The Erosion of Online Privacy Rights in the Recent Tide of Terrorism

by
*Thomas P. Ludwig**

I. Introduction

Imagine a world where any idea or message communicated to another individual is subject to governmental scrutiny for possible criminal, subversive, or terroristic content. The current location of any individual, as well as the places that he or she commonly frequents, can easily be tracked through that person's phone calls, online activity, and financial records, which are all accessible to government agencies. By intercepting e-mails and tracking online browsing, shopping, and other activities, the most intimate details, habits, and preferences of the average individual are readily available to the prying eyes of cyber-criminals and law enforcement officials alike. Scenarios such as this one have been played out in a vast array of films, novels, and predictions.[1] Those of a more pragmatic nature would attempt to dismiss such ideas as fiction created to take advantage of the popular conspiracy theory paranoia that permeates today's culture. Without lending credence to the more bizarre theories circulating among extremist groups and Internet chat rooms,[2] the situation described above is much more realistic than one would like to imagine. In fact, taking into account the surveillance tools that law enforcement agencies are known to possess today, their extensive record of abuse of authority, and the current state of electronic privacy protection law, the above situation is entirely plausible.

There is one question that immediately arises in response to this shocking proposition: how could such a situation develop in a country that was built around the concept of individual freedom? While there are obviously many factors, two reasons stand out above the rest. First, the state of electronic privacy protection law has been unable to keep pace with the rapid

---

* The author received a B.A. in Mathematical Economic Analysis and Managerial Studies from Rice University in May 2001 and is a candidate for Juris Doctor, class of 2004, at Southern Methodist University Dedman School of Law. The author would like to thank the staff of the Computer Law Review & Technology Journal for their helpful editing and his family for their constant support.

1. For some notable examples, see George Orwell's novel *1984* and the recent film *Enemy of the State*. George Orwell, 1984 (1948); Enemy of the State (Buena Vista Pictures 1998).

2. One of the more amusing and popular of such outlandish conspiracy theories involves a United Nations takeover of the United States with "Little Black Helicopters," which have been frequently spotted during operations in various locations around the country. *See* Preston Peet, *Black Helicopters Come in All Shapes and Colors*, Disinformation.com (Dec. 20, 2000), at http://www.disinfo.com/archive/pages/dossier/id458/pg1/.

development of modern wireless and online technology. Legislation enacted decades ago, which was at one time sufficient to protect privacy rights with respect to communication, was only significantly modified once before the turn of the millennium in an attempt to bring the standards of protection up to date with the addition of computers, cell phones, instant messaging, e-mail, and other communication developments.[3] This explosive growth in technology has given criminals greater opportunity and an increasingly vast array of tools with which to commit their crimes,[4] and has also forced law enforcement agencies to develop and utilize similarly advanced means to combat their commission. Meanwhile, innocent citizens are caught in the crossfire; the escalating crime jeopardizes the public's safety, while law enforcement's attempts to prevent such crime often results in the invasion of their privacy. The law has been unable to keep up in regulating this ongoing struggle.

The second major factor behind the current deficiency in electronic communications privacy protection is the recent trend of increasing crime and terrorist attacks, the most significant example being the tragic series of events that took place on September 11, 2001.[5] Evidence that surfaced shortly after September 11 showed that the terrorists responsible for the attacks had relied extensively on e-mail and the Internet to plan the attacks.[6] In addition, according to the FBI, there has been a steady rise in both cybercrimes, such as computer fraud, and crimes planned or accomplished with the aid of electronic communication and the Internet.[7] This increase in criminal and terrorist activity and the public's resulting sense of vulnerability has

3. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (known as the "Wiretap Act"), which was enacted to protect against unlawful interception of wire communications, was amended by the Electronic Communications Privacy Act of 1986 in an attempt to incorporate statutory safeguards for stored and electronic communications. 18 U.S.C. § 2511 (2000).

4. Stephen W. Tountas, Note, *Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?*, 11 WASH. U. J.L. & POL'Y 351, 362-63 (2003).

5. The sarin nerve gas attack in a Tokyo, Japan subway and the bombing of the Oklahoma City Murrah Federal building in 1995 brought terrorism to the forefront of the American public's attention and resulted in pressure on the government to take action. The legislature responded by enacting the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of 18 U.S.C.), and also the Defense Against Weapons of Mass Destruction Act of 1996, 50 U.S.C. § 2301 *et seq*. (2000).

6. David S. Fallis & Ariana Eunjung Cha, *Agents Following Suspects' Lengthy Electronic Trail*, WASH. POST, Oct. 4, 2001, at A24.

7. *Internet and Data Interception Capabilities Developed by FBI: Hearing Before the H.R. Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 5 (2000) (statement of Donald M. Kerr, Assistant Laboratory Division, Federal Bureau of Investigation).

shifted pressure on the government from privacy concerns to safety issues. Not surprisingly, the American public has implicitly conceded a measure of its privacy rights in order to regain some sense of security, and the legislative and executive branches have responded accordingly, most notably with the passage of the USA PATRIOT Act (hereinafter "Patriot Act").[8] The Patriot Act, quickly enacted after the September 11 attacks in an effort to prevent future attacks, further reduced the already insufficient statutory protection of electronic communications privacy.

The September 11 attack made it clear that certain steps and concessions in individual freedoms were necessary in order to allow law enforcement to combat the threat of terrorism effectively. As Chief Justice William Rehnquist once wrote, "It is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime."[9] While this observation rings true now, the current approach unnecessarily disregards privacy protection, especially with respect to electronic communication. This Note will discuss how some of the statutory authority currently granted to law enforcement allows for excessive intrusion into the privacy of innocent individuals and how other law enforcement mechanisms could be tempered with judicial or neutral supervision so that privacy protection is guaranteed without sacrificing the effectiveness of those tools in combating terrorism and crime.

Under the current statutory regime, law enforcement agencies have been given essentially carte blanche to conduct their surveillance, monitoring, and investigation. Only the barest standards of relevance to an ongoing criminal investigation must be established in order to begin most types of surveillance of an individual.[10] For some types of surveillance, obtaining judicial approval is strictly a formality: the judge *must* grant the request or has little real discretionary power to deny it.[11] In most law enforcement investigations, judicial oversight is minimal, occurring only at the outset.

Taking into account past misconduct by law enforcement agencies even when more stringent and up-to-date privacy protection laws were in place,[12] it is frightening to consider the potential invasion of electronic privacy rights by law enforcement unfettered by judicial oversight or a necessary showing of criminal activity. In addition, in both civil and criminal cases involving electronic privacy rights and their statutory protection, courts have consistently interpreted the law in favor of decreased protection and are likely to

8. The full name of the act is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. Pub. L. No. 107-56, § 213, 115 Stat. 272 (2001).

9. WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 224-25 (1998).

10. *See infra* note 108-09 and accompanying text.

11. *See infra* note 109 and accompanying text.

12. *See infra* notes 137-43 and accompanying text.

continue doing so.[13] Such judicial interpretation has only compounded the rate at which privacy rights have been eliminated. It is an oft-stated axiom that this country's government was founded on a system of checks and balances. Such safeguards have been removed, however, with respect to the power of law enforcement agencies and their surveillance of potential criminals and terrorists.

Because any substantive governmental analysis demands a historical perspective, Part II of this Note begins by describing instances from this country's past when it faced threatened or actual foreign attack and how the country reacted to such danger. The governmental responses in each of these past situations egregiously violated the civil liberties of American citizens without significantly achieving the intended goal of safeguarding national security. The manner in which this country overreacted to these past threats and excessively intruded upon personal freedoms should be a warning to the current government not to let history repeat itself. Part II also briefly discusses why the right to privacy in electronic communication is currently the most important liberty at stake as a result of increasing online criminal activity and the added threat of terrorism.

Part III begins by briefly relating the history of legislation affecting electronic communications privacy rights. This description includes examples of how the judiciary has applied this legislation in actual cases. This Part advances the argument that, to counterbalance the current potential for privacy invasion, the judiciary must reverse its trend of interpreting the law in a manner that weakens electronic communication privacy. Weaknesses in the privacy protection legislation prior to the Patriot Act are also noted in this Part for the purpose of demonstrating how the Patriot Act compounded the negative effects of already existing flaws in the statutory regime.

Part IV provides an overview of the Patriot Act as it relates to electronic communication privacy. This Part discusses both the Act's strengths in aiding law enforcement to combat crime and terrorism more effectively and its weaknesses in insufficiently protecting the privacy rights of innocent civilians. While this Note is not intended to provide an exhaustive analysis of the Patriot Act, this Part concludes by offering suggestions for legislative and judicial improvement of the Act and its interpretation.

13. *See e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (following the approach of similar cases from various jurisdictions in holding that the protections of the Wiretap Act do not extend to the unauthorized access of a secure website); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (holding that the government's acquisition of e-mail messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an "interception" under the Wiretap Act); *see also* Carrie L. Groskopf, Note, *If It Ain't Broke, Don't Fix It: The Supreme Court's Unnecessary Departure From Precedent in Kyllo v. United States*, 52 DEPAUL L. REV. 201, 204 (2002) (stating that "the Court will probably bend over backwards to allow U.S. intelligence to take whatever measures are necessary in order to ensure that more American lives are not lost in vain").

Finally, Part V compares the United States' responses to the past national security threats outlined in Part II with its present reactions to the threat of terrorism. Such an analogy provides practical lessons and warnings to those currently serving in each of this nation's three branches of government. This Part explores those safeguarding past situations to shed light on where to draw the line between protecting domestic security and individual liberties.

II. Past Governmental Overreaction to Foreign Threats Resulting in Intrusions on Civil Liberties

Even in this country, most individuals agree that certain personal freedoms must be relinquished in times of war for the sake of additional personal safety or the greater likelihood of emerging victorious. Many alive today remember the major conflicts involving this country over the last century; many of those actually fought or participated in the various war efforts or endured blackouts and shortages in staples of daily living. The likely reason behind the willingness to make such sacrifices is that there is little meaning to the amount of freedom one has as an individual if one is not alive to enjoy that freedom. If a temporary sacrifice in some of those freedoms insures that their future enjoyment will be completely restored, most are willing to make that sacrifice. However, most individuals would also agree that there is a limit to how much of their civil liberties they are willing to sacrifice for the sake of that additional safety, especially when the liberties are fundamental or unnecessary to secure victory or safety. As Benjamin Franklin once wrote, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[14] While this statement was made during a time when this country was fighting for its basic independence, it was no less applicable at any other point in this country's history or even today.

A. World War I

During World War I, it became clear to Americans that Germany's plan for world domination included the United States. Intelligence information intercepted from German naval and diplomatic officials evidenced Germany's destructive intentions toward the United States.[15] British intelligence intercepted the infamous Zimmerman telegram, in which the German Foreign Minister (after whom the telegram later became known) proposed a pact

14. John Bartlett, Bartlett's Famous Quotations 422 (Emily Morrison Beck ed., 14th ed. 1968) (quoting Benjamin Franklin from Historical Review Of Pennsylvania (1759)).

