UIC Law Review

Volume 36 | Issue 4 Article 7

Summer 2003

Privacy to Be Patched in Later - an Examination of the Decline of Privacy Rights, 36 J. Marshall L. Rev. 985 (2003)

Matthew Hector

PRIVACY TO BE PATCHED IN LATER – AN EXAMINATION OF THE DECLINE OF PRIVACY RIGHTS

MATTHEW HECTOR*

"The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[1]

INTRODUCTION

"Big Brother is Watching You" is perhaps one of the best-known quotes from George Orwell's novel, *1984*.[2] The scope and pervasiveness of governmental surveillance has not yet reached Orwellian levels. However, recent changes to the FBI investigation guidelines have restricted privacy protections.[3] Additionally, the Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)[4] has eroded the Fourth Amendment's protections against unreasonable search and seizure.[5] Protecting the nation from terrorist attacks is important; however, maintaining the delicate balance between privacy and security is of the utmost importance.

---

* J.D. Candidate, expected graduation June 2004. The author would like to thank Professor Samuel Olken, Dr. Dan Celander, Patricia Scott, and Anne and Bill Hector for their guidance, advice, and time during this comment's research and writing process.

1. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting). Justice Brandeis argued that all wiretaps are contrary to the purpose of the Fourth Amendment, involving multiple invasions of privacy to achieve their goals. *Id.* at 475-76. "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping." *Id.* at 476. The where and how of an invasion of privacy is immaterial in determining the Constitutionality of a search and seizure. *Id.* at 479.

2. GEORGE ORWELL, 1984 5 (The New American Library, Inc. 1981) (1949). Orwell's vision of the future has yet to come to fruition. However, as technology develops, and governmental interest in national security increases, the risks to privacy become greater.

3. *See* Jerry Berman & James X. Dempsey, *CDT's Guide to the FBI Guidelines: Impact on Civil Liberties and Security – The Need for Congressional Oversight*, CENTER FOR DEMOCRACY & TECHNOLOGY, (June 26, 2002), *at* http://www.cdt.org/wiretap/020626guidelines.shtml (last visited July 29, 2003) (outlining the major privacy issues associated with the May 30, 2002 FBI Guidelines changes, particularly the expanded scope and duration of preliminary investigations, for which the evidentiary threshold is low).

4. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18, 28, and 50 U.S.C.).

5. *See id.* at tit. II, § 201 (allowing law enforcement to use enhanced surveillance procedures to combat terrorism).

The right to privacy has been viewed as a fundamental element of democratic society since the days of Locke and Rousseau.[6] Privacy is not only essential for human dignity, but it provides valuable protections that are essential to the functioning of a democratic society.[7]

The Fourth Amendment arose partially from the Pennsylvania Bill of Rights, which contained a provision similar to our Fourth Amendment.[8] It also addressed the general search warrants the British monarchy used to quell political speech in the Colonies.[9] These influences indicate the Framers' desire to protect democracy by protecting privacy.[10] Without this fundamental "right to be let alone," political speech, and thus the functioning of our democracy, would be stymied.[11]

In the past, our nation has committed grievous violations of civil liberties in order to protect the nation's security. The most egregious of these acts occurred in 1942, when Americans of Japanese decent were subjected to a military "Civilian Exclusion Order."[12] In 1944, the Supreme Court of the United States held that, "when under conditions of modern warfare our shores are threatened by hostile forces, the power to protect must be commensurate with the threatened danger."[13] Unfortunately, in *Korematsu v. United States*, the protection offered to the nation was at the expense of an entire race of citizens.[14] Over fifty years later, we are faced with another national crisis, one that involves a new kind of modern warfare. While it is still necessary to protect our nation against terrorist attacks, a valuable lesson can be learned from the gross misstep of *Korematsu*.[15]

---

6. *See* PHILLIPA STRUM, PRIVACY: THE DEBATE IN THE UNITED STATES SINCE 1945 5-11 (Gerald Nash & Richard Etulain eds., 1998) (discussing the historical foundations of the right to privacy).

7. *See id.* (arguing that privacy is essential for democratic societies).

8. *Id.* at 9-10.

9. *Id.* at 10.

10. *See id.* at 11 (arguing that the Constitution was intended to contain a fundamental right to privacy).

11. *Id.* at 4-6.

12. Korematsu v. United States, 323 U.S. 214, 215-16 (1944). Under that order, "all persons of Japanese ancestry [were] excluded from" the Western United States. *Id.* at 216.

13. *Id.* at 220.

14. *See id.* at 243 (Jackson, J., dissenting) (indicating that as a loyal, native-born American, Korematsu was not prone to subversive activity). Justice Jackson points out one should not be penalized for the treasonous acts of "one's antecedents". *Id.* The logic behind the Civilian Exclusion Order is therefore fatally flawed; excluding an entire group of Americans based on race was a serious blow to liberty. *Id.* at 245-46.

15. *See Olmstead*, 277 U.S. at 479 (Brandeis, J., dissenting) (noting that well-meaning people, in the name of national security, can trample the privacy rights of others). The quote from Justice Brandeis that opens this Comment is especially telling in light of the subsequent example of *Korematsu*. *Id.* Brandeis noted that even the best-intended actions could have a deleterious effect on liberty as a whole. *Id.* The American military, supported by the United States Supreme Court, committed one of the greatest encroachments on individual liberty in the post-Civil War United States; the individuals who allowed this to occur were so dedicated to national security that they did not understand the way their actions would ultimately impact liberty. *Korematsu*, 323 U.S. at 214.

This Comment will first examine the development of the right to privacy, specifically as it is derived from the Fourth Amendment and jurisprudence from 1928 to the late 1960s. It will then examine how search and seizure law has impacted privacy rights in the late 20th and early 21st centuries. The influence of the USA PATRIOT Act on the Foreign Intelligence Surveillance Act (FISA)[16] will be examined; the PATRIOT Act also has implications in conjunction with the latest FBI Guidelines for investigating terrorism issued by the Attorney General.[17] The lowered threshold for obtaining a wiretap warrant, when combined with the decreased levels of proof required to sustain an informal investigation, provide some startling implications for the future of privacy rights.[18] This Comment will examine these implications from a historical and social context. Finally, this Comment will propose measures that will strike a careful balance between national security and the right to privacy.

