method of such an anticipatory response to terrorism is intelligence gathering.[105] In modern constitutional democracies, this is an acutely sensitive issue as the potential for infringing on privacy is often a great concern. With existing terrorism, privacy and communication laws in place, intelligence agencies within the U.S. began pushing for more funding to conduct surveillance of Internet communications, to protect the nation's infrastructure from "information warfare."[106] The Carni-

---

103. *See generally* W. Michael Reisman, *New Scenarios of Threats to International Peace and Security: Developing Legal Capacities for Adequate Responses, in* THE FUTURE OF INTERNATIONAL LAW ENFORCEMENT: NEW SCENARIOS-NEW LAW? 13 (Jost Delbruck ed., 1993).

104. *Id.*

105. *See* Reisman, *supra* note 14, at 15. Other anticipatory yet less active responses by the U.S. and international community include tagging explosive materials to make their detection easier, regulating the sale of highly dangerous chemical and nuclear materials and multilateral conventions. *Id.* at 20-23. *See also,* G.A. Res. 51/210, U.N. GAOR 6th Comm., 51st Sess., 88th plen. mtg., at 3(b), U.N. Doc. A/51/631 (1996) (Measures to Eliminate International Terrorism); Convention on the Marketing of Plastic Explosives for the Purpose of Detection, Mar. 1, 1991, 30 I.L.M. 726; Organization of American States: Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives and Other Related Materials, Nov. 14, 1997, 37 I.L.M. 145; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T. 583.

106. DAVID BANISAR, PRIVACY & HUMAN RIGHTS 2000: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 232 (2000). Elec-

vore Diagnostic Tool, currently "Carnivore," was designed and developed by the FBI as an increasing number of criminal subjects turned to the Internet for communications with each other, producing a need for better digital discrimination in the surveillance of these transmissions where communication channels and addresses are often shared.[107] The program was originally conceived under the name "Omnivore" in February 1997, and later replaced in June 1999 by Carnivore, running on a Windows NT-based operating system.[108] Because many Internet Service Providers ("ISPs") lacked the ability to discriminate between communications in identifying a particular subject's messages to the exclusion of all others, the FBI developed Carnivore. The device provides the law enforcement agency with a "surgical" ability to intercept and collect communications with a warrant, while ignoring all other information transfers.[109] As the FBI describes it, Carnivore will work much like commercial "sniffers" and other network diagnostic tools used by ISPs regularly, except it will have the ability to distinguish between communications that may be lawfully intercepted and those that may not.[110] Basically a network analyzer, it runs as an application program on a normal personal computer ("PC"). It works by "sniffing" the proper portions of network "packets" (the standard unit of Internet traffic)[111] and copying and storing only those that match a finely defined filter set, programmed in conformity with the court order.[112] The

---

Electronic surveillance communication is viewed by the FBI as one of the most important capabilities for acquiring evidence to prevent serious crime (use of a suspects own words). *See* FED. BUREAU OF INVESTIGATION, PROGRAMS AND INITIATIVES, CARNIVORE DIAGNOSTIC TOOL *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited Oct. 1, 2001) [hereinafter CARNIVORE DIAGNOSTIC TOOL].

107. Kerr-House, *supra* note 11, at 13.

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

109. *See* CARNIVORE DIAGNOSTIC TOOL, *supra* note 106.

110. *Id.*

111. *FBI to Release Carnivore Documents*, USA TODAY (Aug. 17, 2000), *at* http://www.usatoday.com/life/cyber/tech/cti411.htm.

112. Kerr-House, *supra* note 11, at 13. For example, if a court order pertains to surveillance of e-mail only, Carnivore can be configured to exclude all others such as Web browsing. As a sniffer, it selects messages based on

device requires not only a court order, but also knowledge and assistance of ISP personnel for installation.[113]

For Carnivore surveillance, along with FISA warrants, interception of criminal wire and electronic communications are authorized under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA").[114] Congress passed Title III in response to the Supreme Court's holding in 1967, that wiretapping is a search and seizure, and that telephone conversations are entitled to protection under the Fourth Amendment.[115] As evidence of the speed in which technology can quickly make congressional action obsolete, Congress further amended Title III to include electronic communications in 1986 after a 1978 4th Circuit case, *United States v. Seidlitz,* established that the interception of a computer transmission was not contemplated by the original statute's concern with "wire communication" of an "aural acquisition."[116]

To view a communication's content, applications under Title III must state the offense being committed, place from which communications are to be intercepted, description of the types of conversations to be intercepted and identity of the persons anticipated to be intercepted.[117] The surveillance procedure also provides for some judicial oversight, limiting court orders to thirty days and requiring both periodic reports every seven to ten days during the surveillance, and justification for order extensions up to thirty days.[118] Upon the expiration of the intercept period, the communications must be presented to a judge and sealed. Even further, annual reports must be published on the number and nature of wiretaps. Only in cases of emergency can surveillance be permitted

---

criteria expressly set out in the court order, such as e-mails transmitted to and from a particular account or user. *Id.* at 14.