15. William C. Banks & M. E. Bowman, *Executive Authority for National Security Surveillance*, 50 Am. U. L. Rev. 1, 20 (2000). Evidence revealed that German naval officers had extensively researched and created numerous plans for invasion of the U.S. at different points along the eastern seaboard.

between Germany and Mexico against the United States in the event that war with this country became unavoidable.[16] "Operations by Germany in the United States were neither extensive nor appreciably effective, but sabotage, intelligence and propaganda operations did occur."[17] Because there was no statutory framework for dealing with such a threat or its perpetrators, steps to counter these dangers stemmed from Presidential authority and directives.[18] President Wilson's administration felt that Germany's greatest threat to the United States was in the form of domestic subversion.[19]

In 1917, the United States declared war on Germany as a result of President Wilson's urging and in reaction to this threat of German domestic subversion. The Espionage Act was enacted in that same year, which prescribed enormous fines, prison sentences, and confiscation of property for those guilty of involvement in a long list of vaguely defined anti-war activities.[20] The Espionage Act also authorized the government to wiretap private communications, search and seize private property, censure writings, restrict the right to public assembly, and even open mail.[21]

The Sedition Amendment of 1918 to Section 3 of the Espionage Act was even more severe in that it authorized extremely harsh penalties for "disloyal, profane, scurrilous, or abusive language" concerning the Constitution, the government, the military, or the flag.[22] Anyone who spoke out or wrote against United States participation in the war was arrested and charged for expressing views contrary to government opinion.[23] In addition to the statutory infringement on basic civil liberties, such legislation, combined with government-promoted coercive propaganda, stirred the public into a frenzy

16. BARBARA TUCHMAN, THE ZIMMERMAN TELEGRAM 146 (1958).

17. Banks & Bowman, *supra* note 15, at 21-22. German operations included fires and explosions targeted at munitions factories.

18. *Id*. at 22.

19. CHRISTOPHER ANDREW, FOR THE PRESIDENT'S EYES ONLY: SECRET INTELLIGENCE AND THE AMERICAN PRESIDENCY FROM WASHINGTON TO BUSH 54 (1995) (noting that "threat of domestic subversion was the primary target of United States wartime intelligence").

20. *See* Espionage Act § 2, *available at* http://www.staff.uiuc.edu/~rcunning/espact.htm (as enacted in 1917).

21. Banks & Bowman, *supra* note 15, at 22.

22. William M. Wiecek, *The Legal Foundations of Domestic Anti-Communism: The Background of Dennis v. United States*, 2001 SUP. CT. REV. 375, 386 (2001).

23. Over 1,500 individuals were arrested and charged under these Acts during World War I. Eugene V. Debs, the famous socialist leader of the time, was sentenced to ten years in a federal penitentiary for an academic speech discussing the economic causes of war. *See* Debs v. United States, 249 U.S. 211 (1919).

of anti-German hysteria.[24] Innocent German-American citizens were verbally and physically abused and even murdered for being subversives and traitors.[25] German books were destroyed, schools ceased to teach the German language, and German towns were renamed.[26] Those dissenting against such activity or the war in general faced similar abuse.

Surprisingly, the courts lent their support to the legislation greatly responsible for these atrocities. In *Schenck v. United States*, the Supreme Court upheld the conviction of the general secretary of the Philadelphia Socialist Party for publishing pamphlets protesting American involvement in the war.[27] Writing for the majority, Justice Oliver Wendell Holmes justified this decision with his now famous statement that, when the exercise of the First Amendment right of free speech constitutes a "clear and present danger" to the nation, Congress possesses the authority to suspend that right.[28] The United States government in its entirety supported the denial of fundamental civil liberties of its own citizens merely to protect against German infiltration and subversion, which was largely non-existent and greatly exaggerated.[29] While it is commonly said that hindsight is 20/20, there is clearly a lesson to be learned in the present regarding perceived threats to national security, even if no blame is attributed to past governmental reaction to public hysteria and paranoia.

B. World War II

During World War II, the United States faced more than the threat of invasion posed by Germany in the previous war. Japan's surprise attack on Pearl Harbor on December 7, 1941, struck a devastating blow to the heart of the United States Navy and left the American public reeling in a state of shock long after the "date which will live in infamy" had passed.[30] The attack was almost completely unexpected, especially since Japanese diplomats remained in the process of conducting peace talks in the final days leading up

24. *See* Wiceck, *supra* note 22, at 386.

25. *Id*.

26. Paul D. Carrington, *Fearing Fear Itself*, 5 GREEN BAG 2d 375, 376 (2002).

27. 249 U.S. 47 (1919).

28. *Id*. at 52 (holding that "[t]he question in every case is whether the words used are used in such circumstances and are of such a nature as to create a *clear and present danger* that they will bring about the substantive evils that Congress has a right to prevent.").

29. Carrington, *supra* note 26, at 376. "There was during the war one detonation of military supplies in New Jersey that may have been an act of sabotage, but there was no other instance of effective espionage or sabotage detected during or after the war to justify mistrust of German-Americans." *Id.*

30. President Franklin D. Roosevelt, Address to Joint Session of Congress (Dec. 8, 1941).

to the attack.[31] Within a period of only two hours, the United States's Pacific fleet had been substantially destroyed and America had a deadly new enemy on its western front. Because intelligence on the Japanese was not entirely reliable, it was unclear what they had planned next and both the public and military feared a Japanese attack on a defenseless Pacific coast.

Following the attack on Pearl Harbor, military and government officials grew concerned that Japanese-Americans felt more loyalty toward Japan than the United States. As a result, they pressured President Roosevelt to sign Executive Order 9066, which granted the military the authority to exclude anyone posing a risk to national security from threatened geographical areas.[32] The only significant opposition to this order came from the American Civil Liberties Union and the Quakers.[33] Japanese-Americans, including women and children, were ordered to leave their homes, businesses, and possessions, and were evacuated into internment camps located in the desert. These Americans were forced to live in poor and cramped conditions as prisoners behind barbed-wire fences for nearly three years following the signing of Executive Order 9066. Even if the displacement of Japanese-Americans was justified by reasons of national security, their brutal and unconscionable treatment at the hands of the camp guards was not. Numerous internees were shot and killed, some in the back, for nothing more than being severely ill or holding protests.[34] From the conclusion of World War II, it took the United States government three years to issue an apology or extend compensation to those forced into camps.[35]

---

31. ANDREW, *supra* note 19, at 212. There remains great intrigue as to whether President Roosevelt was aware of the attack on Pearl Harbor prior to its occurrence. *Id.*

32. Exec. Order No. 9066, 3 C.F.R. 1092 (1942), *available at* http://www.library.arizona.edu/images/jpamer/execordr.html (last visited Oct. 25, 2003). These geographical areas included all of California, half of Washington and Oregon, and one-third of Arizona. *Id.*

33. William R. Tamayo, *When the "Coloreds" are Neither Black Nor Citizens: The United States Civil Rights Movement & Global Migration*, 2 ASIAN L.J. 1, 5-6 (1995).

34. Eric L. Muller, *All the Themes But One*, 66 U. CHI. L. REV. 1395, 1408-09 (1999); SANDRA TAYLOR & HARRY KITANO, JAPANESE AMERICANS: FROM RELOCATION TO REDRESS 52-53 (Roger Daniels ed., Univ. of Utah Press 1986).

35. Robert Westley, *Many Billions Gone: Is it Time to Reconsider the Case for Black Reparations?*, 40 B.C. L REV. 429, 450 (1998). In 1948, Congress passed the American-Japanese Evacuation Claims Act, which granted internees a paltry 10 cents for every dollar lost, provided they were able to establish the requisite proof of loss. *Id*. Japanese-Americans would not truly begin receiving reparations for their losses until President Ronald Reagan signed the Civil Liberties Act of 1988 into law, more than 40 years after they were released from the internment camps. *Id*. at 451.

As it did during World War I, the judiciary supported the executive and legislative branches' extreme reactions to the Japanese threat. Fred T. Korematsu, a Japanese-American, challenged the discriminatory nature of the forced relocation to internment camps in *Korematsu v. United States*.[36] In that case, the Supreme Court held that although the compulsory exclusion order based on race was "inconsistent with our basic governmental institutions," the extreme circumstances caused by the threat of hostile Japanese forces necessitated the extreme measures.[37] The Court claimed that the government had necessarily taken such exclusionary action based on evidence of disloyalty on the part of Japanese-Americans.[38] The bitter irony behind this statement was that during the entire course of the war, ten people were convicted of spying for Japan, all of whom were Caucasian.[39] The Supreme Court also attempted to bolster its reasoning with a dubious twist of logic, arguing that Korematsu was not excluded based on any hostility towards his race, but rather because America was at war with the Empire of Japan.[40] This argument was clearly inaccurate, however, considering that the same Japanese-Americans forced into internment on suspicions of disloyalty were also drafted to fight against Japan.[41]

Following the precedent of World War I, all three government branches united to systematically deny American citizens their civil liberties. A plaque on a former Japanese relocation center probably best summarizes the lesson to be learned from this shameful moment in American history, one that was obviously not learned from the previous world war: "May it serve as a constant reminder of our past so that Americans in the future will never

36. 323 U.S. 214 (1944). Possibly even more disconcerting than the holding in this case is the fact that the Supreme Court delayed its decision upholding Executive Order 9066 until December 18, 1944, the day after Public Proclamation No. 21 allowed the evacuees to return home. *Id.*

37. *Id*. at 220.

38. *Id*. at 223.

39. DEBRA LAFOUNTAINE & PEI P. WANG, HISTORICAL BACKGROUND (1995); *see also* Curtis B. Munson, *The Munson Report*, *available in part at* http://www.curriculumunits.com/crucible/whunts/munson_report.htm (last visited Oct. 25, 2003) (noting in this special report to President Roosevelt that all evidence pointed to the fact that Japanese Americans were perfectly loyal to the United States). This special report, which was based on investigation into Japanese-Americans residing in Hawaii and California, was kept secret by the military and the executive branch in order to better facilitate the evacuation of the Japanese-Americans. Had this report been released to the public, as it undoubtedly would have been had the results been different, it would have been extremely difficult to justify the evacuation. *Id.*

40. *Korematsu*, 323 U.S. at 223.

41. ERIC MULLER, FREE TO DIE FOR THEIR COUNTRY: THE STORY OF JAPANESE AMERICAN DRAFT RESISTERS IN WORLD WAR II 4 (2001).

again be denied their Constitutional rights and may the remembrance of that experience serve to advance the evolution of the human spirit. . . [.]"[42]

C. The Cold War

World War II officially ended on August 12, 1945, bringing an uneasy peace to those ravaged by two global conflicts. Although tentative allies during World War II, the United States quickly found itself at odds with the communist regime of the Soviet Union.[43] With the onset of the Cold War, the sacrifice of civil liberties began anew with overzealous attempts to ferret out domestic support of communism and rid the United States of its potential dangers.[44]

Any student of American history is familiar with the Palmer raids, which resulted in the arrest and deportation of many innocent non-citizens without probable cause. The unrestricted and unauthorized electronic surveillance of anyone that the executive branch perceived to be a threat to national security and the accompanying public "Red Scare" hysteria also characterized this era.[45] Senator Joseph McCarthy's name, even a half-century later, remains synonymous with the period of outrageous, unwarranted accusations and political witch hunts.[46]

Not surprisingly, the judiciary again supported legislative and executive action that intruded on privacy rights. In *Barenblatt v. United States*,[47] the Supreme Court upheld the petitioner's conviction for contempt of Congress for refusing to answer questions regarding his alleged involvement in the Communist Party.[48] This hyper-cautious political and economic environment was fueled in part by the communist takeover of Eastern Europe, China, and

---

42. '*Gulity' of Being Muslim?*, The Daily Star Online Edition (Feb. 20, 2003) (excerpt from an inscription on a plaque hung at the Poston Japanese-American relocation center in Arizona), *at* http://www.dailystar.com/opinion/edits/2003/02/ed0220.html.

43. Michael F. Dowley, *Government Surveillance Powers Under the USA Patriot Act: Is it Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War*, 36 SUFFOLK U. L. REV. 165, 175 (2002).

44. *Id*. at 176.

45. Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179, 186-87 (2002).

46. Dr. Harvey Klehr, *Red Scare Revisited: Was McCarthy Right About Soviet Espionage?*, (CNN Perspective Series on the Cold War, *available at* http://www.cnn.com/SPECIALS/cold.war/episodes/06/then.now/ (last visited Oct. 25, 2003).

47. 360 U.S. 109 (1959).

48. *Id*. at 133-34 (determining that the government's interest in investigating communist activities within the United States outweighed the petitioners interest in not divulging his association with communists).