I. BACKGROUND

A. The De-evolution of Privacy Rights in the 20th and 21st Centuries

The right to privacy springs from the Fourth Amendment, as well as from pre-constitutional sources.[19] The Search and Seizure Clause of the Fourth Amendment can be viewed as a response to invasions of privacy suffered by the Colonists at the hands of the British.[20] For over one hundred

16. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62 (2000) (amended 2001).

17. John Ashcroft, *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*, (May 30, 2002), *available at* http://www.usdoj.gov/olp (last visited July 21, 2003). This document will be referred to as "Guidelines."

18. *See* Berman & Dempsey, *supra* note 3 (discussing the impact of newly approved methods of obtaining data such as random web-browsing). Also, the directive permits the FBI to "subscribe to any commercial or non-profit profiling and data mining service." *Id.* The evidentiary threshold has plummeted to the point that almost any scintilla of suspicion is enough to justify a preliminary investigation. *Id.* Another problematic change is the length of time an investigation can continue for without producing any true evidence of wrongdoing. *Id.*

19. STRUM, *supra* note 6, at 9-11. A portion of the Constitution's Bill of Rights is based on the Pennsylvania Bill of Rights. *Id.* at 9-10. Enacted in 1754, the Pennsylvania Bill of Rights states as follows:

> The people have a right to hold themselves, their houses, papers and possessions free from search and seizure; and therefore warrants, without oaths or affirmations first made, affording a sufficient foundation for them, and whereby any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his or their property not particularly described, are contrary to that right, and ought not be granted.

Id. at 9. This foundation of the notion of privacy has been shaken by the revised FBI Guidelines. *See* Berman & Dempsey, *supra* note 3 (demonstrating that the evidentiary threshold for invading the privacy of an individual is so low that it negates the concept of sufficient foundation for a warrant).

20. STRUM, *supra* note 6, at 10. Invasions of privacy committed by the British include the following: political surveillance, requiring a license for the publication of all books

years, American jurisprudence was largely silent on the issue of privacy.[21] Although a handful of Supreme Court opinions may have dealt with privacy issues earlier, Justice Brandeis' dissent in *Olmstead v. United States*[22] that case highlighted the idea that technological advances should not bar a citizen from protecting his or her right to privacy.[23] The intent of the framers, Brandeis argued, was to "protect Americans in their beliefs, their thoughts, their emotions, and their sensations."[24] Drawing on his 1890 law review article, he found that protection in the right to privacy was implied in the Constitution.[25] As the legal community absorbed Justice Brandeis' ideas, change slowly began to occur in American privacy jurisprudence.

By the mid-1960s, the Supreme Court began to lean towards a reading of the Fourth Amendment that was similar to Brandeis' reading.[26] In *Katz v. United States*,[27] the majority, speaking through Justice Stewart, expanded the right to privacy.[28] The Court abandoned the physical invasion test[29] of

---

and pamphlets, requiring that all of the same bear the name of the author, and quartering troops in the homes of Colonists. *Id.*

21. *See id.* at 3 (noting that Samuel D. Warren and Justice Louis Brandeis' December 1890 article, *The Right to Privacy*, in the *Harvard Law Review*, was the first American argument that there was a fundamental and "identifiable 'right to privacy'").

22. 277 U.S. at 438.

23. *Id.* at 475. "There is, in essence, no difference between the sealed letter and the private telephone message." *Id.* Brandeis continued to point out that wiretapping is more invasive than intercepting a letter. *Id.* at 475-76. Brandeis also discussed the interplay between the Fourth and Fifth Amendments, stating that obtaining evidence in violation of the Fourth Amendment and then using it in a trial also violates the Fifth Amendment protection against self-incrimination. *Id.* at 476-78. Brandeis moved away from the majority's literal interpretation of the Constitution, stressing that while the framers could not have contemplated the act of wiretapping, the Constitution was intended to protect against many types of governmental violations of privacy. *Id.* His dissent also acknowledges that over time, new methods of invading the privacy of citizens would become available, perhaps even one day, "[the government] will be enabled to expose to a jury the most intimate occurrences of the home." *Id.* at 474.

24. *Olmstead*, 277 U.S. at 478.

25. *Id.* In addition to each invasion being a violation of the Fourth Amendment, Brandeis equates any use of improperly obtained evidence as a violation of the Fifth Amendment. *Id.* at 476-78. Brandeis argued that this marriage of the Fourth and Fifth Amendments necessarily made wiretapping unconstitutional. *Id.* Brandeis acknowledged the need to balance the interests of law enforcement against the rights of the people. *Id.* at 479. However, at the time, many states had made wiretapping illegal. *Id.* at 480. Justice Brandeis argues that federal agents should not be allowed to collect evidence through a method that violates the laws of the states. *Id.*

26. *See* Katz v. United States, 389 U.S. 347 (1967) (adopting a right to privacy).

27. *Id.*

28. *Id.* at 353. This was the result of the gradual development of other privacy cases, especially those related to search and seizure. *Id.* Ultimately, *Katz* overturned *Olmstead* and adopted the Brandeis analysis of a more expansive, functionalist reading of the Fourth Amendment, abandoning the strict physical invasion reading taken by the majority in the *Olmstead* Court. *Id.* "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Id.* at 352. By acknowledging that changes in technology have required re-defining the scope of the Fourth Amendment, the *Katz* Court took the focus off of literal physical invasion. *Id.* at 353.

earlier decisions, which required an actual physical entry into a protected area, like a residence, to establish a violation of privacy.[30] The Court adopted a new, person-centric[31] test.[32] This test required demonstrating an expectation of privacy; however, that expectation had to be reasonable.[33]

In *Katz*, the petitioner used a public telephone booth with the door closed.[34] The Court recognized this attempt to maintain privacy and acknowledged that the expectation of privacy in a phone booth was reasonable because Katz had taken affirmative steps to guarantee his privacy.[35] The Court acknowledged that regardless of the manner of the search, its legality required a warrant.[36] This warrant requirement for electronic searches echoed the tone of Brandeis' dissent in *Olmstead*.[37] The Court held that regardless of the specific scope of the wiretap, it did not release the agents from their Fourth Amendment obligation to obtain a specific warrant.[38] The individual's right to privacy was gaining popular

29. *Olmstead*, 277 U.S. at 463-64. The majority, speaking through Chief Justice Taft, applied a physical test to determine a violation of the Fourth Amendment. *Id.* Essentially, if investigators did not physically enter the "private quarters of the defendant," they had not committed a violation of the defendant's Fourth Amendment rights. *Id.* at 464. The Court further tried to differentiate between the interception of physical objects, like letters, and the interception of oral communications, like phone calls. *Id.*

30. *See Katz*, 389 U.S. at 351 (noting that the issue is not whether physical places are protected by the Fourth Amendment, but whether people are protected by the Fourth Amendment).