113. *Id.* at 14.

114. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2711 (1994) [hereinafter ECPA].

115. *See* Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).

116. United States v. Seidlitz, 589 F.2d 152, 156-57 (4th Cir. 1978), *cert. denied,* 441 U.S. 922 (1979).

117. ECPA § 2518.

118. *Id.*

to proceed immediately with authorization from high-level Department of Justice ("DOJ") officials, as long as a court order is filed within forty-eight hours.[119]

The ECPA amendments specifically extended statutory legal protection to wire and electronic communications, but on a 1986 basis when the Internet was just coming into common use and e-mail was barely used by the public. Statutory privacy protection was further created for "transactional records" of electronic communications, such as addressing, routing and billing, but nowhere do the laws come close to mentioning modern day e-mail.[120] In order for the FBI to view these types of records, an ECPA court order is necessary under Sections 3122-23.[121] To view the communication's actual content, a Title III (probable-cause based) order is used, as under Section 2703(a), and only those communications stored for over 180 days are readable by the FBI.[122]

Under 18 U.S.C. § 3121, the FBI is permitted to use "technology reasonably available to it" to conduct electronic surveillance.[123] While the technology of commercial sniffers at the time worked well, they were designed neither with deference to privacy rights nor as a law enforcement surveillance tool.[124] These detractions created shortcomings in the FBI's battle to combat acts of terrorism, threats to national security and cyber-crimes, primarily in the inability to distinguish between different communications. Like a funnel, everything that went through the sniffer was decoded without prejudice. What was needed was a device capable of filtering with precision certain electronic computer traffic like binary code, enabling government personnel to receive and view only

---

119. *Id.*

120. ECPA § 2703(c)-(d).

121. 18 U.S.C. § 3122-23 (1994). Here, the ECPA adopted the pen register and trap and trace statute, governing real-time interception of the numbers dialed or otherwise transmitted on a phone line. The pen register collects the electronic impulses that identify the number dialed, and the trap and trace device collects the originating number for incoming calls. This type of court order was first introduced under Title III for telephone communications. *See* Dempsey, *supra* note 30, at 23.

122. ECPA § 2703(a).

123. 18 U.S.C. § 3121(c) (1994).

124. *See* Kerr-Senate, *supra* note 40.

those specified communications as pertaining to the Section 3121 or Title III order.[125]

With this in mind, the tool, described by Marcus Thomas, head of the FBI's Cyber-Tech Section as nothing more than a PC with proprietary software,[126] is still not always necessary. If an ISP is capable of "completely, properly, and securely" complying with a court order for interception of a suspect's communication or account information, Carnivore is not deployed.[127] In the case of EarthLink Inc., the Atlanta based ISP serving 4.2 million subscribers nationwide, as they possess the ability to comply with a court order, they reached an agreement with the FBI to do all surveillance themselves without the use of Carnivore.[128]

If Carnivore is used, however, it is installed with the cooperation and technical assistance of the ISP technicians, via a bridging device, so that it can be positioned exclusively upon the small segment of network traffic where the subject's communications are directed.[129] Once deployed, Carnivore's first task is to filter a portion of an ISP's high-speed network traffic, or binary code, looking for the particular identifying information of the criminal subject.[130] If detected, the packets of the subject's communication are segregated for further filtering and storage according to the specific warrant. All other binary code that passed through the filter is neither recorded nor saved by the FBI.[131] Only after electronic filtering does the information leave the device in human readable form for FBI analysis. Current upgrades are also adding an integrity feature by imprinting on the readable communication the collection mode being used.[132] As the FBI intends, this will demonstrate that no alteration has been made to the filter settings.

---

125. *Id.*

126. *FBI E-Mail Snooping Sparks Controversy*, USA TODAY (July 13, 2000), *at* http://www.usatoday.com/life/cyber/tech/cti213.htm.

127. Kerr-Senate, *supra* note 40.

128. *See EarthLink Dodges FBI's Carnivore*, USA TODAY (July 14, 2000), *at* http://www.usatoday.com/life/cyber/tech/cti231.htm.

129. *See* Kerr-Senate, *supra* note 40.

130. *See* Ted Bridis & Neil King, Jr., *Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000, at A28.

131. *See* Kerr-Senate, *supra* note 40.