Korea, as well as Soviet development of nuclear capabilities.[49] It seemed to the American public that they had overthrown one terrible totalitarian dictatorship only to see another arise, this time one armed with nuclear weapons. The perils of communism and the threat of a third world war seemed imminent.

One of the major differences between the Cold War period and the two World Wars was that, unlike the supposed menace posed from within the country by German- and Japanese-Americans, the internal communist threat to the national security of the United States was very real and very significant, perhaps even more so than imagined by the American public at the time.[50] While the FBI, under J. Edgar Hoover's direction, wrongly violated the privacy rights of innocent individuals and the legislature conducted manhunts for communists and those deemed "un-American," a real threat of communist spies and subversives remained active and largely undetected in the United States.[51]

The end of the Cold War and collapse of the Soviet Union allowed evidence to surface that threw shocking light on the extent of the activities of the Communist Party U.S.A. during the 1940's and 1950's.[52] This evidence established that more than 350 Americans secretly worked for Soviet intelligence during World War II, a number of whom served in extremely powerful and important positions within the United States government and only half of whom were ever legitimately identified.[53] Most American communists were not spies and had no realization of the actual clandestine activities organized by their party.[54] Ironically, these Americans, innocent of wrongdoing, were the predominate targets of the anti-communist investigation and denunciation spurred by the paranoia of the Cold War period.[55] The false accusations leveled at innocent Americans by Senator McCarthy and his supporters trivial-

49. Henderson, *supra* note 45, at 187.

50. Klehr, *supra* note 46.

51. *Id*.

52. *Id*. Archives of communist party records and National Security Administration decrypted messages intercepted between communist headquarters in the U.S. and Moscow as well as other information has been released to American scholars. *Id.*

53. *Id*. Among those identified: Julius Rosenberg, who led a spy ring that obtained scientific secrets, most notably information relating to the development of atomic bombs; Alger Hiss, a member of Roosevelt's State Department, who is believed by most scholars to have earned his conviction as a spy; and others in high places in the War Department, Treasury Department, and branches of the military. More than 150 other American officials acting as Soviet spies were unable to be identified due to their use of indecipherable cover names in communications with Moscow. *Id.*

54. *Id*.

55. *Id*.

ized and weakened valid charges.[56] Those who were genuinely guilty of subversive communist activity were able to portray themselves as innocent victims of fanatical McCarthyism due to the great number of obviously erroneous charges.[57] While the threat of Soviet spies and subversive elements was very real during this time, the widespread intrusion on Americans' civil liberties actually undermined the goal of protecting national security rather than furthering it. Again, this example demonstrates that extreme government reaction to a threat to national security was ineffective in defending against that threat, despite the fact that it clearly existed in this case.

These three situations from United States history possess general similarities to each other and to the current public and political climate following September 11. In each of these cases, the government took action, primarily through legislation enacted to empower the executive branch, which struck an inappropriate balance between protection of civil liberties and national security. Widespread public sentiments of anger and fear, whether or not legitimately justifiable, were fostered and created environments where the rights of free speech, privacy, and possession were devalued by the people themselves in their hunger for safety, truth, justice, and often retribution.

Another recurring theme has been the judicial support of such extreme actions taken by the other two branches of this country's government. Rather than tempering the harmful effects on civil liberties from increases in executive power in times of war or threats against domestic security, the judiciary has allowed even the most extreme legislation or executive action to strip away Americans' most fundamental liberties. While the appearance of a strong, unified federal government is important for many reasons, when either the executive or the legislative branch oversteps its authority and intrudes on personal civil liberties in an unconscionable manner, the judiciary has a responsibility to channel those actions back into Constitutionally legitimate territory. Finally, each of these cases demonstrates that such extreme and overly intrusive action by the government is relatively ineffective in uncovering or diffusing threats to domestic security. While the sacrifice of civil liberties during wartime may be necessary, radical infringements on fundamental rights are generally unnecessary and counterproductive.

D. Today's "War on Terrorism"

Before comparing the similarities between these past conflicts and the threat of domestic terrorism that exists today in the United States, there are at least two key differences that are relevant to this discussion. First, the menace of crime and terrorism is not likely to be eradicated in the near future, if at all.[58] The fact that the perils of terrorism are relatively new to the United

56. *Id.*

57. *Id.*

58. John W. Whitehead & Steven H. Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and*

States does not mean, of course, that they are a recent development or a temporary trend of attempts at political persuasion. Throughout history, man has perpetrated heinous crimes against his fellow man, and a constant threat of terrorism is a part of daily life for individuals in many parts of the world. This war that the United States has declared on terrorism is not against an enemy that can be targeted and defeated in a traditional war. There will always be those who feel that violence is the most efficient solution to conflicts and problems, and it is impossible to completely root out and eliminate the threat that such individuals and organizations pose.

Unlike previous wars in which the United States has been involved, "this time, enemies may not reach a truce that would signal the return of civil liberties."[59] Personal freedoms voluntarily relinquished in the past due to the necessities of domestic defense have always been returned to the people at war's end, often times in a form more protected than before.[60] This historical trend is likely one factor behind the American public's general willingness to concede intrusions into even basic civil liberties: there is an implicit expectation that these personal freedoms and rights will be summarily returned when the threat is eliminated or diminished. "In today's world, however, once civil liberties are fenced, they may never be freed, becoming captive to the warden of national security."[61] Because there can be no guarantee that terrorism has been eliminated due to the nature of its perpetrators, a continued desire for safety would likely outweigh the return of these civil liberties.

The second major difference between previous wars and today's "War on Terrorism" lies in the nature of the specific civil liberties that are at stake. In the previous examples, the focus centered on the right to equal treatment, the right of free speech, the right of free association, the right of possession, and several others. While most of these personal freedoms are affected at least indirectly by the current state of the war on terrorism, the most prominent, and the most vulnerable, is the right to privacy. This is especially true in the arena of electronic communications.

Several reasons explain why electronic communication privacy rights have become so crucially important and why these rights are highly susceptible to excessive intrusion by legislation, law enforcement, and criminal activity. The first reason is a corollary of the fact that in today's world, information is power. Information has effectively become as powerful as currency among developed and developing nations. The fastest growing means of information communication is electronically, whether via e-mail or

---

the Justice Department's Anti-Terrorism Initiatives, 51 AM. U. L. REV. 1081, 1085 (2002).

59. *Id.*

60. *Id.*

61. *Id.*

the Internet.[62] The growth in electronic communications and the corresponding rise in the ease and familiarity with which individuals and corporations utilize such tools have resulted in their use to transmit increasingly important and sensitive information. This fact makes electronic communications an even more desirable target for both cyber-criminals and law enforcement agencies. The growing lure of electronic communication as a target for intrusion renders it all the more susceptible to the slightest breakdown in the framework of privacy protection.

A second reason the protection of electronic communications privacy is so important during this period of political, social, and legislative flux is the fact that privacy protection laws, with respect to electronic communications, have consistently lagged far behind technological advancements.[63] In addition, courts have described electronic communications privacy legislation as a "complex, often convoluted, area of the law."[64] While temporarily reducing protection of the more established civil liberties, such as the right to free speech or the right to contract, would not likely cause them irreparable damage, weakening privacy protection for electronic communication would sink the already sagging state of law in this new area into further functional debt.

Finally, even if such beliefs are not entirely well-founded, most e-mail and Internet users have expectations of anonymity and privacy with respect to their online activity at least as strong as those relating to telephone use.[65] Internet users are frequently reminded when they are viewing or transmitting information over an insecure connection and are regularly asked to decide whether to continue anyway.[66] Many Internet users are also familiar with the common use of devices known as "cookies" and their ability to reveal personal preferences to marketing companies by tracking an individual's online activity.[67] A recent survey by AT&T showed that nearly 90% of individuals

62. Robert Zakon, *Hobbes' Internet Timeline*, *at* http://www.zakon.org/robert/internet/timeline (last visited Oct. 25, 2003). At the time of the ECPA's enactment in October 1986, there were approximately 5,000 host computers connected to the Internet. Today there are more than 160 million host computers with Internet access in the U.S. alone. *Id.*

63. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (noting that "the existing statutory framework is ill-suited to address modern forms of communication like [a] secure website").

64. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

65. Maricela Segura, *Is Carnivore Devouring Your Privacy?*, 75 S. CAL L. REV. 231, 253 (2001).

66. Kimberly A. Horn, *Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 FORDHAM URB. L.J. 2233, 2265 (2002). The fact that a user willingly continues his or her online activity, despite such warnings, evidences an "affirmative recognition of the privacy risks associated with online use." *Id.*

67. *Id*. at 2266.

possess serious concerns regarding the privacy of their online activity and information.[68]

Despite these concerns and cautionary road signs along the Internet superhighway, growth in the public's use of the Internet for highly personal online activities such as banking and shopping demonstrates that many users still harbor expectations of privacy.[69] To date, few cases have dealt with this issue. The United States Court of Appeals for the Armed Forces held in one such case that the defendant had a reasonable expectation of privacy in his personal e-mail account.[70] At least one other case has followed this decision.[71] Whether these opinions will be upheld or extended to other online activity will depend on how the courts interpret the new Patriot Act. Because Internet and e-mail users have arguably reasonable expectations of privacy in at least some of their online activities, it is important that these privacy expectations are given sufficient protection. Current privacy law for electronic communications, however, is not nearly as well developed or as protective as that in place for wire communications, such as phone calls.[72]

68. *See* Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT & T Labs Research Technical Report TR 99.4.3 (Apr. 14, 1999), *available at* http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm (last visited Oct. 25, 2003).

69. *See Business Week/Harris Poll: A Growing Threat*, Business Week Online (March 20, 2000), *at* http://www.businessweek.com/2000/00_12/b3673010.htm (last visited Oct. 25, 2003). This is likely due in large part to the fact that most Internet users have either not been victimized by an intrusion into their online privacy or do not realize that their privacy has been violated. *Id.*

70. United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996); *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (setting up the two-pronged test used by the courts today in determining whether government activity constitutes a search and thus implicates Fourth Amendment privacy interests: (1) whether the individual had an actual expectation of privacy; and (2) whether society is prepared to accept the individual's expectation of privacy as reasonable).

71. United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000) (finding that users of a government e-mail system had a reasonable expectation that law enforcement officers would not intercept their messages even though there was specific notice that the system administrator was monitoring the e-mail).

72. Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 LAW LIBR. J. 601, 606 (2002) (outlining the differences in statutory treatment of e-mail and voicemail privacy protection). Not only is legislative protection against the interception or acquisition electronic communication less encompassing than that for wire communication, the courts' interpretations of those statutes are also much more clear and protective with regard to wire communications. Due to the various stages involved in the transfer of electronic communication, courts have been indecisive about which laws apply during the different steps of the transfer process. *Id.*

For each of the above reasons—the growth in the importance and use of electronic communication in this information-dependent era, technology's drastic outpacing of privacy law with respect to electronic communication, and Internet users' expectations of privacy—the arena of electronic communication will be the battleground for the seemingly irreconcilable conflict between privacy and national security protection in this new chapter of our nation's history. Before a proper comparison can be made between past infringements on civil liberties during times of war and the effect that the government's reaction to the recent threats of terrorism will have on electronic communication privacy rights, it is necessary to examine the legal basis for such rights. Part III will briefly discuss the framework of legislative and judicial treatment of electronic communications privacy law leading up to the recent passage of the Patriot Act.