31. *Id.* The Court held that the umbrella of Fourth Amendment protection attached to the individual, not physical locations. *Id.* If an individual seeks to keep something private, it is protected by the Constitution. *Id.*

32. *Id.* "[T]he Fourth Amendment protects people, not places . . . . [W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.*

33. *Id.* at 361 (Harlan, J., concurring).

34. *Katz*, 389 U.S. at 361. For Justice Harlan, the fact that the petitioner had closed the telephone booth door was key. *Id.* Had the petitioner been having a conversation with someone in the open, outside the confines of a telephone booth and the telephone wires, he would not have had a reasonable expectation of privacy. *Id.*

35. *Id.* Harlan articulated a two-pronged test for evaluating whether an individual has a reasonable expectation of privacy: "[F]irst that a person have exhibited [sic] an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* Standing nude in one's window would not demonstrate an expectation of privacy, nor would one speaking in a crowded bar be recognized as demonstrating a reasonable expectation of privacy. *Id.*

36. *Id.* at 356. The Court further held that the exceptions to the Fourth Amendment warrant requirement did not apply to electronic searches. *Katz*, 389 U.S. at 357-58.

> Even electronic surveillance substantially contemporaneous with an individual's arrest could hardly be deemed an 'incident' of that arrest. Nor could the use of electronic surveillance without prior authorization be justified on grounds of 'hot pursuit.' And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect's consent.

Id. The Court did not, however, answer the question of whether this rule applied to matters of national security. *Id.*

37. *See Olmstead*, 277 U.S. at 473-74 (indicating that non-physical, technologically advanced searches demand Fourth Amendment protection).

38. *Katz*, 389 U.S. at 358-59. *Cf. Olmstead*, 277 U.S. at 475-76 (Brandeis, J.,

support and a foothold in the political community.[39]

However, this right, vested in the individual, was not without its limits. *Terry v. Ohio*[40] addressed the question of "the scope of a policeman's power when he confronts a citizen without probable cause to arrest him."[41] A plain-clothed police officer observed petitioner, Terry, apparently casing a store.[42] The officer approached Terry and his associates in an attempt to further ascertain their purpose.[43] After brief questioning, the officer spun Terry around and frisked him.[44] The search revealed a concealed revolver.[45]

The circumstances surrounding the search were the crux of Terry's objections to the introduction of the gun at trial.[46] The Supreme Court took issue with the holdings of the lower courts that a stop could be distinguished from a seizure.[47] Chief Justice Warren also took issue with the lower courts' holdings that a frisk was not a search.[48] The Court refused to modify its past

---

dissenting) (noting that writs of assistance and general warrants seem similar to wiretaps, as they allow any person at any time and place to be searched). *See also* STRUM, *supra* note 6, at 115 (discussing writs of assistance and general warrants). Allowing law-enforcement agents to police themselves in the process of wiretapping could lead to abuse, no matter how specific the wiretap. *Katz*, 389 U.S. at 358-59.

39. STRUM, *supra* note 6, at 121. President Johnson's stated, in his January 1967 State of the Union Address, that "We should protect what Justice Brandeis called the 'right most valued by civilized men' – the right to privacy." *Id.*

40. *Terry v. Ohio*, 392 U.S. 1 (1968).

41. *Id.* at 16. A key issue in *Terry* was balancing the rights of the individual (the reasonable expectation of privacy) against the public interest of law enforcement officers neutralizing a potentially dangerous, armed individual. *Id.* at 10-11. To guide this balancing act, the Court adopted the standards set forth by Justice Harlan in *Katz*. *Id.* at 9. However, the fuzzy notion of a "reasonable" expectation of privacy has led to further ambiguity in Fourth Amendment search and seizure interpretation. STRUM, *supra* note 6, at 123.

42. *Terry*, 392 U.S. at 5-6. Officer McFadden, the arresting officer, alleged that the behavior of Terry and his associate was typical of criminals preparing to perform an armed robbery. *Id.*

43. *Id.* at 6-7.

44. *Id.* at 7.

45. *Id.*

46. *Id.* at 7-8. The trial court denied Terry's objection to the introduction of the gun into evidence. *Id.* at 8. Special attention was paid to the language used to describe the encounter between Terry and Officer McFadden. *Terry*, 392 U.S. at 8. The trial court, and later the appellate court, held that a stop and frisk was distinguishable from a search and seizure. *Id.*

47. *Id.* at 16. Chief Justice Warren reasoned that not every seizure must take the form of an arrest. *Id.* The threshold for seizure of a person is when that person is not free to walk away, or when that freedom has been restrained. *Id.*

48. *Id.* at 16-17. Chief Justice Warren's indignation that the lower courts would trivialize the nature of a public body search is apparent from his choice of words. *Terry*, 392 U.S. at 16-17.

> [I]t is nothing less than sheer torture of the English language to suggest that a careful exploration of the outer surfaces of a person's clothing all over his or her body in an attempt to find weapons is not a 'search.' Moreover, it is simply fantastic to urge that such a procedure preformed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a 'petty indignity.'