132. *Id.*

Carnivore employs new technology to counter the growing threats of the Information Age. It is currently being argued that privacy rights will remain protected by the same judicial oversight that has applied effectively for the last thirty years. [133] But as will discussed later, the time has come for the U.S. to adopt a new set of Internet privacy laws that set out surveillance guidelines based on modern 21st century technology and understanding, not via 1968, 1978 and 1986 standards. To its credit, Carnivore has only been used sparingly, in cases where an ISP itself cannot undertake the surveillance effectively, which explains why as of July 2000, Carnivore had only been deployed twenty-five times between 1998 and 2000, mainly for terrorist investigations.[134] In response to those who began ringing the alarm a few years ago, warning of the implications of undetectable criminal and international terrorist activity, Carnivore will now attempt to respond and fill that gap.[135] A gap still remains, however, in governing Carnivore via laws that are designed with modern international terrorist threats, capabilities and technologies in mind. To repair this, the U.S. must turn its attention to the U.K.'s RIPA for guidance.

## V. THE BRITISH ADVANCEMENTS WITH RIPA

Europe has viewed privacy as an important issue for hundreds of years. As early as 1361, the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers.[136] Parliamentarian William Pitt wrote in 1763, "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King of England

133. *See* Letter from John E. Collingwood, Assistant Director, Office of Public and Congressional Affairs, Federal Bureau of Investigation, to Brian Gallagher, Editor of the Editorial Page, USA Today (July 24, 2000), *available at* http://www.fbi.gov/hq/lab/carnivore/letter1.htm.

134. *Id.*

135. *See* Andrew W. Yung, *Regulating the Genie: Effective Wiretaps in the Information Age*, 101 DICK. L. REV. 95, 98-100 (1996).

136. Justices of the Peace Act, 1361, 34 Edw. 3, c. 1 (Eng.).

cannot enter."[137] This trend continued into the 20th century as Europe enacted the first data protection laws.[138] In the modern era, international bodies such as the United Nations, Council of Europe and European Union ("EU") have continued the trend in listing privacy as a human right. From these international conventions, Great Britain enacted RIPA to both deal with changes in technology and extend a tradition of privacy protection for the Internet.

### *A. International Privacy Protection in Europe*

In its Universal Declaration of Human Rights, the United Nations made it a point at its formation in 1948 to include privacy as a fundamental human right. Article 12 specifically states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attack."[139] The Council of Europe followed those same sentiments on the continent in the Convention for the Protection of Human Rights and Fundamental Freedoms ("Convention on Human Rights"). In Article 8, Member States agreed that:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health morals, or for the protection of the rights and freedoms of others.[140]

Both the European Commission of Human Rights

---

137. BANISAR, *supra* note 106, at 5.

138. *See* DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989).

139. G.A. Res. 217 A (III), U.N. GAOR, 3d Sess., Supp. No. 1, at 71, U.N. Doc. A/810 (1948).

140. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, 230 [hereinafter Convention].

and the European Court of Human Rights ("ECHR") enforce the articles of the Convention on Human Rights. Holding privacy to be an important right, the ECHR has consistently viewed the protections of Article 8 broadly and interpreted the reservations narrowly.[141] If a Member State such as the U.K. fails to impose wiretapping regulations, sanctions will be ordered.[142] Also drafted by the Council of Europe in 1980 was the Organization for Economic Cooperation and Development Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[143] Under these guidelines, specific rules for the handling of personal information must be enacted by each Member State. Personal data must be obtained fairly and lawfully, used only for original specified purposes, must be accurate, accessible to the subject, kept secure and destroyed after its purpose is complete.[144]

The EU has also weighed in on privacy in recent years. In the Data Protection Directives of 1995 and 1997, the EU sought to harmonize laws throughout its Member States to ensure consistent levels of protection for citizens and allow for the free flow of personal information.[145] Basic personal privacy guidelines were extended, and spe-

---

141. *See* Karen C. Burke, *Secret Surveillance and the European Convention on Human Rights,* 33 STAN. L. REV. 1113, 1122 (1981).

142. *See* BANISAR, *supra* note 106, at 7.

143. Organization for Economic Cooperation and Development, Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, Sept. 23, 1980, OECD Doc. C (80) 58, *reprinted in* 20 I.L.M. 422.

144. *See id.* The Council of Europe also adopted Recommendation No. R (99) 5 in February 1999, outlining the guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways (applies mostly to ISPs and Internet safety concerns for users). Council of Europe, Comm. of Ministers, Recommendation No. R (99) 5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet, adopted Feb. 23, 1999 at the 660th meeting of the Ministers' Deputies, *available at* http://www.coe.fr/dataprotection/rec/ elignes.htm (last visited Oct. 1, 2001).

145. *See generally* Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Council Directive 95/46]; Council Directive 97/66 of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 24) 1 [hereinafter Council Directive 97/66].

cifically, the Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector ("Directive 97/66") gave specific protections covering telecommunication networks.[146] The Protection Directives mainly deal with the right to know what data is being kept about you and further strengthens protections for sensitive personal data. One of the specific requirements is the creation of a data protection commissioner or "supervisory authority" within each Member State.[147] The commissioner's role is to consult with the government on legislation, conduct investigations of privacy violations, hear complaints and begin legal proceedings in cases of violations.[148] With these international directives and provisions in mind, the U.K. enacted RIPA.