III. Development of Electronic Communication Privacy Law Prior to the Enactment of the Patriot Act

A. Constitutional Protection

In retracing the trail of authority for any fundamental civil liberty in this country, one must necessarily arrive at the United States Constitution and its various Amendments. Although the right to privacy is not explicitly granted in the Constitution, the Supreme Court has held that such a right is fundamental and, thus, subject to strict scrutiny.[73] While the Court has had some difficulty in agreeing on the precise Constitutional source of that right, the accepted theory is that the right to privacy is implicitly protected under the due process clauses of the Ninth and Fourteenth Amendments.[74] In addition to this implicit right of privacy, the Fourth Amendment expressly safeguards the rights of individuals from government intrusion:

> The right of the people to be secure in their persons, houses, papers, effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.[75]

While the language of this Amendment seems both clear and simple, the Supreme Court's interpretation of it has been forced to evolve through the years to keep up with technological advances in crime fighting.[76]

The telephone wiretap was the first major technological advancement in crime fighting that raised serious privacy rights concerns. In *Olmstead v.*

73. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

74. Roe v. Wade, 410 U.S. 113, 153 (1973).

75. U.S. Const. amend. IV.

76. Horn, *supra* note 66, at 2238.

United States,[77] the Supreme Court held that wiretapping telephones without a warrant did not violate the Fourth Amendment because it only protected tangible property.[78] Because wiretapping did not amount to a search or seizure of tangible property or require law enforcement to trespass on the defendants' homes, the Court held that there was no violation of the Fourth Amendment.[79] The court concluded its analysis in *Olmstead* by inviting the legislature to clarify search and seizure law to prohibit wiretapping, which Congress attempted to do in enacting section 605 of the Communications Act of 1934.[80]

In *Katz v. United States*,[81] the Supreme Court reversed its holding in *Olmstead*, stating that a warrant based on probable cause must be obtained before conducting an authorized wiretap.[82] The Court rejected the trespass requirement from *Olmstead*, substituting it with the two-pronged test in Justice Harlan's concurrence.[83] Now, Fourth Amendment privacy interests are implicated whenever the government infringes upon an activity where there is both a subjective and an objective expectation of privacy.

B. Title III of the Omnibus Crime Control and Safe Streets Act of 1968

In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act[84] to clarify and codify the results of the preceding case law concerning the availability of wiretaps to law enforcement. Title III, or the "Wiretap Act" as it became known, is especially relevant to this discussion because it was later amended to include electronic communication.[85] Title III was hotly debated in Congress, where many legislators were concerned with the amount of authority that it conferred upon law enforcement and the threat that it posed to individual's privacy rights.[86]

77. 277 U.S. 438 (1928).

78. *Id*. at 464.

79. *Id*. at 466.

80. Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064 (codified as amended at 47 U.S.C. §§ 151-714 (2000)). However, through various technicalities and loopholes in § 605, federal law enforcement was able to circumvent this restriction on their ability to wiretap. *Id.*

81. 389 U.S. 347 (1967).

82. *Id*. at 353.

83. *Id*. at 359. *See also Katz*, 389 U.S. at 361 (describing Justice Harlan's two-pronged test).

84. Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 *et seq*. (2000) (codified as amended).

85. *See infra* Part II.D. of this Note.

86. Horn, *supra* note 66, at 2243. One senator dryly referred to Title III as the "End to Privacy Act." *Id.*

The Wiretap Act made it an offense to intercept aural or wire communications without a specially approved court order. To obtain such an order, a senior Justice Department official must first approve the application.[87] The application must then be presented to a judge, who must make four findings before approving the order: (1) that there is probable cause that at least one of a series of enumerated offenses is being or will be committed; (2) that there is probable cause that particular communications concerning that offense will be obtained through such interception; (3) that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and (4) that there is probable cause that the facilities where the interceptions are to take place are or will be used in connection with the commission of the offense.[88]

In addition to this high standard for approval, there are several other statutory safeguards to protect against the misuse of wiretaps. First, the issuing judge may require reports to be made to him at regular intervals "showing what progress has been made toward achievement of the authorized objective and the need for continued interception."[89] Also, once the interception has been completed, the law enforcement officers must inform the individual subject to the wiretap order of the surveillance.[90] Finally, any evidence obtained from an unauthorized or non-compliant interception may be suppressed as inadmissible.[91] As written, this piece of legislation allows law enforcement to monitor the communications of suspected criminals while remaining subject, at least in theory, to strong judicial supervision.

C. Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act of 1986 (hereinafter "ECPA") was enacted "to update and clarify Federal privacy protections and standards" in light of the rapid technological advances in the second half of the twentieth century.[92] Title I of the ECPA amended the Wiretap Act in an attempt to reconcile it with modern technology.[93] This section also governs the interception of communications during their period of transmission.[94] Ti-

87. *See* 18 U.S.C. § 2516(1) (2000). Such an application may be approved by the Attorney General or any Deputy, Assistant, or Associate Attorney General. *Id.*

88. *See* 18 U.S.C. § 2518(3) (2000).

89. *Id.* § 2518(6).

90. *Id.* § 2518(8)(d). The individual subject to the wiretap must be given notice of the wiretap, the period of time that it was in place, and whether or not any communications were actually intercepted. *Id.*

91. *Id.* § 2518(10)(a).

92. S. REP. NO. 99-541, at 1 (1986).

93. Note that although Title I of the ECPA amended the Wiretap Act, it is still referred to as "Title III" (of the Omnibus Crime Control and Safe Streets Act).

94. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002).

tle II of the ECPA created the Stored Communications Act to give a broader range of privacy protection to the contents of communications while in storage, before and after their transfer.[95] Title III of the ECPA applied express standards to surveillance techniques that acquire non-content related information from communications. This Act has become the foundation of communications privacy law, and each part will now be discussed in greater detail.

1. The New Wiretap Act

The Wiretap Act remained virtually unchanged for nearly two decades before Congress addressed its ineffective protection of communications due to the rapid developments in technology. Many new forms of communication were introduced, such as cellular phones, pagers, and e-mail, which did not fall within the purview of the Wiretap Act.[96] Congress extended the same protections of the Wiretap Act to these forms of "electronic communication" with Title I of the ECPA.[97]

Although law enforcement agencies must follow the same basic procedures for intercepting the contents of e-mail as for telephone conversations, there are several subtle differences between the treatment of wire communications and electronic communications that afford significantly less protection for the latter.[98] First, any government attorney can authorize an application for a Title III order to intercept electronic communication, while the interception of a wire communication requires the approval of a senior justice department official.[99] Second, the interception of an electronic communication must only be related to the commission of *any* federal felony, rather than the narrower scope of enumerated offenses that must be the subject of a wire communication interception.[100] Finally, the mandatory suppression at trial of communications intercepted either improperly or without a Title III order only applies to wire communications, not electronic.[101] Unlawfully intercepted electronic communications may still be admissible as evidence in court.[102] These are substantial discrepancies that demonstrate that the Wiretap Act still lagged behind technology and provided insufficient privacy protection to electronic communications even after the ECPA amended it. Unfortunately, the latest amendment of the Wiretap Act by the

95. *Id*. at 878-79.

96. Segura, *supra* note 65, at 244 (citing H.R. REP. NO. 99-647, at 18 (1986)).

97. S. REP. NO. 99-541, at 2 (1986).

98. Horn, *supra* note 66, at 2251.

99. *Id*. (citing 18 U.S.C. § 2518(1) (2000)).

100. *Id*. (citing 18 U.S.C. § 2516). Section 2516 gives the list of offenses of which there must be probable cause of at least one. *Id.*

101. *Id*. (citing 18 U.S.C. §§ 2515, 2518(10)(a)).

102. *Id*.

Patriot Act did nothing to correct these discrepancies, but rather built on them, thereby magnifying the problem of insufficient statutory protection.

2. The Stored Communications Act

In addition to regulating the interception of electronic communications, the ECPA also created what is known as the Stored Communications Act.[103] As its name suggests, this Act added privacy protection for wire and electronic communications while they are in electronic storage. To "access" private communications while they are in storage, law enforcement officers must obtain what is known as a section 2703(d) court order or a warrant issued pursuant to the Federal Rules of Criminal Procedure, depending on the amount of time that the communication has been in storage.[104] If an email or other electronic communication has been in storage for 180 days or less, then a traditional criminal search warrant must be obtained.[105] This requires establishing to a judge that probable cause exists that the communications sought will produce evidence of the commission of a crime.[106] No prior notice to the recipient of the communication is required. If the electronic communication has been in storage for more than 180 days, it is afforded less protection. A law enforcement agency must only acquire a section 2703(d) order in such a situation.[107] This merely requires certifying to the judge that the contents of the communication are relevant and material to an ongoing criminal investigation.[108] If section 2703(d) is read closely, it is apparent that the judge does not even have the authority to reject such an application.[109] In addition, under a section 2703(d) order, notice to the recipient of the communication may be delayed for up to 90 days if the law enforcement agency can establish to the court that such notice would jeopardize the investigation or produce adverse consequences.[110]

103. 18 U.S.C. §§ 2701-2711 (2000).

104. *Id.* § 2703(a).

105. *Id.*; *see also* FED. R. CRIM. P. 41 (proscribing the requirements for a criminal search warrant, including the establishment of probable cause).

106. 18 U.S.C. § 2703(a) (2000).

107. *Id.* § 2703(b). This standard is much lower than that of probable cause. Communications in storage for longer than 180 days may also be acquired by a traditional warrant (discussed above) or with an administrative or grand jury subpoena (which requires no probable cause or judicial approval, but does require advance notice). *Id.*

108. *Id.* § 2703(d) (2000).

109. Section 2703(d) states in part that as long as there are "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication are relevant and material to an ongoing criminal investigation," the court *shall* issue the order. *Id.*

110. *Id.* § 2705(a)(1)(A).

Not only are the standards for obtaining stored electronic communications much less stringent than those for intercepting electronic communications during transfer with a Title III warrant, but there is also no reporting requirement in the Stored Communications Act. The judicial supervision that is so important to the Wiretap Act is not present when stored communications are accessed. There is also no requirement equivalent to the provision in the Wiretap Act that law enforcement agencies minimize the acquisition of irrelevant data or exhaust all other avenues of investigation first.[111]

Despite the weaker protections of the Stored Communications Act, one would assume that they combine with those of the Wiretap Act to provide a broader range of privacy protection for electronic communication than existed before the ECPA's enactment. The lack of clarity in the language of the ECPA and the fact that it was outdated by technology almost from its inception, however, has given courts difficulty with its interpretation. More specifically, the courts have had great trouble in determining the boundaries between the Wiretap Act and the Stored Communications Act.[112] When it comes to communications such as secure websites and private e-mails, courts have struggled to determine when to apply one Act or the other or whether to apply either at all. For example, a website is stored on a host computer, but anytime it is accessed by an outside viewer, that information must be transferred. If the website is private and secure and the outside viewer accesses that site without authorization—by hacking into it or other illicit means—which Act applies?[113] Also, when e-mail is sent, storage is incidental to its transfer. When, if at all, during the transfer process does each Act apply? The ECPA is unclear on these issues and others and, as a result, its interpretation by the courts has drastically reduced the privacy protections originally intended by the drafters of the ECPA.