Id. Chief Justice Warren was especially wary of the distinction between terms because of

positions that an initially acceptable search can violate the Fourth Amendment.[49]

In assessing the constitutionality of the officer's actions, the Court stressed the need to balance the public interest against the rights of the individual.[50] The Court held that given the observations of the officer leading up to the search of Terry, the officer was justified in searching Terry to protect his own safety, and that of others.[51] Terry may have expected that the contents of his pockets would remain private; however, the Court reasoned that suspicious conduct would vitiate the right to privacy.[52]

Katz was merely making a phone call;[53] Terry was casing a store.[54] While *Terry* dealt with physical searches of citizens by the police, the reasoning of the Court has been applied to various types of search and seizure cases since 1968.[55]

In the realm of drug-related law-enforcement, the Supreme Court seems to have developed two different standards.[56] In *Kyllo v. United States*, two federal agents used a thermal imager to scan Kyllo's home.[57] This scan produced infrared emissions from Kyllo's home, indicating the possibility of marijuana cultivation inside the house.[58] At trial, Kyllo contested the

---

the implications for the Fourth Amendment. *Id.* at 17.

49. *Id.* at 19. This inquiry must be fact-based, pertaining to the specifics of each encounter with the police. *Id.* In light of the development of this branch of Fourth Amendment rights, the Court stated that the "scope of the particular intrusion, in light of all the exigencies of the case" was the crucial factor in determining whether a search was reasonable. *Id.* The Court felt that attempting to give an exact definition to the terms search and seizure would risk judicial review taking on legislative qualities not delegated to the courts. *Id.*

50. *Terry*, 392 U.S. at 20-1. This balancing of policies necessarily requires initial accountability on the part of the officer. *Id.* at 21. Without additional accountability on the part of the courts, a stop and frisk by a police officer, based on "subjective good faith," becomes equivalent to a general warrant. *See id.* at 22 (noting that if "subjective good faith" really is the only test for justifying searches and seizures, people are no longer "secure in their persons, houses, papers, and effects").

51. *Id.* at 30-31.

52. *Id.*

53. *Katz*, 389 U.S. at 348.

54. *Terry*, 392 U.S. at 6.

55. STRUM, *supra* note 6, at 125. Strum points out that the trend in the 1980s and 1990s was towards situational favoring of the interest of law enforcement over individual rights. *Id.* Specifically, drug-related and drunk driving search and seizure cases have been decided in favor of law enforcement. *Id.*

56. *See* Kyllo v. United States, 533 U.S. 27 (2001) (placing sense-enhanced searches of a home within the scope of the Fourth Amendment). *Cf.* Florida v. Bostick, 501 U.S. 429 (1991) (holding that all encounters between police and passengers on a bus are not *seizures per se*) *and* United States v. Drayton, 536 U.S. 194 (2002) (holding that searches of bus passengers, even if made without probable cause, were not coercive or subject to Fourth Amendment protections). This split seems largely based on electronic versus physical searches.

57. *Kyllo*, 533 U.S. at 29-30.

58. *Id.* While the scan did not prove the presence of marijuana plants within Kyllo's home, the cumulative effect of this scan and other tips was enough to justify a search warrant. *Id.* at 30.

validity of the warrant used to obtain this scanner evidence.[59] The trial court upheld the warrant, and on appeal, the Ninth Circuit held that it met the requirements of the *Katz* and *Terry* tests of reasonable expectation of privacy.[60] The Supreme Court reversed the determination of the lower courts, unwilling to allow technological advancements to further erode the reasonable expectation of privacy that has existed since *Katz*.[61] Viewed in the scope of *Olmstead* and *Katz*, *Kyllo* echoes Justice Brandeis' fear that technological advances could disastrously erode privacy, even if the means provide a seemingly less invasive method of searching.[62]

However, in two other recent cases, the Supreme Court has been unwilling to extend the protection of the Fourth Amendment to low-tech, warrantless, suspicionless searches of bus passengers. *Florida v. Bostick*[63] carries forward the concept that a *Terry* stop can become unconstitutional if coercion is present.[64] The Court left the decision to the Florida Supreme Court to determine on remand whether questioning within the confines of a bus was coercive.[65] In *United States v. Drayton*,[66] the Court expanded upon *Bostick*, flatly refusing to require that law enforcement officers inform citizens that warrantless searches are voluntary.[67] It would seem reasonable that absent suspicious behavior, the contents of one's pockets would be private; however, these cases illustrate that the *Terry* standard has eroded

---

59. *Id.*

60. *Id.* at 31. Specifically, the Ninth Circuit held that Kyllo's failure to conceal the heat emissions negated his reasonable expectation of privacy, and that given the nature of the search, his expectation of privacy was not objectively reasonable. *Id.*

61. *Id.* at 34. Specifically, Justice Scalia stated, "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Id.* Justice Scalia reasoned that the Court was unwilling to further erode the *Katz* test for the benefit of law enforcement, noting the slippery slope created by encroaching on the accepted boundaries of the reasonable expectation of privacy. *Kyllo*, 533 U.S. at 35-36.

62. *See Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) (writing that "in the application of a constitution, our contemplation cannot only be of what has been but of what may be").

63. *Bostick*, 501 U.S. at 429.

64. *Id.* at 437. Specifically, officers cannot state that compliance with a request to be searched is mandatory. *Id.* The Court also stated that the reasonable person standard for determining coercion presupposes an *innocent* person. *Id.* at 438.

65. *Id.* at 437. The Court reasoned that its refusal to determine whether the nature of the request to search was constitutional was to maintain the holding of *Terry*. *Id.* at 439. However, in *Terry*, the Court did address whether the specific facts of the case breached Fourth Amendment protections. *Terry*, 392 U.S. at 30. A possible explanation for this discrepancy can be seen in the *Bostick* Court's dicta: "this Court is not empowered to forbid law enforcement practices simply because it considers them distasteful." *Bostick*, 501 U.S. at 439.

66. *Drayton*, 536 U.S. at 194.

67. *Id.* at 206-7. The Court also carried forward the reasonable innocent person language. *Id.* at 201-02. In support of its decision that bus stops of this nature are not coercive *per se*, the Court pointed to the freedom of the passenger to leave the bus. *Id.* at 205.

since the 1960s.