### *B. The Regulation of Investigatory Powers Act*

While RIPA replaces a number of older British telecommunication and law enforcement laws, two privacy laws are also in effect. The Human Rights Act 1998 ("HRA") incorporates the Convention on Human Rights into domestic law and establishes an enforceable right to privacy.[149] The Data Protection Act 1998 updates the older Data Protection Act 1984 in accordance with the requirements of the EU's Data Protection Directives.[150] It ensures limitations on the use of personal information and is enforced by the independent Office of the Data Protection Commissioner.[151]

By 1999, British officials were reaching the same conclusions the FBI had a few years previous, that terrorists and criminal elements were turning to the Internet in droves to plan, communicate and carry out their crimes. Needing a step-up from telecommunication laws that were as old as the U.S.'s ECPA, the combination of a drastic improvement in technology and the guarantee of privacy rights in the HRA were the "twin drivers" for the

146. *See* Council Directive 97/66, *supra* note 145, arts. 2(c)-(d), 4-6.
147. *See* Council Directive 95/46, *supra* note 145, art. 28.
148. *Id.*
149. Human Rights Act, 1998, c. 42 (Eng.).
150. Data Protection Act, 1998, c. 29 (Eng.).
151. *Id.* § 51.

RIPA campaign.[152] Receiving Royal Assent on July 28, 2000, Home Secretary Jack Straw described the bill as playing a "crucial role in helping law enforcement agencies combat drug trafficking, terrorism and other serious crime."[153]

At its most basic, the benefit of RIPA is that in great detail, the law outlines the legal boundaries and obligations in modern Internet interception and surveillance. The law speaks directly to ISPs and the issues that make Web intercepts different from telephone wiretapping. Part I of RIPA repeals the Interception of Communications Act 1985 and provides a new regime for interception of communications in light of recent technological advancements.[154] Further, it incorporates Article 5 of Directive 97/66 requiring Member States to safeguard the confidentiality of communications.[155]

Section 1 creates the offense of unlawful interception of any communication that is being transmitted via telecommunication systems or the postal service.[156] This applies to "intercepted materials," or more specifically, the actual contents of the communication itself.[157] In order to lawfully intercept an Internet communication, either consent (including interception within the operation of the ISP services) or an "interception warrant" is required.[158] The penalty for violation of Part I is two years imprisonment and a civil fine of £5,000. For law enforcement agencies to obtain an interception warrant, an application must be made directly to the Secretary of State showing an electronic interception is necessary and the "conduct

152. James Middleton, *Encryption at the Mercy of the Law*, NETWORK NEWS (February 28, 2000), *at* http://www.vnunet.com/Analysis/107421 (quoting Home Sec. Jack Straw).

153. *Police Powers Expanded for Tapping of Wireless Internet* (June 23, 1999), *at* http://www.vnunet.com/News/85638.

154. *See Explanatory Notes to Regulation of Investigatory Powers Act 2000*, ¶ 8, *at* http://www.legislation.hmso.gov.uk/acts/en/2000en23.htm (last visited Oct. 1, 2001) [hereinafter *Explanatory Notes*].

155. *Id.* ¶ 9.

156. *See* RIPA, 2000, c. 29, § 1 (Eng.). "Telecommunications system" specifically covers communications transmitted via the use of "electrical or electro-magnetic energy." *Id.* § 2(1).

157. *Id.* § 20.

158. *Id.* §§ 3-5.

authorized by the warrant is proportionate to what is sought to be achieved by that conduct."[159] A warrant can only be deemed necessary by the Secretary for the same reasons as set out in Article 8 of the Convention on Human Rights, that the e-mail interception is in the interests of national security, the prevention of serious crime or for the safeguarding of economic well being.[160] If for economic well being, a warrant is only necessary when the information relates to acts or intentions of persons outside the U.K.[161]

To be effective, all warrants must name one person as the interception subject or the set of premises to be intercepted.[162] The specific type of communication to be intercepted must also be laid out, including any addresses, numbers or other factors that will be used in identifying the communication to be intercepted, such as name of the sender or receiver.[163] With this information, the Secretary of State is required to authorize a certificate describing the material that may be intercepted by law enforcement. Only that information contained in the certificate may legally be viewed.[164] A warrant issued in the interest of national security will remain effective for six months, and with cause, renewal is possible.[165] The Secretary of State may also modify the description of material interceptable if necessary.[166]

To implement the warrant, either the law enforcement agency or the ISP itself will be authorized to conduct the surveillance.[167] An ISP's failure to comply fully with the request is a convictable offense.[168] Further, all ISPs and law enforcement personnel are prevented from disclosing any knowledge of the warrant, interceptions or the information contained in any communication.[169] British ISPs will now be required to maintain a "reasonable"