The majority approach has been to narrowly construe the term "intercept" used in the Wiretap Act to require acquisition that is contemporaneous with the actual transfer of the electronic communication.[114] Thus, the greater protection of the Wiretap Act has generally applied only to communications

111. Segura, *supra* note 65, at 246.

112. Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 625, 633 (E.D. Pa. 2001). "Courts and scholars have struggled to determine the precise boundaries of and also the intended relationship between [these two acts]." *Id.*

113. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002). The issue is whether the website constitutes a stored electronic communication or whether the communication of the website from the host computer to the visiting computer constitutes an electronic transfer within the scope of the Wiretap Act. *Id.* Courts have held that in such a situation, the website constitutes stored electronic communication and thus does not fall under the greater protection of the Wiretap Act. *Id.*

114. *See generally id.*; *see also* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

acquired en route in the transfer process, while communications located in any type of electronic storage are only afforded the lesser protection of the Stored Communications Act. Taking into account the functional aspects of e-mail and the transfer of information over the Internet, this narrow interpretation virtually eliminates the possibility that the Wiretap Act will ever be applied in the context of electronic communication. Typically, information sent over the Internet is transferred nearly instantaneously in small pieces, called "packets."[115] These packets generally take different routes to their final destination, where they are then reassembled in correct order.[116] As can be surmised from this description, unless an individual has direct access to the sending or receiving computer or their servers, it is nearly impossible to "intercept" such an electronic communication within the meaning courts have conferred upon the Wiretap Act. The period of transfer is instantaneous and unless each packet is intercepted, the communication would be meaningless. The privacy protection of the Wiretap Act becomes moot with respect to electronic communication if no such interception is possible.[117]

An additional consideration is that storage of electronic communication is often incidental to its transfer. Between the instant that a key or button is pushed that sends the communication and when that communication is actually received, it is often stored temporarily or permanently in the sending computer, the receiving computer, and various host computers along the way.[118] The majority interpretation of the intersection of the Wiretap Act and the Stored Communication Act makes a distinction between these arbitrary stages of transfer.[119] Ironically, electronic communications are most vulnerable when they are in a state of storage, yet that is where they receive the least protection during the transfer process.

The reason these practical issues exist lies in the fact that Congress simply hung the provisions regarding these new forms of electronic communication on the old framework of privacy protection for wire communication. While the distinction between transfer and storage is fairly clear and straightforward in a situation involving communication via telephone, the line becomes blurred when the same standard is applied to the complexities of

115. Victoria A. Cundiff, *Protecting Trade Secrets from Disclosure on the Internet Requires Diligent Practice*, 74 N.Y. ST. B.J. 8, 10 (2002).

116. *Id.*

117. Tools or utilities with such capabilities do exist, however, and are generally known as "packet sniffers." The FBI's infamous "Carnivore" program is such a tool, but even it must be attached directly to the target's ISP hardware. This program is also a fairly recent development and clearly not within the scope of the legislature's consideration in 1985, when enacting the ECPA. *See infra*, note 130.

118. *Konop*, 302 F.3d at 879, n6. The various computers through which an electronic communication travels are known as routing computers or "routers." *Id.*

119. *Id.*

electronic communication. The distinct and greater protections of the Wiretap Act make much more sense in the context of a phone conversation that is intercepted by law enforcement. Directly analogizing between wire and electronic communications and applying the same statutory regulations to law enforcement's surveillance of either type is facially irreconcilable.

3. Pen Registers & Trap and Trace Devices

Before moving away from the topic of the ECPA, a short discussion of another form of law enforcement surveillance covered by the ECPA is pertinent at this point. The preceding paragraphs have described the ECPA's attempts to protect the *content* of electronic communications from unauthorized acquisition, whether those communications are in storage or in transit. For quite some time, law enforcement has had another tool at its disposal, one that acquires information about a communication, such as its source and recipient, without acquiring its contents. These tools are known as pen registers and trap and trace devices and the information that they acquire is called "addressing information." In the context of wire communications, a pen register device is able to record outgoing telephone numbers dialed from a particular phone.[120] A trap and trace device records the phone numbers of all incoming calls.[121] Together these two tools are known as pen register searches. In *Smith v. Maryland*,[122] the Supreme Court held that the installation of pen registers does not violate Fourth Amendment privacy rights, and thus law enforcement officers do not need a warrant because pen registers do not constitute a search.[123] The Court reasoned that individuals do not have a reasonable expectation of privacy concerning the phone numbers that they dial since the number must necessarily be made known to the phone company in order to place the call.[124] Such devices do not constitute interceptions because at no time is the content of the communication ever revealed.[125]

Despite the holding in *Smith v. Maryland*, setting a pen register search in place is not automatic; Title III of the ECPA lays out the procedure that must be followed to implement such a device.[126] The standards are very

120. *CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections*, Center for Democracy & Technology (April 4, 2000), *available at* http://www.cdt.org/security/000404amending.shtml (last visited Oct. 25, 2003).

121. *Id.*

122. 442 U.S. 735 (1979).

123. *Id.* at 745-46.

124. *Id.* at 742.

125. United States v. N.Y. Tel., 434 U.S. 159, 167 (1977).

126. 18 U.S.C. § 3123 (2000).

similar to the requirements for obtaining electronic communications that have been in storage for more than 180 days, basically a rubber stamp.[127] The information sought by the pen register must only be relevant to an ongoing investigation.[128] Also, an affidavit stating the identity of the party being investigated, the identity of the party whose phone line is being monitored, and the probable offense to which the information likely relates must be submitted with the order application.[129]

These standards, despite being very minimal, seem appropriate for a relatively non-intrusive form of surveillance. Most individuals understand that the numbers that they dial are not private information, especially when making long distance or collect calls. This area of the ECPA, however, fails in the same way the rest of the Act does: it is obsolete with respect to the various types of electronic communication. Before the Patriot Act amended it in late 2001, the ECPA did not even address the applicability of these pen register standards to electronic communication. This amendment came much too late, more than two years after the FBI developed and utilized technology that was capable of acquiring addressing information from e-mails sent to and from specific computers in a manner comparable to pen register searches.[130] In addition, the amendment basically applied the old standards governing wire communication to electronic communications, expressly providing what courts had been hesitant to do—apply old legislation to a very different form of communication by analogy.[131] The Patriot Act and its effects will be discussed later in greater detail, but suffice it to say that legislators and the courts have attempted again to fit an old statutory framework intended for wire communication to the field of electronic communication and it again fails to provide satisfactory privacy protection in an age of modern technology.

---

127. *CDT's Analysis of S. 2092*, *supra* note 120.

128. 18 U.S.C. § 3123(a)(2) (2000).

129. *Id.* § 3123(b).

130. Peter J. Georgiton, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831, 1834-35 (2001). In 1999, it became known that the FBI had developed DCS1000, infamously known as "Carnivore," which was capable of monitoring e-mails sent or received by a particular computer. This program is attached to the suspect's Internet service provider's facility, where it is able to filter through the data packets as they are transmitted from and received by the suspect's computer. Carnivore is able to operate either as a "pen register" (only acquiring addressing information) or as a Title III interceptor (acquiring the contents of the e-mail as well as the addressing information). *Id.*

131. *See* United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999).

D. Federal Intelligence Surveillance Act (FISA)

Another separate branch of federal legislation substantially impacting Americans' communication privacy rights is the Federal Intelligence Surveillance Act of 1978.[132] FISA is a distinct body of law because it applies specifically to intelligence gathering conducted for purposes of national security.[133] The statutory and common law discussed up to this point provides privacy protection in the context of criminal investigations by federal law enforcement agencies. Because this Note analyzes the U.S. reaction to recent surges in both Internet crime and terrorism, and because FISA now has the potential to affect the average citizen, both branches of the law must be discussed.

Several factors motivated Congress to enact FISA. The first was the Supreme Court's holding in *United States v. United States District Court*, referred to as "*Keith*."[134] In *Keith*, the Court held that the reason for the interception of the communication is irrelevant; the Fourth Amendment prohibits warrantless searches or seizures, even in the interests of protecting domestic safety from threats to national security.[135] Writing for the majority, Justice Powell invited Congress to provide different regulations for the surveillance of those suspected to be a threat to national security if the standards of Title III were inappropriate for such situations.[136]

Another motivating factor was the increasing public awareness of the extent to which Americans were subject to the executive branch's abuse of its surveillance powers. The Watergate scandal, involving then President Richard Nixon's aides' burglarizing and wiretapping of the Democratic National Committee headquarters, occurred at the same time *Keith* was decided. This scandal "caused many people to question the authority claimed by the executive branch."[137] The FBI's unauthorized surveillance during the 1960's of prominent civil rights leaders, including Martin Luther King, came to light just prior to this same period.[138] Also, the NSA intercepted most of the international telegrams leaving the United States between 1945 and 1975 in a secret program codenamed "Shamrock."[139] The public became aware of Shamrock when a Senate Committee publicized its investigative report on

132. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified in part as amended at 50 U.S.C. §§ 1801-11 (2000)).

133. Henderson, *supra* note 45, at 185.

134. 407 U.S. 297 (1972). The case received its nickname from Judge Damon J. Keith, who was the federal district judge that originally heard the case. *Id.*

135. *Id*. at 320-21.

136. *Id*. at 322-23.

137. Henderson, *supra* note 45, at 189.

138. *Id*. at 223, n.70.

139. Eric M. Freedman, *Freedom of Information and the First Amendment in a Bureaucratic Age*, 49 BROOK. L. REV. 835, 841 n.16 (1983).

the program.[140] Lastly, when the Wiretap Act was passed in 1968, law enforcement was required to record and report its wiretapping activities. The reports revealed that an enormous number of conversations were being intercepted with shockingly small results in terms of crime prevention.[141] These events and others led to public outcry against unregulated surveillance by the executive branch in the name of national security.[142] Congress realized the need to strike a balance between the executive branch's ability to safeguard national security and the American public's right to privacy.[143]

In FISA's most significant provision, Congress established a special court specifically to review applications for domestic national security surveillance activities.[144] Before being amended by the Patriot Act, FISA established several seemingly strict requirements that an application was required to meet for approval. First, the Attorney General had to approve the application before it could be submitted to the FISA court.[145] Second, the application itself was required to (1) establish probable cause that the target of the surveillance was either a foreign power or the agent of a foreign power,[146] (2) establish probable cause that the facilities under surveillance were being used or would be used by a foreign power or the agent of a foreign power,[147] (3)

140. *Id.*

141. Ira Glasser, *The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 NOVA L. REV. 625, 642-43 (1999). "In the first four years after the 1968 bill was passed, 1.1 million conversations were overheard, 93,080 people were spied upon, 6,131 people were arrested and a total of 1,154 people were reported convicted—barely more than one percent." *Id.*

142. Henderson, *supra* note 45, at 188.

143. S. REP. NO. 95-604, pt. 1, at 9 (1978).

144. 50 U.S.C. § 1803(a) (2000).

145. *Id.* § 1804(a).

146. *Id.* § 1804(a)(4)(A). Section 1801(a) defines a "*foreign power*" as a foreign government, whether or not recognized by the United States, a faction of a foreign nation or nations, an entity that is openly acknowledged by a foreign government to be directed and controlled by such foreign government, a group engaged in international terrorism or activities in preparation therefore, or a foreign-based political organization. *Id.* Section 1801(b) defines an "*agent of a foreign power*" as any person other than a United States person who acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power, or who engages or seems likely to engage in clandestine intelligence activities in the United States contrary to the interests of the United States. *Id.* Section 1801(c) defines "*international terrorism*" as activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States and that appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. *Id.*

147. *Id.* § 1804(a)(4)(B).

certify that the information sought was foreign intelligence information,[148] (4) certify that the purpose of the surveillance being conducted was to obtain such information,[149] and (5) certify that the information could not be obtained by other less intrusive techniques.[150] FISA also contained a minimization requirement.[151] Because this legislation was a significant departure from surveillance law for purposes of traditional law enforcement, FISA also imposed limits on the use of information obtained under its authority. Information discovered under FISA surveillance could only be used in a criminal proceeding if the government could establish that foreign intelligence gathering had been the "primary purpose" of that surveillance and if reasonable notice was given to the defendant of the surveillance.[152] Before 1998, FISA contained no provision for the use of pen registers or trap and trace devices in this type of investigation.[153] Since 1998, the required standard for judicial approval of a FISA pen register has been that the communications to be monitored must be used in activities that involve or might involve a violation of criminal laws.[154]

While these standards seem fairly rigorous, there are three considerations that imply otherwise. First, while these requirements seem restrictive on their face, they are not so in fact. Surprisingly, "in the more than twenty years that have passed since FISA was enacted, only two applications have been rejected."[155] Second, these requirements are completely ineffective if law enforcement agencies engage in clandestine and abusive surveillance without reporting to the FISA court. The track record of the FBI and other law enforcement and security agencies has been shockingly poor in this regard, which was one reason for FISA's enactment in the first place. Finally, the requirements listed in the previous paragraph are those that existed prior to amendment by the Patriot Act. The new requirements, which will be discussed shortly, are significantly less protective, and this amendment has dramatic effects for even ordinary citizens who would not consider themselves a threat to domestic security.