The reasonable expectation of privacy has been further complicated by the advent of the Internet and digital phones.[68] As technology advances, law enforcement has an interest in using it to enhance its ability to investigate criminal activity.[69]

Since the Foreign Intelligence Surveillance Act (FISA)[70] was passed in 1978, wiretaps using the national security loophole from *Katz* have increased at an alarming rate.[71] The Foreign Intelligence Surveillance Court (FISC) had never turned down a request for an intelligence wiretap until May 17, 2002.[72] In its first publicly released opinion, the FISC cited governmental admission of material errors in seventy-five warrant applications.[73] In its opinion, the FISC held that further information sharing between criminal and intelligence investigators corrupts the intent of FISA.[74] The August 22 release of the FISC opinion resulted in demands for greater oversight of the FISA process, particularly the activities of the FBI and the Justice Department.[75]

Even more telling for the development of privacy law is that government intelligence gathering is nothing new.[76] Current FISA standards are not as permissive as past governmental espionage, but as new technologies arise, so do new concerns.[77] In addition to the clamoring

---

68. STRUM, *supra* note 6, at 159-60.

69. *Id.*

70. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62 (2000) (amended 2001).

71. STRUM, *supra* note 6, at 160. According to the Justice Department, the FISA Court permitted "207 [taps] in 1979, 512 in 1987, and 576 in 1994." *Id.*

72. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, (FISC May 17, 2002), *available at* http://www.washingtonpost.com/wp-srv/onpolitics /transcripts/fisa_opinion.pdf (last visited July 23, 2003). These wiretaps had been permissively granted under the lowered probable cause standard implemented under FISA. *Id.* at 9.

73. *Id.* at 16. These mistakes and omissions related in part to whether an investigation blended a criminal investigation with a FISA investigation. *Id.* at 17. This blending of investigations and sharing of information is prohibited under FISA. *Id.*

74. *Id.* at 22.

75. Nat Hentoff, *Who Watches the Secret FISA Court?*, THE WASH. TIMES, Sept. 2, 2002, at A19. Hentoff demands that the FISC explain its past permissiveness. *Id.* He also takes Congress to task for not exercising greater oversight over the FBI and the Justice Department. *Id.*

76. John Podesta & Peter Swire, *Speaking Out About Wiretaps*, THE WASH. POST, Aug. 30, 2002, at A23. Of note are the FBI's COINTELPRO and the CIA's Operation Chaos, which kept tabs on various political groups. *Id.* Martin Luther King, Jr., Senators Adlai E. Stevenson III and Eugene McCarthy, and groups like the ACLU and the NAACP, were all targets of these two government intelligence programs. STRUM, *supra* note 6, at 150.

77. Bruce Fein, *What FISA Did and Didn't Do*, THE WASH. TIMES, Aug. 27, 2002, at A14. If a FISA search produces information that can lead to prosecution, the potential defendant cannot access necessary documents to challenge the validity of the warrant because, "the statute mandates in camera, ex parte review by the district court." *Id.* Further, the government is free to keep almost any information on a subject as long as it meets the low threshold of evidentiary relevancy set by the statute. *Id.*

amongst the media, civil rights groups are concerned about the impact of the recent changes to intelligence gathering rules.[78]

II. ANALYSIS

A. Digital Space and Communications – A Brave New Virtual World

With the advent of the Internet, new privacy issues have arisen regarding e-mail, websites and the servers that store them, and message boards.[79] Congress has made efforts to codify new privacy rules for this brave new virtual world, particularly the Electronic Communication Privacy Act (ECPA).[80] For instance, the Wiretap Act[81] required that investigators obtain warrants for electronic surveillance, even in espionage cases.[82] This statutory requirement, however, has been pushed aside by the Executive Branch in the name of national security.[83] Although this "loophole" is only applied to foreign agents and those suspected of being foreign agents, the potential for abuse seems clear.[84]

The misuse and abuse of semantics is also eroding privacy in this new area of the law. Though not involving search and seizure, *Konop v. Hawaiian Airlines, Inc.*[85] sets a disturbing precedent for the interpretation of the ECPA.[86] Konop, an employee of Hawaiian Airlines, maintained a website where he actively voiced his criticisms of the company, the

78. *See* Berman & Dempsey, *supra* note 3 (outlining the Center for Democracy and Technology's concerns about the May 30, 2002 FBI Guideline revisions). The Center for Democracy and Technology has taken multiple exceptions with the new Attorney General Guidelines for FBI General Investigations. *Id.* Additionally, the Electronic Privacy Information Center (EPIC), has voiced concerns about the recently released FISC opinion, and the impact of the USA PATRIOT Act on privacy rights. *FBI Official Claims 'Love of Freedom' Despite Wiretap Abuses*, 20 LONG-DISTANCE COMPETITION REPORT No. 18, (Sept. 2, 2002).

79. STRUM, *supra* note 6, at 157-58.

80. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 (2000). This amended version of the statute corrected the notion that only aural communications were shielded by the Wiretap Act of 1968. The Wiretap Act was codified as 18 U.S.C. §§ 2510-2522 (2000) (amended 1986). The ECPA extended privacy protections to various new forms of communication devices including e-mail, cell phones, voice and text pagers, and computer transmissions. 18 U.S.C § 2511 (2000). *See also* STRUM, *supra* note 6, at 158 (describing the constraints the ECPA puts on "the government's ability to intercept and record new forms of electronic . . . communication.").

81. 18 U.S.C. §§ 2510-2522 (2000) (amended 1986).