159. *Id.* § 5.
160. *Compare id. with* Convention, *supra* note 140, at 230.
161. RIPA § 5.
162. *See id.* § 8.
163. *See id.* at (2-3).
164. See *Explanatory Notes*, *supra* note 154, at ¶ 79.
165. RIPA § 9.
166. *Id.* § 10(1)(b).
167. *Id.* § 11.
168. *Id.* § 11(7).
169. *Id.* § 19.

surveillance and interception capability.[170] Lacking a Carnivore type system, British law enforcement will be forced to rely on the less sophisticated and discriminating commercial sniffers available to ISPs. In the U.S., such a provision may be unnecessary with the FBI's diagnostic tool, but the benefit of a clear statute creating a duty amongst ISPs to assist in effective interceptions of the target's communications cuts to the heart of the matter.

Once information has been intercepted, strict restrictions are placed on its storage and handling. Distribution and disclosure of the communication must be kept to a minimum, and any copies made must be destroyed once they are no longer necessary. [171] In the years ahead, as investigations may begin to compile personal electronic communications, it is in the interest of the suspect's privacy that her information be handled and maintained carefully by law enforcement.

RIPA also makes the advancement of distinguishing between interception of a communication's content and interception of transactional information. Chapter II of the Act applies to "communication data" or the addressing information at the top of an e-mail, excluding content.[172] As with content interception, such acquisition must be deemed necessary. Those include interests of national security, prevention or detection of crime, economic well-being, public safety, protecting public health and preventing death in an emergency.[173] Compared to the criteria for sensitive e-mail content, circumstances have been expanded whereby only addressing information can be intercepted. Placing further protections on privacy, in order to view addressing information, authorization must be applied for as not only necessary but proportionate to the conduct involved.[174] Once authorization is granted, an ISP may be instructed, with notice, to disclose or obtain the specific e-mail data. If unable to do so, compliance is

170. *Id.* § 12.
171. *See* RIPA § 15.
172. *Id.* § 21.
173. *See id.* § 22(2)(a-h).
174. *Id.* § 22(5).

not required.[175] The authorization will remain effective for one month.

While Part I specifically applies to the interception of messages and transactional type data, Part II further merges all possible types of law enforcement surveillance into one compact law by creating a system of authorizations for physical "surveillance" and "covert human intelligence."[176] Surveillance is broken down into two types: "[D]irected" and "intrusive."[177] The former is defined as covert surveillance in relation to a specific investigation likely to result in obtaining private information about the subject, and the later as covert surveillance in relation to anything taking place on residential premises (usually by surveillance apparatus).[178] Like communication data interceptions, authorization applications to the Secretary of State must prove the normal necessity and proportionality.[179] For surveillance, authorization may also be obtained from officials within the National Criminal Intelligence Service or the National Crime Squad.[180] Overseeing these authorizations is the Surveillance Commissioner who has the power to "quash" or "cancel" any order.[181]

Part III of RIPA is by far the most radical and useful to law enforcement in analyzing Internet interceptions. It introduces a power to enable police, customs officials and members of the judiciary to serve notices on individuals or bodies requiring the disclosure of encrypted information or messages, in order to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal use of encryption.[182] As the White House recently announced safeguards on the most powerful types of encryption, this type of provision may be unnecessary in the U.S.[183] Currently, U.S. export control policy limits those countries to which American manufactur-

175. *See id.* § 22(4).
176. *Id.* § 26.
177. RIPA § 26(1).
178. *See id.* § 26(2)-(5).
179. *Id.* § 26(3-4).
180. *Id.* § 33(1).
181. *Id.* § 37.
182. *See Explanatory Notes, supra* note 154, at ¶¶ 225-27.
183. *See* Press Release, The White House, Administration Announces New Approach to Encrytion (Sept. 16, 1999), *available at* http://www.epic.org/crypto/legislation/cesa/WH_release_9_16.html.

ers may sell powerful data and voice-scrambling software and products. After a one-time review by the government, such security programs may be sold to foreign buyers in approved countries, excluding those countries that support terrorism.[184] The FBI also states that it has yet to encounter any encrypted messages via Carnivore surveillance it could not decode. Such a provision, requiring that citizens either turn over the "key" (a key, code, password, algorithm or other data that allows access to the electronic data or facilitates the putting of the data into an intelligible form)[185] they used in encoding the scrambled message, or in the least providing law enforcement with a plain text version of communications lawfully intercepted or seized,[186] deals with privacy and surveillance issues the FBI had no intention of addressing in its creation of Carnivore.