148. *Id.* § 1804(a)(7)(A). If the individual under surveillance is a United States person, the information to be obtained must be "necessary" for the protection of national security. If the targeted individual is not a United States person, the information must only be relevant to national security to constitute "foreign intelligence information." *Id.*

149. *Id.* § 1804(a)(7)(B).

150. *Id.* § 1804(a)(7)(C).

151. *Id.* § 1804(a)(5).

152. Henderson, *supra* note 45, at 192 (citing § 1806(c)).

153. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404 (1998) (codified at 50 U.S.C. § 1842 (2000)).

154. *Id.*

155. Henderson, *supra* note 45, at 193.

This brief analysis of the various federal sources of communications privacy protection demonstrates that the legislative and judicial framework was clearly insufficient with respect to electronic communications even prior to the enactment of the Patriot Act. This was due in large part to the fact that Congress simply applied existing legislation for wire communications directly to electronic communications. An extensive analysis is not necessary to arrive at the conclusion that these two forms of communication are significantly different on many levels. It seems clear that a direct translation of privacy protection law, from the relatively simple situation involving a phone conversation to the much more complex situation where secure information is transmitted over the Internet through various computers, would necessarily fall short in many respects. The privacy protections afforded to electronic communication were not strong enough in the first place to support the weakening effects of the Patriot Act.[156] In addition, the lack of clarity in the ECPA, which is the foundation of communications privacy protection, has severely restricted the judiciary from interpreting the law in a manner that would insure the Constitutional safeguards of the Fourth Amendment in the area of electronic communication. The courts have found that individuals have a legitimate expectation of privacy with respect to at least some of their online communications.[157] This expectation could be lost, however, if the current trend of decreasing privacy protection for electronic communications continues further. If there can be no objective expectation of privacy in electronic communications due to express contravention by law, then the second half of the two-prong test laid out in *Katz* can never be satisfied.[158] No reasonable explanation exists for declining to extend the same protections that guard the privacy of a personal phone conversation between two individuals to a private e-mail between the same two individuals. Part IV next discusses how the Patriot Act further exacerbates the problem of weakening privacy protection for electronic communications.

IV. The USA Patriot Act: The U.S. Reaction to Terrorism

The Patriot Act brought about significant changes to each of the statutory schemes discussed in Part III. While the stated purpose of the Act was to aid law enforcement in proactively combating the threats of violent crime and terrorism, its enactment alarmed privacy rights activists already concerned about the state of privacy law. Although the Act affected many areas of personal privacy, this Note will only focus on those related to electronic communication.

156. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002). (holding that "Congress chose to afford stored electronic communications less protection than other forms of communication.").

157. *See supra* notes 70-71 and accompanying text.

158. Katz v. United States, 389 U.S. 347, 361 (1969) (Harlan, J. concurring).

Many of the provisions of the Patriot Act were originally proposed in the Anti-Terrorism Act of 2001 and in other previous bills unrelated to terrorism, but were rejected by a Congress concerned with civil liberties and granting the executive branch overly broad investigative powers.[159] The tragedies of September 11, 2001 provided the impetus to overcome these concerns, and on October 26, 2001, these provisions passed by an overwhelming margin[160] in the form of the Patriot Act.[161] The fact that it took something so severe to allow some of the provisions of this Act to be passed raises significant apprehension concerning its effect on civil liberties. The massive scope of this legislation and its broad impact on existing law triggers additional concerns; the fact that this legislation was passed in merely six weeks only amplifies them.[162] While prompt action was necessary to respond to the legitimate threat of further terrorist attacks, there was insufficient time in which to hear expert testimony, to debate the various provisions, or even to comply with normal procedures for the passage of legislation.[163] These issues in the passage of the Patriot Act explain—but do not justify—the inconsistencies and problems within the provisions of the Act pertaining to the surveillance of electronic communication.

The Patriot Act made significant changes to the laws in place that govern the manner in which law enforcement conducts surveillance. As Part III pointed out, these laws already suffered from ambiguity and inadequacy and greatly required updating with respect to modern electronic communication. Instead of updating or clarifying the existing communications privacy protection laws, however, the Patriot Act simply weakened their provisions, making it easier for law enforcement to conduct surveillance, without strengthening the statutory authority granting such powers. Because the confusion surrounding the interpretation of the ECPA and related statutory

159. Michael T. McCarthy, *Recent Development: USA PATRIOT Act*, 39 HARV. J. ON LEGIS. 435, 437 (2002).

160. *Id*. at 435 n.4. The House vote was 357-66 and the Senate vote was 98-1, with only Senator Russell Feingold (D-Wis.) voting against the Act. *Id.*

161. *Id*. at 435. One author noted that the full name of the Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, is somewhat misleading because many of its provisions have nothing to do with protecting against terrorism. Pikowsky, *supra* note 72, at 608-09.

162. *See EFF Analysis of the Provisions of the USA PATRIOT Act that Relate to Online Activities*, Electronic Frontier Foundation, ¶ 1 (Oct. 31, 2001), *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html. The bill, which had more than four different names and versions in the 6 weeks before its passage, is 342 pages long and make changes to over 15 different statutes. *Id*. at ¶ 2.

163. *Id*. The threat of anthrax contamination, which disrupted Congressional operations and forced evacuations, further hindered effective review and consideration of the legislation. *Id.*

schemes already rendered these laws inadequate with respect to protecting the privacy of electronic communication, there was little or no room to eliminate any privacy safeguards. While there is a persuasive argument for increasing law enforcement's ability to discover and track down perpetrators of terrorism before there is a repeat of the horrors of September 11, this goal could have been achieved within the context of the more important long-term objective of reinforcing the statutory framework guaranteeing privacy protection. In addition, many of the provisions of the Patriot Act do not necessarily even relate to terrorism or significantly improve law enforcement's capability to fight it. The following sections will discuss how the Patriot Act made major changes to each of the statutory schemes described above that unnecessarily weaken the existing framework of electronic communications privacy protection.

A. Effects on Acquiring Communication Content Under the Wiretap and Stored Communications Acts

In one of the Patriot Act's more controversial sections, Congress statutorily affirmed the use of "sneak and peek" warrants, which provide for searches and seizures without providing notice to the subject under surveillance beforehand.[164] As mentioned above in the description of the Stored Communications Act, law enforcement already had limited authority to delay notification for searches of stored electronic communications in the possession of a third party if it could show that notification would result in certain negative consequences.[165] The enactment of section 213 of the Patriot Act took this very limited authority and expressly expanded its scope to a degree that directly conflicts with the protections of the Fourth Amendment against unreasonable searches and seizures. Section 213 provides that, in any criminal investigation, notice may be delayed for "a reasonable period" in the seizure of any communication or tangible property if "the court finds reasonable cause to believe that providing immediate notification of the execution

164. Patriot Act, Pub. L. No. 107-56, § 213, 115 Stat. 272 (2001). Neither federal statutory law nor Rule 41 of the Federal Rules of Criminal Procedure (which governs federal search warrants) expressly authorized sneak and peek search warrants before the enactment of Section 213 of the Patriot Act. McCarthy, *supra* note 159, at 451.

165. *See supra* note 110 and accompanying text; *see also* 18 U.S.C. § 2703 (2000). Even before the ECPA, however, "the FBI and the DEA . . .embarked upon a widespread series of [court-authorized] covert entries in a variety of criminal investigations, and by the end of 1984 had persuaded federal judges and federal magistrates to issue at least 35 sneak and peek warrants." The courts were persuaded to grant these warrants even though Rule 41 of the Federal Rules of Criminal Procedure expressly requires advance notice. Note, *Covert Searches*, 39 STAN. L. REV. 545, 546-47 (1987).

of the warrant may have an adverse result."[166] This delay of notification period may also be extended "for good cause shown."[167]

Although the practicality of such a provision must be acknowledged in the context of criminal or terrorism investigations, section 213 raises many different privacy concerns. First, this provision is not restricted to those suspected of planning or perpetrating terrorism. This would seem to imply that the tragedy of September 11, 2001, was used as an opportunity to pass overly broad legislation that normally would not have been approved. If preventing terrorism were truly the focus of this section, it would have been phrased accordingly in a narrower fashion. Second, this section provides for inadequate supervision of law enforcement agencies exercising searches under "sneak and peek" warrants. Who or what entity would hold law enforcement accountable to carry out such searches appropriately? While judicial endorsement is initially necessary to obtain such a warrant, unless the delay of notification is extended, there is no further judicial oversight or evaluation. The potential for abuse by law enforcement is virtually unbounded, since the individual subject to the search would not be aware of it for purposes of supervision.[168] For example, if the FBI intercepted or otherwise acquired a suspect's e-mail, but found no evidence of criminal activity, it seems unlikely that they would admit that they subjected an innocent person to a covert search. The individual would likely never find out about it. Proper surveillance would be better guaranteed if section 213 required law enforcement agencies employing "sneak and peek" warrants to report to the issuing judge at the end of the investigation. Third, the standard that must be met for delaying notice is extremely low: virtually a rubber stamp.[169] Indeed, as mentioned above, courts were persuaded to grant such search warrants even before they were technically legal. Because obtaining a "sneak and peek" warrant is now so easy, there is strong potential that such searches or seizures would become the norm rather than the exception. These concerns might seem somewhat attenuated or unfounded, but if they are considered in light of known past abuses of power by law enforcement and the executive branch,

166. Patriot Act, Pub. L. No. 107-56, § 213.

167. *Id.*

168. Gail Armist, Note, *Freitas After Villegas: Are "Sneak and Peek" Search Warrants Clandestine Fishing Expeditions?*, 26 SAN DIEGO L. REV. 933, 946 (1989).

169. *How the USA Patriot Act Expands Law Enforcement "Sneak and Peek" Warrants*, American Civil Liberties Union, *available at* http://www.aclu.org/Redirect.cfm?pg=%2Fcongress%2Fl102301b%2Ehtml (last visited Oct. 25, 2003). Forcing law enforcement agencies to demonstrate the likelihood of an "adverse result" from timely notification in a surveillance operation does not appear at all restrictive for such an invasive procedure. Also, the term "reasonable period" is extremely vague, creating potential for abuse. *Id.*

they take on greater significance.[170] Finally, unlike most of the more controversial provisions of the Patriot Act, section 213 will not sunset at the end of 2005; it is permanent law.

Undoubtedly, section 213 will be challenged on Fourth Amendment grounds, but based on relatively recent case law, it is unlikely that the courts will find that it is unconstitutional. In *Dalia v. United States*, the Supreme Court held that the Fourth Amendment does not *per se* bar court-authorized covert entries.[171] The Second Circuit followed this holding in *United States v. Villegas*.[172] Courts have also upheld the admissibility of evidence obtained in covert searches in criminal trials.[173] Such cases do not imply that the courts will act to temper the authority that has been granted to the executive branch and prevent abuse of this new power. Instead, these cases seem to suggest that this is yet another situation where the authority of the executive branch will remain relatively unchecked until some type of abuse is discovered and made public.