82. STRUM, *supra* note 6, at 158.

83. *Id.* "[E]very president since [the Wiretap Act's] passage has ignored this provision with the assertion that the president has the inherent power to wiretap . . . suspected foreign agents." *Id.*

84. *Id.*

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

86. *Id.* at 872. The Ninth Circuit withdrew a previous decision in the case, Konop v. Hawaiian Airlines, Inc., 262 F.3d 972 (9th Cir. 2001), changing the opinion to affirm a district court ruling that held Konop's Wiretap Act claim did not meet the standards established by the ECPA. *Id.*

executives, and the current union.[87] Konop had secured the site with a username and password system, which included explicit terms of use.[88] The court did not reach the issue of whether Konop had a reasonable expectation of privacy under the Wiretap Act; these measures were indicative of that expectation.[89] Just like Katz had closed the door to his phone booth,[90] Konop had closed the door to his website.[91]

The Ninth Circuit, however, escaped the reasonable expectation issue with dubious readings of the Wiretap Act, the ECPA, and the USA PATRIOT Act.[92] The Court reasoned that since Congress had eliminated "stored electronic communications" from both the definition of wire and electronic communication, a communication can only be "intercepted" during its original transmission, and not when retrieved from storage.[93]

This distinction is troubling. While the Court used the plain-language definition of "intercept" in its decision,[94] it failed to understand the essential nature of how the World Wide Web functions. Unlike a phone call, which is communicated at the moment of creation, an electronic transmission, like loading a web page in a browser, differs. When a user visits a specific Uniform Resource Locator, the speech contained on the web page is transmitted contemporaneously to the user.[95] Each page load becomes its

87. *Konop*, 302 F.3d at 872.

88. *Id.* at 872-73. These terms of use included provisions forbidding access to the site by any member of the airline's management. *Id.* at 873. The terms of use also prohibited the dissemination of the site's contents. *Id.*

89. *See id.* at 872-73 (outlining the measures Konop took to secure his website). Similar to the privacy of a phone booth, a secured website should be treated as if its user expects privacy. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (explaining the notion of a reasonable expectation of privacy). Konop implemented the password and user agreement system to limit access. *Konop*, 302 F.3d at 872-73. This is similar to calling someone on the phone, where the expectation is that only the intended recipient receives the communication.

90. *Katz*, 389 U.S. at 352.

91. *Konop*, 302 F.3d at 872-73.

92. *Id.* at 876-79. The Ninth Circuit pointed to the standard established by the Wiretap Act to demonstrate that Congress had differentiated between stored electronic and wire communications when drafting the Act. *Id.* at 877. Specifically, the Court cited the following section of the Wiretap Act as modified by the ECPA:

> Until October 2001, "wire communication" was defined as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception . . . and *such term includes any electronic storage of such communication* . . ."

Id., Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510(1) (2000). (Emphasis added by the court).

93. *Konop*, 302 F.3d at 878. This distinction is aided by the USA PATRIOT Act; in enacting this statute, Congress removed "stored electronic communication" from the definition of wire communications. *Id.*

94. *Id.* at 878. The Court defined "intercept" as meaning, "to stop, seize, or interrupt in progress or course before arrival." *Id.*

95. *Surf the Web: How the Web Works*, LEARNTHENET.COM, (2003), *at* http://www.learnthenet.com/english/index.html (last visited July 22, 2003).

own communication to the recipient.[96] Therefore, the contemporaneous communication resulting from a page load can be intercepted within the Ninth Circuit's definition.

The dissenting opinion in *Konop* highlighted some other difficulties with the majority's decision.[97] Citing a past Ninth Circuit decision, the dissent pointed out that in determining whether a wire communication has been intercepted, the court rejected a contemporaneous transmission requirement.[98] The dissent further argued that this contradiction creates a massive loophole in the electronic communications clause of the ECPA.[99] Under the Ninth Circuit's reading of the ECPA, most electronic communications do not enjoy protection, providing a foothold for warrantless electronic searches by federal law enforcement.[100]

B. Beyond the Civil Ream –The Delimitation of the Fourth Amendment

1. Thinning the Bright Line between Intelligence and Criminal Investigations

On May 17, 2002, the FISC did something it had never done before: it denied the Department of Justice a foreign intelligence surveillance warrant.[101] The Department of Justice had filed a motion with the FISC seeking to almost fully remove the minimization and separation procedures required under the FISA, and as established by past Attorney General Guidelines.[102]

The FISC acknowledged that the primary role of the FISA is not only to preserve national security in the present, but also to look forward toward preserving "a constitutional democracy under the rule of law."[103] The court

---

96. *Id.*

97. *Konop*, 302 F.3d at 886 (Reinhardt, J., dissenting). The dissent finds that "stored electronic communications" should not be exempt from the protections of the ECPA. *Id.* at 886-87.

98. *Id.* at 887. The dissent also found that there was no justification for holding differently for electronic communications, especially since doing so would effectively eviscerate the decision regarding wire communications. *Id.* at 887-88.

99. *Id.* at 888.

100. *Id.*

101. Anne Gearan, *Court's Ruling May Test Domestic Spying Powers*, THE RECORD (BERGEN COUNTY, N.J.), August 24, 2002, at A01.

102. *In re All Matters*, (FISC May 17, 2002) at 1. Minimization procedures are designed to protect the privacy rights of Americans by requiring that information that does not lead to a deeper investigation be destroyed. *Id.* at 12. "Wall" procedures are information screening procedures that guarantee any information shared between intelligence and criminal investigators is only that which is necessary to further the criminal investigation. *Id.* at 15-16.

103. *Id.* at 5. While the FISC casts itself in the role of the arbiter of the FISA's higher purpose, the Court declined to rule on the Department of Justice's assertion that the primary purpose of FISA was now law enforcement. *Id.* at 6 n.2. The Attorney General made the assertion on March 6, 2002, that after the USA PATRIOT Act's amendments to the FISA, the FISA could "be used *primarily* for a law enforcement purpose, so long as a significant foreign intelligence purpose remains." *Id. See also* John Ashcroft, *Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence*

acknowledged that the minimization procedures and information sharing procedures were already intrusive, their scope already codified into the FISA.[104] In particular, the court noted that the foreign intelligence standard of probable cause was significantly lower than the criminal standard, and that investigators only had to show the potential for a facility to be used for espionage or terrorist activities.[105]

In addition to these lowered standards, the minimization rules are significantly lax, presenting problems for a defendant in a trial where the government is using FISA-based evidence.[106] Given the past misrepresentations made to the FISC by Department of Justice officials, allowing the Attorney General's office to prevent a defendant from accessing the warrants and applications used to obtain evidence by submitting an affidavit to the trial court seems akin to letting the fox guard the henhouse. In an effort to prevent the Department of Justice from "[amending] the [FISA] in ways Congress has not," the court rejected section IIB and III of the government's application for reduced minimization and wall standards.[107]

Preserving the FISA probable cause standard for primarily foreign intelligence investigations was a positive step towards protecting the rights of citizens. However, by failing to address the Department of Justice's allegation that the USA PATRIOT Act authorized the use of FISA for primarily criminal investigative purposes, the Court left the door open for further Department of Justice abuses of the FISA.[108]

Investigations Conducted by the FBI, OFFICE OF THE ATTORNEY GENERAL, (March 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html (last visited July 23, 2003) (making this assertion).