Examination of this provision by U.S. lawmakers and enforcers is beneficial, however, in understanding the overall new trends in effectively countering the growing threats of Internet based terrorism and technical advancements in crime worldwide. Under Part II of RIPA, disclosure can be required with "appropriate permission" by high ranking national security officers if the encoded communication is found "necessary" in the interests of national security, prevention of crime and economic well being of the country.[187] A notice to disclose can be served on private citizens for their seized or intercepted communications, and corporations as well for their encrypted files pertaining to an investigation.[188] These parties will receive compensation for any costs incurred in disclosing the requested information.[189] Failure to comply, however,

---

184. Countries on the approved sale list include members of the EU, Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. "Terrorist nations" include Iran, Iraq, Libya, Syria, Sudan, North Korea and Cuba. *See Clinton Proposes Updated Wiretap Laws*, USA TODAY (July 17, 2000), *at* http://www.usatoday.com/life/cyber/tech.cti236.htm; *US Eases Restrictions on Overseas Sales of Encryption Products* (September 17, 1999), *at* http://vnunet.com/News/90097.

185. RIPA § 56.

186. *Id.* § 49.

187. *Id.* § 49(3).

188. *Id.* § 49.

189. *Id.* § 52.

is a criminal offense. To preserve the covert nature of the operation, any person notified by security services to turn over a key or full text message is also barred from "tipping-off" others as to the investigation.[190]

Wisely, Part IV of RIPA enacts a system of oversight and judicial review, as well as a forum for filing complaints in the protection of privacy rights. Judicial review is by far one of the greatest fears of American civil libertarian groups in their opposition to Carnivore.[191] Section 57 provides for the creation of a special Interception of Communications Commissioner, who specifically oversees this new type of electronic surveillance and interception. The Commissioner's duties include a review of: Actions by the Secretary of State, the interception and surveillance regime, decryption notices and the adequacy of current arrangements for the protection of intercepted material.[192] Second, Part IV creates the position of Chief Surveillance Commissioner, whose role is to review the use of surveillance, agents, informants, undercover officers, decryption notices and the arrangements for protecting decryption keys to insure they remain within the boundaries of RIPA.[193] Finally, for the judicial oversight of this Act, a special Tribunal is created.[194] It will serve as the new forum for complaints charging the government with actions incompatible with the Convention on Human Rights, complaints by anyone subject to use of investigatory powers under RIPA and hold proceedings filed against any intelligence service.[195] This assures a direct avenue of recourse for anyone injured by the U.K.'s new 21st century electronic surveillance capabilities.

## VI. WHAT THE U.S. CAN TAKE FROM RIPA

The time has come to address the emerging threats of international terrorism through use of Carnivore. But in making such advancements in electronic surveillance of the expanding Internet, privacy rights and protection

190. *Id.* § 54.
191. *See* Dempsey, *supra* note 30, at 25.
192. *See* RIPA § 54.
193. *Id.*
194. *See id.* § 65.
195. *Id.*

must also be given an update, bringing them in line with current technological capabilities, standards and Internet threats. The U.K. is the first amongst the common law nations, and the world, to implement just such a change. By adopting several of RIPA's protections, the U.S. must harmonize existing privacy and surveillance law, currently covering three different avenues of obtaining taps into one new law in line with the realistic capabilities of the 21st century.

One of the most pressing needs for new regulation in the U.S. is the growing fear of Carnivore concerning protection of privacy. When word of the tool was announced in spring 2000, civil libertarians and many in Congress began calling for a strengthening of privacy laws as revolutionary changes in communication have left current statutory protections outdated.[196] Of equal concern, is that as Carnivore examines all network traffic looking for its target, it has the potential to capture the communications of those not subject to an order.[197] By filtering out just the transmission information, Carnivore still has the potential to capture the entire content of the electronic message.[198] In an attempt to respond to these fears,[199] Attorney General Janet Reno announced in July 2000 that the technical specifications of the system would be reviewed by an independent outside group of experts.[200]

In December 2000, the Illinois Institute of Technology Research Institute ("IITRI") released its evaluation of Carnivore version 1.3.4.[201] As to the direct inquiries of the

196. *See* Dempsey, *supra* note 30, at 24-25; Ted Bridis, *Congressional Panel Debates Carnivore as FBI Moves to Mollify Privacy Worries,* WALL ST. J., July 25, 2000, at A24.

197. *See Carnivore's Challenge to Privacy and Security Online: Hearings Before the House Comm. on the Judiciary, Subcomm. on the Constitution,* 106th Cong. (2000) (testimony of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology), *available at* http://www.cdt.org/testimony/000724davidson.shtml (last visited Oct. 1, 2001) [hereinafter Davidson].

198. *Id.*

199. A recent study also found 87% of Americans were concerned about their on-line privacy. *See* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf (last visited Oct. 1, 2001).

200. *Reno to Accelerate 'Carnivore' Review*, USA TODAY (August 4, 2000), *at* http://www.usatoday.com/life/cyber/tech/cti341.htm.