B. Effects on Acquiring Pen Register Orders Under the ECPA

Another one of the larger changes brought about by the Patriot Act is that pen registers and trap & trace orders may now be applied to electronic communications, as well as wire communications. The courts have struggled with this issue, which is essentially whether it is appropriate to apply the same standards to the acquisition of electronic addressing information as are applied to the acquisition of incoming and outgoing telephone numbers. The Patriot Act answered this question unilaterally in the affirmative.[174] Such a decision, however, raises several privacy concerns. First, electronic communication addressing information, which includes any communication information not containing substantive content,[175] is not directly analogous to phone numbers used in wire communications. Incoming and outgoing phone numbers, which are obtained with pen registers and trap and trace devices, give no information other than the names and locations of those in contact with the individual under surveillance. Addressing information in the context of electronic communication, however, may give rise to other information of a much more personal nature. For example, when an individual runs

170. *See supra* notes 137-43 and accompanying text.

171. 441 U.S. 238, 248 (1979).

172. 899 F.2d 1324, 1336 (2d Cir. 1990) (holding that sneak and peek warrants do not violate the 4th Amendment or Rule 41 of the Federal Rules of Criminal Procedure).

173. *See e.g.*, United States v. Pangburn, 983 F.2d 449, 455 (2d Cir. 1993) (holding that a "sneak and peek" warrant's violation of the notice requirement of Rule 41 did not require suppression).

174. Patriot Act, Pub. L. No. 107-56, § 216, 115 Stat 272 (2001).

175. *Id.* Addressing information includes web (http), IP, and e-mail addresses, but would not include, for example, the subject line of e-mail. *Id.*

an Internet search, the terms used in the search are displayed in the web address, which may be acquired under a pen register order. Other types of web addresses reveal similar types of personal information about an individual. When shopping online, items visited or purchased are generally embedded in the web address. While obtaining the phone numbers that an individual calls probably will not reveal much regarding his or her actions, preferences, or attributes, obtaining that same individual's addressing information likely will. Much can be determined about a person from discovering the websites that they frequent or the searches that they run.

Second, while individuals do not have a legitimate expectation of privacy in the phone numbers that they dial or the phone numbers of those calling them,[176] individuals should and do have an expectation of privacy with respect to the more personal information that can be gleaned from a web address.[177] Web addresses themselves would not seem to inherently raise a legitimate expectation of privacy, but there could be a legitimate expectation of privacy with regard to a particular activity that was engaged in during a visit to a website, which could be revealed by the addressing information.[178] For example, an individual might not be concerned with whether or not others discover that he visited a particular website, but in many instances, he would still expect privacy with respect to the purchase of an item or subscription from that website.[179]

Even though it seems somewhat attenuated to make a direct analogy between phone numbers and addressing information, courts are very unlikely to reject the Patriot Act's application of existing pen register standards to electronic addressing information.[180] For this reason, law enforcement agencies may be able to discover significant amounts of subjective information about an individual, while remaining within boundaries that allow nearly automatic approval under the standard of relevancy to an ongoing investiga-

176. Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

177. *See supra* notes 65-72 and accompanying text.

178. Geoffrey A. North, *Carnivore in Cyberspace: Extending the Electronic Communications Privacy Act's Framework to Carnivore Surveillance*, 28 RUTGERS COMPUTER & TECH. L.J. 155, 189-90 (2002).

179. The existence of cookies and other Internet usage tracking tools weakens such an argument in the case of the average online user, but what about for those who take steps to block such devices? *See* Paul Lansing & Mark D. Halter, *Internet Advertising and Right to Privacy Issues*, 80 U. DET. MERCY L. REV. 181, 198 (2003).

180. F*ield Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, Computer Crime & Intellectual Property Section, U.S. Dept. of Justice, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Oct. 25, 2003) (noting that numerous courts had already applied the pen/trap provisions communications on computer networks).

tion.[181] A better approach would have been for the legislature to develop an entirely different standard, taking into account the functional differences in wire and electronic communications. The enactment of the Patriot Act gives a not-so-subtle warning to Internet users to be careful as to what sites they visit and what they enter into online search engines.

C. Effects on Surveillance Under FISA

The Foreign Intelligence Surveillance Act is part of the dividing wall that Congress erected between domestic law enforcement and foreign intelligence agencies. Congress deemed such separation necessary as a result of the tremendous abuse of power that had taken place at the hands of the executive branch, namely that investigation and surveillance of ordinary individuals was being conducted in the name of national security.[182] Until the passage of the Patriot Act, the barriers between traditional law enforcement agencies and intelligence agencies ran all the way from the separation of their duties to the lack of information sharing between them. Those conducting intelligence investigations related to national security have enjoyed broader powers and fewer restrictions.[183] The prohibitions against sharing most information discovered in the context of such an investigation with those in traditional law enforcement or against using such information in a criminal trial existed to prevent traditional law enforcement from using investigation in the name of national security as an end-run around the stricter procedural requirements of criminal investigations.[184]

The events of September 11, however, caused the country to realize that more cooperation between domestic law enforcement and foreign intelligence agencies was necessary for the protection of national security.[185] Congress responded by enacting section 203 of the Patriot Act, which "facilitates this cooperation by allowing 'foreign intelligence information' gathered in

181. *See supra* note 122 and accompanying text; *see also* 18 U.S.C. § 3123(a)(2) (2000). Note that an individual does not have to be a suspected terrorist or even be a criminal to be subjected to this type of surveillance; the law enforcement agency must only certify that it is relevant to an ongoing investigation. *Id.*

182. *See supra* notes 137-42 and accompanying text.

183. McCarthy, *supra* note 159, at 443.

184. *Id.* at 442-43.

185. Some of those involved in the terrorist attacks of September 11, 2001 had lived in the United States for some time and had run-ins with domestic law enforcement. Domestic law enforcement learned information that would have raised red flags with various agencies responsible for national security had a system of information sharing been in place. *Agent: Moussaoui "could fly. . .into the WTC"* (May 14, 2002), CNN, *at* http://www.cnn.com/2002/US/05/12/inv.moussaoui.fbi/index.html.

criminal investigations by domestic law enforcement to be shared with the intelligence community."[186]

One concern that has arisen since the Patriot Act removed many of the boundaries between law enforcement and intelligence communities is that it may now be easier for law enforcement agents to use FISA to circumvent the more stringent requirements of the Wiretap Act for the purpose of obtaining an intercept order.[187] Before the enactment of the Patriot Act, a major issue existed, which was whether or not intelligence information gathered under FISA on spies or terrorists operating domestically could be used to criminally prosecute them.[188] FISA attempted to answer this issue by establishing that information obtained under its provisions could be disclosed for law enforcement purposes if the information was to be used in a criminal proceeding and if authorized by the Attorney General.[189] This solution was inadequate, however, because it was difficult to determine, at the beginning of an investigation, whether or not a suspect would ever be prosecuted or if there would ever be enough evidence to obtain a Title III order.[190] Courts responded to this dilemma by allowing information obtained pursuant to FISA to be used as evidence in criminal proceedings if intelligence gathering was the "primary purpose" of the surveillance.[191] The Patriot Act subsequently changed this "primary purpose" language to the broader requirement of "significant purpose."[192] This new language raises the concern that there is now more room for abuse by law enforcement. More specifically, based on this new requirement, law enforcement may now begin to conduct surveillance under a more easily acquired FISA warrant on a greater number of individuals, who may or may not be a foreign agent or a threat to national security. The new requirement would allow information obtained in such a situation to be admitted as evidence more frequently. The potential for abuse is enormous: as occurred during the 1960's and 1970's, intelligence surveillance could be utilized against ordinary U.S. citizens. Basically, "facilitating the use of FISA to circumvent Title III intercept order requirements potentially puts non-terrorists at risk of being investigated and prosecuted as terrorists."[193]

There are many who argue that the attacks of September 11 demonstrate the necessity of a change to less stringent rules governing intelligence gather-

186. John Podesta, *USA Patriot Act: The Good, the Bad, and the Sunset*, 29 HUM. RTS. Q. 3 (2002).

187. Henderson, *supra* note 45, at 194.

188. *Id*.

189. *Id*. (citing 50 U.S.C. § 1806(b) (2000)).

190. *Id*.

191. *See* United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987); United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984).

192. Patriot Act, Pub. L. No. 107-56, § 218, 115 Stat. 272 (2001).

193. Henderson, *supra* note 45, at 203.

ing and sharing. Evidence from investigation of the attack indeed appears to support this argument.[194] Still, section 203 could have been safeguarded somewhat from the potential for abuse by the executive branch if it had explicitly provided for judicial oversight of some kind. Such a provision would not have detracted from the purpose of the section, but would have gone a long way to insure against its misuse.

Another major change that the Patriot Act wrought in the FISA framework relates to the ability of intelligence agencies to use what are known as roving wiretaps.[195] These were previously available only under the Wiretap Act for use by domestic law enforcement, but section 206 of the Patriot Act amended FISA to include this tool in the intelligence community's arsenal as well.[196] Under the Wiretap Act, law enforcement must establish that the targeted individual is actually using the communication devices to be tapped,[197] but the new FISA standard is much lower. Now the government must only show that the target is likely to thwart surveillance that monitors only a single device.[198]

Roving wiretaps are inherently highly invasive because they allow the government to monitor the communications of individuals completely unrelated to its investigations.[199] As a practical example in the context of electronic communication, take the case of a suspected spy or terrorist whose communications were being monitored under a roving wiretap pursuant to FISA. If the targeted suspect used a public computer to send or receive e-mail, the investigating agency might continue to monitor communications on that computer in the event that he or she would return. Consequently, the electronic communications of any other individual using that computer would be monitored as well. They would be subject to one of the most intrusive forms of surveillance without ever being aware of it and without a warrant ever having been issued for such purposes. While the standard used under the Wiretap Act helps to minimize this privacy concern, there is no

194. David Johnston & Philip Shenron, *FBI Curbed Scrutiny of Man Now a Suspect in the Attacks*, N.Y. TIMES, Oct. 5, 2001, at A1. The FBI refrained from criminally investigating an individual involved in the attacks because it would have made it difficult to later obtain approval for covert surveillance under FISA. *Id.*

195. Roving wiretaps allow the monitoring agency to conduct surveillance or interceptions on multiple communication devices under the authority of a single intercept order. They received their name from the fact that they must change locations as the individual subject to the surveillance moves. Patriot Act, Pub. L. No. 107-56, § 206.

196. *Id.*

197. 18 U.S.C. § 2518(12) (2000).

198. Patriot Act, Pub. L. No. 107-56, § 206, 115 Stat. 272 (2001).

199. *How the Anti-Terrorism Bill Limits Judicial Oversight of Telephone and Internet Surveillance*, American Civil Liberties Union, *available at* http://www.aclu.org/congress/1102301g.html (last visited Oct. 25, 2003).

such built-in protection in the corresponding FISA provision.[200] Moreover, Section 206 does not provide for any method of judicial oversight, such as requiring the agencies conducting the surveillance to report periodically to the judge who issued the warrant. Such a requirement would dramatically decrease the likelihood that such an expansive authority would be abused.[201] Fortunately, this provision of the Patriot Act sunsets in December, 2005, but if it is to be reinstated, Congress must build in some type of privacy safeguard, so that Americans' civil liberties are protected as well as their safety.

These changes and others brought about by the enactment of the Patriot Act have greatly alarmed privacy rights activists. The executive branch has a poor track record of remaining within its legislatively dictated boundaries, which gives reason to be concerned with respect to a piece of legislation that grants greatly increased powers to that branch without providing sufficient judicial balance or oversight.[202] There seems to be evidence that drastic changes were necessary in order to afford the public better protection against this new type of concealed enemy,[203] and advocates of the Patriot Act argue that it should not be judged prematurely on its face, but rather on its effectiveness in protecting the safety of the American public.[204] While this is a persuasive argument, it basically asks the country to wait and see whether the Act is effective or whether the executive branch abuses the authority that it grants. The difficulty is that the public or the rest of the government may never see abuses of these new powers by law enforcement or intelligence agencies because, by their very nature, they are exercised covertly. The system lacks judicial accountability and that can only exacerbate these privacy issues.