104. *In re All Matters*, (FISC May 17, 2002) at 9-11.

105. *Id.* at 9-10.

106. *Id.* at 12. Information is only minimized if it "*could not be* foreign intelligence." *Id.* Additionally, any information used in a prosecution, and the orders and applications associated with it, are largely inaccessible to the party being investigated. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1825(g) (2000). In particular, § 1825(g) states:

> In camera and ex parte review by district court . . . whenever any motion or request is made by an aggrieved person . . . to discover or obtain applications or orders or other materials relating to a physical search authorized by this subchapter . . . the United States district court . . . shall . . . review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, . . . only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

Id. As a result of this in camera and ex parte review of FISA warrants, it becomes difficult for a defendant to argue for suppression of evidence resulting from a FISA search. As seen above, the FBI has admitted to multiple misstatements and falsehoods in 75 different FISA warrant applications, making this provision exceptionally difficult to swallow. *In re All Matters*, (FISC May 17, 2002) at 16.

107. *In re All Matters*, (FISC May 17, 2002) at 22-23.

108. *Id.* at 6. The language of the Attorney General's memorandum is still open to abuse, as the court did not address the primary purpose issue. *Id.* The Attorney General's assertions are not directly supported by the text of the USA PATRIOT Act which states:

2. Dimming the Bright Line Between Criminal and Intelligence Investigations

The FISA, as amended by the USA PATRIOT Act, mandates a significant foreign intelligence purpose for a FISA application.[109] However, FISA also specifically states that the information sought must be foreign intelligence information.[110] The FISA definition section does not specifically include evidence of domestic crimes as foreign intelligence information.[111]

In its appellate brief to the Foreign Intelligence Surveillance Court of Review, the Department of Justice attempted to justify its reading of the USA PATRIOT Act's amendments to the FISA.[112] In particular, the Department of Justice argued that current minimization practices allow for intelligence investigators to disseminate information to criminal investigators.[113] However, the brief takes a dangerous misstep in logic in attempting to reverse this equation.[114] Allowing criminal investigators to use the lower FISA standard to obtain surveillance warrants effectively removes the protection of the Fourth Amendment.[115]

> Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer . . . . Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter . . . . (A) that the certifying official deems the information sought to be foreign intelligence information; (B) that a significant purpose of the surveillance is to obtain foreign intelligence information; (C) that such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(7) (2000).

109. 50 U.S.C. § 1804(a)(7) (2000).

110. *Id.* § 1804(a)(7)(D) (2000).

111. *Id.* § 1801(e) (2000).

112. Brief for the United States, In the United States Foreign Intelligence Surveillance Court of Review, (FISC Aug. 21, 2002) (No. 02-001), *available at* http://www.fas.org/irp/agency/doj/fisa/082102appeal.html (last visited July 24, 2003).

113. *Id.* The Government argued that this dissemination is distinctly codified in the FISA as a result of the USA PATRIOT Act. *Id.* The purpose behind allowing intelligence investigators to disseminate information to criminal investigators is to secure action against a terrorist or foreign agent without exposing national security issues. *Id.*

114. *Id.* The Government argues that there is "no constitutional basis for distinguishing between law enforcement efforts and other means of protecting this country against foreign spies and terrorists." *Id.* While allowing an intelligence investigator to refer a target to the criminal division for further investigation, appropriate minimization procedures can prevent a wholesale violation of Fourth Amendment rights. *Id.* However, allowing criminal investigators, who have a greater burden of proof to obtain surveillance warrants, to use the FISA burden of proof raises the specter of general warrants and writs of assistance as discussed in Justice Brandeis' dissent in *Olmstead*. *See Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting) (explaining the historical origins and reasoning behind the Fourth Amendment).

115. *See* Brief for the United States, *supra* note 112 (outlining the government's argument for invading the privacy of individuals in the name of national security). The Department of Justice argues that using the FISA to obtain evidence for a criminal prosecution could have a foreign intelligence purpose if the target is potentially a threat to national security. *Id.*

3. *Crossing the Line: The May 30, 2002 Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*

Thirteen days after the FISC rejected the March 6, 2002, application for new minimization procedures, the Department of Justice released revised Guidelines for the FBI's various investigative branches.[116] The USA PATRIOT Act indicated that racketeering enterprises may fall under the umbrella of terrorism enterprise investigations.[117] Additionally, the new Guidelines designate strategies for bringing investigations under the lower evidentiary standard required for terrorism investigations.[118]

While the Guidelines are aimed at prevention and early detection of a threat to national security, or the potential commission of a crime, the methods authorized for even a simple background check and information gathering are cause for concern. When dealing with a terrorism investigation, the Attorney General has given the FBI wide discretion in the methods it may use to gather information.[119] For instance, instead of browsing the World Wide Web as part of an investigation or inquiry, the FBI is now authorized to randomly search for evidence of a potential crime, regardless of whether it is a terrorist act.[120] Further, the FBI is authorized to attend any public gathering or place to monitor activities there, with the caveat that "[n]o information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity."[121] This caveat is dubious at best.

The Guidelines also extend the duration of a terrorism investigation to one year, renewable for up to a year at a time.[122] Investigations of all types may utilize any lawful methods, balancing the intrusiveness of those

116. Guidelines, *supra* note 17.

117. *Id.* at 3. The USA PATRIOT Act enumerates the various activities that constitute a federal crime of terrorism, including, but not limited to, possession of plastic explosives, arson and bombing of property used in interstate commerce, torture, and various associations with terrorist organizations. USA PATRIOT Act of 2001, 18 U.S.C. § 2332b(g)(5)(B) (2001).