201. IIT RESEARCH INST., INDEPENDENT TECHNICAL REVIEW OF THE

DOJ, the IITRI concluded that: When used in accordance with a Title III court order, Carnivore provides investigators with only the permitted information; no operational or security risks are posed to ISPs; Carnivore reduces, but does not eliminate the risk of FBI agents acquiring unauthorized electronic communication information; and taking into account the high level of risks, Carnivore still requires more protections.[202] IITRI's general conclusions as to broader concerns were that Carnivore is more effective in protecting privacy than commercial sniffers, and while FBI and DOJ policy require oversight, U.S. law has yet to address it.[203] Further, Title III fails to extend statutory suppression for illegal interception by FBI agents to electronic communications.[204] Carnivore also lacks the "power 'to spy on almost everyone with an e-mail account,'" nor does it read and record all e-mail messages flowing through an ISP or "monitor web-surfing and downloading habits of all . . . ISP[] customers."[205]

Of the RIPA benefits that can be applied to Carnivore and some of the issues raised by IITRI, the most basic is its update and harmonization of surveillance and court order requirements for electronic surveillance. In 1986, when the ECPA was enacted, the Internet and its communication capabilities could not have been understood to evolve into what we are now facing. After all, the boom occurred only within the last eight to nine years. Under the ECPA, "electronic communications" have changed drastically since 1986.[206] Section 3121 trap and trace court orders[207] are even arguably outdated for the Web, as instead of running through a dedicated circuit for an entire telephone conversation, information sent across the Net via packet switching technology breaks the transmission down into data packets and sends them

---

CARNIVORE SYSTEM: FINAL REPORT (2000), *available at* http://www.cdt.org/security/carnivore/001214carniv_final.pdf (last visited Oct. 1, 2001) [hereinafter FINAL REPORT]. For an in-depth review of the components and abilities of Carnivore, see *id.* at 3-1-28.

202. *Id.* at xii.

203. *Id.*

204. *Id.*

205. *Id.* at xiii.

206. ECPA, 18 U.S.C. § 2510 (1994).

207. 18 U.S.C. § 3121 (1994).

through multiple networks to their destination.[208] Further, a pen-trap device used in these court orders, by definition, is attached to a telephone line and records only numbers dialed from or into that telephone line.[209] Carnivore, on the other hand, has the capability of intercepting the contents of communications, not phone numbers.[210] This technology is quite different from the standard telephone capabilities of 1986. When FISA was enacted in 1978 to allow surveillance of terrorist organizations, wire telephones were the primary source of communication put under surveillance. The Internet at that time was still a device for scientists.[211] An update now would allow for legislation to be written in modern Web terms, specifically contrasting traditional telephone numbers with more revealing addressing information of e-mails.

New legislation would also merge existing statutes into one section. Under the current mix, Carnivore surveillance orders can be issued through three different means – the ECPA (Title III), FISA and Section 3121. With a new law compiling them, one act can be divided between Carnivore interception of e-mail content as in RIPA Chapter I; interception of a communication's transactional addressing information as in Chapter II; and official oversight as in Part IV.

It is Part IV of RIPA, high-level oversight, which is also an imperative of any new U.S. legislation. Recent reactions to Carnivore have voiced a concern that under the current system written in terms of telephone surveillance, a diagnostic tool with the possible capabilities of scanning all Internet network traffic demands greater oversight.[212] As RIPA creates the new positions of Interception of Communications Commissioner and Chief Surveillance Commissioner,[213] so too must Congress appoint officials, even within the DOJ, whose specific role is to oversee the legal use of Carnivore and ensure privacy is protected.

---

208. *See* Wiseman, *supra* note 27.

209. *See* 18 U.S.C. § 3127(3)-(4) (1994).

210. *See* PRIVACY FOUND., LEGAL AND TECHNICAL ANALYSIS OF CARNIVORE CRITIQUE 1-2 (2000), *available at* http://www.privacyfoundation.org/pdf/CarnivLT.pdf (last visited Oct. 1, 2001).

211. *See* Wiseman, *supra* note 27.

212. *See* Davidson, *supra* note 197.

213. RIPA, 2000, c. 29, §65 (Eng.).

Monthly reports should be required, outlining the current state of the device and how often it is being employed. With a tool as radical and advanced as Carnivore, DOJ openness concerning its use will do much in calming fears of the device's capabilities.