V. Comparing Past and Present

Parts III and IV of this Note argued that in passing the Patriot Act, the government might have overreacted to the threat of domestic terrorism by excessively intruding on Americans' civil liberties. While the life and safety of any individual cannot be overly emphasized, some of the provisions of the Patriot Act do not even relate to terrorism and others grant powers to the

200. Congress is currently considering proposed legislation that would lower the standard for obtaining roving wiretaps under the Wiretap Act to the new standard for obtaining FISA roving wiretaps. While such legislation would promote consistency, this minimal standard would be employed for any roving wiretap, broadening the potential for surveillance of innocent third parties.

201. *See How the Anti-Terrorism Bill Limits Judicial Oversight*, *supra* note 199.

202. The Patriot Act, as passed by Congress, did contain significant privacy protection improvements as compared to the original bill, including the sunset provision and increased judicial and congressional oversight. McCarthy, *supra* note 159, at 439. Many would argue, however, that these were not enough.

203. *Id*. at 437-38.

204. *Id*. at 436.

executive branch that do not properly balance the interests of national security and privacy protection. The Patriot Act was basically a "rush job" on the heels of September 11 and was passed as a quick fix to the immediate dangers presented by terrorism and inadequate law enforcement and intelligence capabilities.[205] Those in the legislature with their own agendas were able to pass drastic provisions unrelated to terrorism because of the sheer size of the Act and the time constraints involved in its passage. Due to the extreme pressures of the situation and hurried nature in which this legislation was enacted, it should be viewed more as a temporary, stopgap measure, rather than permanent law. The fact that the threat of terrorism is unlikely to end in the near future, unlike the dangers of war in years past, may ensure that this legislation lives on in its current and inadequate form. It took extreme circumstances to bring the Patriot Act into existence; what will it take to bring about major modifications or reform to its provisions? A brief comparison between the current situation and the historical examples presented in Part II provides both lessons and warnings for those presently in control of domestic policy.

A. The Likelihood of Disproportionate Effects on Minorities

The most obvious commonality among the historical examples described in Part II is the fact that minority groups bore the brunt of the infringement on civil liberties as a result of the government's reaction to foreign threats. The victims were of the same nationality or ideology as those that presented the foreign threat. During World War I, German-Americans were subjected to unnecessary abuse as a result of hysteria fueled by government propaganda and legislation. During World War II, Japanese-Americans were dispossessed, relocated, mistreated, and even murdered as a result of an executive order that was supported and affirmed by the other two branches of the government. During the Cold War, those who supported communist ideology and those who openly stood up against their mistreatment were publicly and politically abused. Sadly and ironically, virtually none of those who suffered these deprivations of basic human rights had any part in the foreign threat that existed in each of these cases.

Wrong or right, most people tend to associate the threat of terrorism with those of Middle Eastern backgrounds.[206] This conception could result in the unfair and disproportionate electronic surveillance of Middle Eastern Americans. The historical examples discussed earlier tend to show that it would be much more likely in present times for an American citizen of Mid-

205. *EFF Analysis*, *supra* note 162.

206. In the list of notable U.S. encounters with terrorist attacks, stands Timothy McVeigh, the Oklahoma City bomber, who was not Middle Eastern. The infamous Theodore Kaczynski, known as the "Unabomber," was also not Middle Eastern in background. The most recent attacks on September 11, 2001, however, were perpetrated by the Islamic terrorist organization Al Qaeda, which is centered around the Middle East and Southern Asia.

dle Eastern descent, as opposed to a citizen of Caucasian ancestry, to fall within the scope of intelligence surveillance with its newly relaxed procedural requirements. Many of foreign backgrounds retain ties with their countries of origin through written, electronic, and wire communication. The passage of the Patriot Act, which expanded the scope and reduced the requirements of FISA surveillance, could result in the illicit interception of international communications from those of Middle Eastern backgrounds.[207] The risk is especially great with respect to electronic communications with its decreased protection and its greater vulnerability to undetectable acquisition. As discussed in Part IV, there are many cracks in the framework of electronic communications privacy law, and since the enactment of the Patriot Act, there are many ways to circumvent the more stringent requirements for conducting surveillance. Borderline cases involving those of foreign backgrounds would be much easier to manipulate through the cracks and loopholes in these laws. Senator Russ Feingold, the lone dissenter in the Senate's vote to approve the Patriot Act, addressed his concern that the enhanced authority to profile and engage in electronic surveillance would be disproportionately wielded: "In the wake of these terrible events our government has been given vast new powers and they may fall most heavily on a minority of our population [Arab, Muslim, and South Asian immigrants] who already feel particularly acutely the pain of this disaster."[208] This country's past responses to similar situations would seem to support Senator Feingold's concerns.

B. Lack of Appropriate Levels of Judicial Oversight

Another trend that seems to repeat itself historically is that the government seems to unite itself in response to and against foreign threats. In general, this is a positive reaction, but it can also have a negative effect, as it did in each of the historical examples outlined above. In times of war or when threats to the national security of the United States materialize, the executive branch requires greater powers than it does during peacetime. This additional authority must be granted by the legislative branch, which must determine what levels of power are appropriate for dealing with the crisis at hand. The judiciary responds to complaints that either the legislation enacted by Congress does not comport with Constitutional standards or that the executive branch has overstepped the authority it has been granted by Congress. The delicate equilibrium that exists in this system of checks and balances is

207. *See supra* notes 139-40 and accompanying text; *see also 'Guilty' of Being Muslim?*, *supra* note 42. As noted above, this very practice has been implemented in the past, also during a time of relaxed or non-existent procedural requirements for intelligence surveillance. *Id.*

208. *The USA PATRIOT Act*, Electronic Privacy Information Center, *available at* http://www.epic.org/privacy/terrorism/usapatriot/ (last visited Oct. 25, 2003) (citing Senator Russ Feingold's statement on the Anti-Terrorism Bill (Oct. 25, 2002)).

easily upset in times of war or crisis. In an effort to present a united front against threats to national security, the various branches of government have been hesitant to take a stand against abuses of power by the other branches.[209] For example, in times of war, the Supreme Court may uphold emergency legislation that would never pass Constitutional muster during peacetime, or the judiciary and Congress may allow the executive branch to take certain action that they would never allow in normal situations.[210] As discussed earlier, during World War I, Congress passed legislation that severely diminished the individual's right to free speech and the Supreme Court upheld convictions under that legislation. Neither Congress nor the Supreme Court interfered with President Roosevelt's Executive Order 9066, which resulted in the deplorable treatment of Japanese-American citizens during World War II. These examples demonstrate that even during times of war, the various branches of government can exceed legitimate levels of authority, and in such situations it is the duty of the other branches to intervene and prevent injustice in the name of national security.

This lesson is especially poignant today in the area of privacy with respect to electronic communications. The Patriot Act has granted the executive branch unprecedented authority to monitor and conduct surveillance of electronic communications. A successful balance between protecting national security and individual privacy rights may only be achieved with the cooperation of all three branches of the government. Most importantly, the judiciary must maintain a watchful eye on the actions of law enforcement and intelligence agencies as they conduct their surveillance and investigations under this new legislation, and the judiciary must also draw sharp boundaries around what the new legislation allows. The Patriot Act, however, "continues an alarming trend known as court-stripping—removing authority from the judiciary—in time of crisis."[211] In addition, even before the Patriot Act, the recent judicial trend has been to decreasingly favor privacy rights interests in the area of electronic communication.[212] If the historical trend has also been for the judiciary to refrain from interfering with the executive and legislative branches in times of crisis, there seems to be little reason to expect that the courts will provide the oversight necessary to preserve the appropriate balance between the preservation privacy rights and national

209. Whitehead & Aden, *supra* note 58, at 1084-85.

210. *Id.*

211. Emmanuel Gross, *The Influence of Terrorist Attacks on Human Rights in the United States: The Aftermath of September 11, 2001*, 28 N.C. J. INT'L L. & COM. REG. 1, 2 (2002) (stating that "[a]s it has done in times of past tragedy, the government responded by passing legislation that reduces or eliminates the process of judicial review and erodes our civil liberties.").

212. *See e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d at 868, 878-79 (9th Cir. 2002) (construing narrowly the protections of the Wiretap Act to prohibit only interceptions of electronic communications that are contemporaneous with the transfer of those communications).

security.[213] These trends must be broken if the United States is to avoid flagrant violations of civil liberties similar to those that have taken place in past crisis situations.

C. Misconstruing the Threat to National Security

During World War I, the threat of German subversive activities in the United States was very much exaggerated. Of the ten individuals convicted of espionage in the United States during World War II, none were of Japanese descent. During the "Cold War," there was a very real threat of Communist counter-intelligence activity, but due to the inappropriate overreaction by those in power in the federal government at the time, the true sources of that threat were not discovered until much later. In each of these cases, the infringement upon the civil liberties of Americans did nothing to pinpoint or protect against the feared threat.

While the threat of terrorism is clearly very real and very dangerous, these examples demonstrate that the indiscriminate violation of the civil rights of ordinary Americans will not alleviate it. Enacting more stringent standards that must be satisfied before surveillance can take place would prevent a repeat of the past. Establishing at least a modicum of evidence that points toward probable cause should be a requirement before even the most non-intrusive methods of surveillance could be performed. Limiting the provisions of the Patriot Act to the surveillance of those suspected of crimes actually relating to terrorism or to those suspected of being involved in the perpetration of terrorism would also help to prevent the overly broad application of new surveillance powers to ordinary citizens or even common criminals. And again, judicial oversight is necessary to enforce such standards and insure that improper surveillance is not being conducted with respect to those who do not pose any real threat of terrorism. Requests for warrants should no longer be merely a process of rubberstamping. Judges should not only have the authority to reject an application for conducting surveillance, but they should also not be afraid to use it. Judges have not generally utilized their authority in this area even in times without a serious threat of terrorism;[214] there can be no assumption that they will begin to do so in more dangerous times.

VI. Conclusion

Under the most favorable of circumstances, the predictions offered in this Note warning against governmental infringement on electronic communications privacy rights will never materialize. Hopefully, law enforcement and intelligence agencies will keep their surveillance techniques within reasonable limits, and the courts' interpretations of the Patriot Act will not stretch the framework of privacy protection law to its breaking point. This

213. Groskopf, *supra* note 13, at 204.

214. *See* Henderson, *supra* note 45 and accompanying text.

optimistic outcome should not be left to chance, however, but rather pursued with diligence. The events of September 11 created a new paradigm for the existence of individual privacy rights. The protection of domestic security from further terrorist attacks is a basic necessity that inherently conflicts with individuals' ability to exercise the civil liberties to which they have become accustomed. For this reason, individual privacy rights cannot simply exist as they have in the past; they must be restructured and bolstered against the attacks of a hidden enemy whose goal is to destroy those rights and the way of life that they afford. President George W. Bush promised, "We will not allow this enemy to win the war by changing our way of life or restricting our freedoms."[215] While the Patriot Act may not have been designed to restrict the privacy rights of American citizens, it appears to have done just that in overreacting to the threat of terrorism and in inappropriately restructuring privacy protection law, especially in the area of electronic communication. Government officials and leaders must learn from the mistakes made by their predecessors: the courts must take a more active role in overseeing the increased executive powers, the legislature must carefully tailor provisions directly affecting privacy rights, and the executive branch must be careful to avoid overstepping the bounds of its expanded authority. As the adage warns, those who do not learn from the mistakes of the past are doomed to repeat them. Moreover, American citizens must not sit idly by, watching as their privacy rights are taken from them, expecting them to be returned when relative safety has been restored. It would be a travesty to lose the right to privacy with respect to electronic communication before it has even been completely secured. The future of this right lies in the hands of the American people and government; to throw it and every other civil liberty away in the name of personal security would only give terrorists victory.

215. *After the Attacks: Bush's Remarks to Cabinet and Advisers*, N.Y. TIMES, Sept. 13, 2001, at A16.