RIPA also creates another balance between privacy and countering terrorism that may work well in the U.S. Within Part I, ISPs are directed to provide a "reasonable interception capability" in their networks.[214] If law enforcement is unable to make a communication interception, the ISP will be instructed to do so. This occurs because British law enforcement lacks the capabilities of affecting a seizure itself. The ISPs, using commercial diagnostic tools, will be primarily relied upon. Carnivore, on the other hand, is employed in exactly the opposite fashion – if an ISP cannot conduct the discriminatory surveillance, only then will the FBI bring in its device.[215]

What if, however, the role was reversed, as in the case of RIPA, and the FBI turned over Carnivore PCs to ISPs so they could conduct the ordered surveillance themselves. This would further aleviate fears as it would no longer be the government possessing the ultimate power to survey our network connections but the ISPs themselves, who have far less incentive to act the "Big Brother" role than the government. Currently, an ISP is capable of viewing its network traffic anyway, and does so in time of repair work. With proper constraints and duties placed on ISPs in a new bill, Congress could enact strict guidelines and liability, forcing ISPs to conduct the surveillance within the constraints of the court order. Further, disclosure of information should be barred to anyone other than the FBI who has requested it. This type of "anti-tipping" statute is already a part of RIPA.[216]

These changes, taken together in a new U.S. Internet surveillance and privacy bill will allow for the safe use of Carnivore while satisfying the concern of both civil libertarians and members of Congress, such as Rep. Bob Barr (R-Ga.), who, in the past has called for the tool to be

214. *Id.* § 11.
215. *See* Kerr-Senate, *supra* note 40.
216. *See* RIPA § 54.

reined in, with more constraints then currently exist.[217] As more and more personal information is being moved onto network based files, a law following the current trend of RIPA, based on decades if not centuries of European privacy ideals has the best chance of finding a middle ground in satisfying both our national security concerns in light of new international terrorism, and our desire for privacy in this new form of 21st century communication that is unfortunately employed by both good and bad alike.

## VII. CONCLUSION

Privacy is a fundamental human right, but so is security. In the new century, the capabilities of those who wish to bring harm to the United States will increase drastically through use of the Internet. Combined with realities that in the near future, nuclear, chemical and biological weapons will be used within these borders, this threat must be countered immediately and as effectively as possible. Through the employment of the Carnivore Diagnostic Tool, the FBI will have the capability to track terrorist communications as they enter the U.S. from around the globe. This device must, however, be deployed in conjunction with a new, comprehensive communication surveillance law that balances new threats with privacy concerns as well as the full capabilities of the Net. In its creation, the United Kingdom's RIPA must be followed as a model for Internet privacy in the 21st digital century.

## VIII. POSTSCRIPT

Regardless of the outcome in Afghanistan in the coming months, the threat of international terrorism will not be quashed any time soon. While Osama bin Laden may eventually be killed or brought to trial in the U.S., his terror network and others just like it still span the globe.[218] Others will be willing to take his place. The goal

---

217. *Timetable Set for 'Carnivore' Disclosures*, USA TODAY (Aug. 3, 2000), *at* http://www.usatoday.com/life/cyber/tech/cti333.htm.

218. *See* Patrick E. Tyler, *British Detail bin Laden's Link to U.S. Attacks*, N.Y. TIMES, Oct. 5, 2001, at A1

of wiping out terrorism is one that will take many years and an international undertaking the likes we have never seen.

In the aftermath of September 11th, Congress has rushed new legislation to the floor in an attempt to prevent further attacks. One specific bill directly addressing electronic communication surveillance is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.[219] Of its proposed amendments, Section 203(b) would empower local and federal authorities to share knowledge of the contents of any wire, oral or electronic communication in order to prevent an attack on the U.S. by a foreign power or international terrorist group.[220] FISA surveillance orders targeting foreign powers would also now be extended to one year.[221] Further pertinent would be an amendment to the ECPA allowing ISPs to disclose the contents of a subscriber's electronic communication to any government authority, if the ISP reasonably believes an emergency involving danger of death or serious physical injury is imminent.[222] By this, ISPs would now be encouraged to screen e-mails sent through their system, looking for suspicious communications in the name of home defense.

The possibility of FBI abuse of Carnivore looms larger than ever before, now that we have entered the reactionary faze in our response to the attacks. While the system is invaluable in tracking the communications of terrorist cells around the world, a protection of privacy must still remain a factor in this new era. These are the times that fundamental rights must be upheld, despite the tendencies to take drastic measures. In expanding surveillance orders and encouraging an overall sense of ISP vigilance, definitive standards for Carnivore's full implementation, taking the unique nature of an e-mail's transmission information and content into account, are still lacking. Clear oversight should be implemented. Carnivore is clearly a necessary step in the new war on terrorism, now that *al Queda's* capabilities have been

219. H.R. 3162, 107th Cong. (2001).
220. *Id.* § 203(b).
221. *Id.* § 207(b).
222. *Id.* § 212.

seen on U.S. soil, and fears of future attacks and Anthrax are on the minds of many Americans. Yet Congress must still take heed to adopt uniform safeguards and greater oversight in the 21st century's new war on terrorism.

*Seth R. Merl*[*]

[*] To all those who lost their lives on the morning of September 11th, be it at work or in the line of duty at the World Trade Center, the Pentagon and in a Pennsylvania corn field. We have all been filled with sorrow and a sense of helplessness, and like all New Yorkers, I have wanted to do something to help rebuild my city. The dedication of this Note is but a small token.