118. Guidelines, *supra* note 17, at 4-5. Three triggers for a terrorism investigation are, "threats or advocacy of violence or other covered criminal acts," "apparent ability or intent to carry out violence or other covered activities," and "potential federal crime." *Id.* This proactive stance looks towards early prevention.

119. *Id.* at 18-23. These new Guidelines have raised flags amongst various civil liberties groups, such as the Center for Democracy and Technology. *See* Berman & Dempsey, *supra* note 3 (indicating that the decreased supervision of investigators, combined with intrusive methods and long term data-retention, threatens privacy rights).

120. Guidelines, *supra* note 17, at 22. *See also* Berman & Dempsey, *supra* note 3 (browsing the World Wide Web allows investigators to randomly search, without probable cause, to gather information that may or may not result in the detection of terrorist activity).

121. Guidelines, *supra* note 17, at 22. However, the elements of terrorist activity are to be viewed as a whole, giving a large amount of latitude to investigators. *Id.* at 4. The guidelines state that words and actions combined may create a terrorist threat that triggers the lower evidentiary standard. *Id.* Additionally, appearing ready and able to commit acts of violence can bring an individual under the terrorism umbrella. *Id.* at 5.

122. *Id.* at 17-18.

methods against the perceived threat.[123] Given the Ninth Circuit's opinion in *Konop*,[124] the scope of what might be considered a lawful method has expanded.

For instance, if all page loads from a secured web site are to be considered exempt from the protections of the ECPA[125] and the Wiretap Act,[126] then FBI agents can access those sites without a warrant. This loophole is apparent from that part of the new Guidelines where authorization is given to the FBI to "access online sites and forums as part of such research on the same terms and conditions as members of the public generally."[127]

Additionally, reasonable people might not want FBI agents secretly attending and monitoring their political, religious, or social functions. Part of the motivation for the Pennsylvania Bill of Rights, and our Fourth Amendment, was to prevent the squelching of political speech enacted via general warrants and writs of assistance.[128] While it is important to protect our nation from those who would harm it, a balance with civil rights must be forged.

III. OVERSIGHT AND UNIFORMITY–A POLICY PROPOSAL

This Proposal will address policy choices that should be made to ensure that the goals of national security are balanced against the privacy rights our nation seeks to protect. First, it will address the need for increased Congressional oversight of the Department of Justice and the FBI. Second, it will present the legislation and policy choices necessary to achieve the goal of increased oversight. Third, this Proposal will discuss the need for uniform definitions within the Wiretap Act[129] and the ECPA.[130]

A. Who Watches the Watchers? The Need For Congressional Oversight

In 1976, Attorney General Edward Levi drafted the precursor to the current Attorney General Guidelines,[131] the FBI Domestic Security Guidelines.[132] These Domestic Security Guidelines were a substitute for legislative regulation of the FBI.[133] Although it was never made part of the United States Code, it was understood that any revisions to these Guidelines would be "subject to prior Congressional review and public input."[134] The

123. *Id.* at 18.
124. *Konop*, 302 F.3d at 868.
125. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523 (2000).
126. The Wiretap Act of 1968, 18 U.S.C. §§2510-2523 (2000) (amended 1986).
127. Guidelines, *supra* note 17, at 22.
128. *See* STRUM, *supra* note 6, 8-10 (indicating various factors that contributed to the drafting of the Fourth Amendment).
129. 18 U.S.C. §§ 2510-2522 (2000) (amended 1986).
130. 18 U.S.C. §§ 2510-2522 (2000).
131. Guidelines, *supra* note 17.
132. *See* Berman & Dempsey, *supra* note 3 (describing how this initial set of Guidelines was amended and reissued by the Carter and the Reagan administration).
133. *Id.*
134. *Id.*

new FBI Guidelines released by Attorney General Ashcroft did not receive any such review.[135] While this breach of convention may have expedited the response to the attacks of September 11, 2001, the new Guidelines themselves were not released until May 30, 2002, thirteen days after the FISC opinion was decided.[136]

As shown above, the FBI admitted to seventy-five material omissions in FISA warrant applications in the past two years.[137] This fact was one of the reasons FISC gave for denying the Attorney General's request for less stringent minimization procedures.[138]

A recent development also accentuates the need for greater Congressional oversight. On November 19, 2002, the FBI admitted that it "lost control" over a list of individuals wanted for questioning after September 11, 2001.[139] The people listed were not suspects, nor were they explicitly linked to the terrorist attacks.[140] The main danger of the list being posted on various websites is that those postings are out of date, and threaten the privacy and reputations of those no longer on it.[141] The time to consider who watches the watchers has come.

B. Keeping The Fox Out Of The Henhouse: A Plan For Oversight

It is apparent that statutory solutions to the problems presented in this Comment are necessary. This section will describe some of the remedial methods available to Congress. Although the Judiciary can also play a role in safeguarding privacy rights, a Legislative solution is needed to give the Judiciary interpretive guidelines.

In its May 17th opinion, the FISC modified the Attorney General's proposal to return the portions relating to minimization and information sharing to its 1995 incarnation.[142] Since the FISC is the most experienced court that interprets the laws in question, its modifications should carry considerable weight when drafting appropriate legislation. To that end, Congress should adopt the 1995 guidelines, as augmented in January 2000 and August 2001, creating a new Act regulating the FBI.[143]

This new regulatory legislation should follow the historical intent of

---

135. *Id.*

136. Guidelines, *supra* note 17; *In re All Matters*, (FISC May 17, 2002). The short span of time between the May 17 opinion and the May 30 release of these Guidelines can also be seen as a direct response to FISC from the Attorney General's office. Notwithstanding this response, the Department of Justice nevertheless appealed FISC's decision. *Id.*

137. *In re All Matters*, (FISC May 17, 2002) at 16-17.

138. *Id.* at 18-19.

139. Kelli Arena, *U.S. Watch List Has 'Taken On Life Of Its Own,' FBI Says*, CNN, (November 20, 2002) *at* http://www.cnn.com/2002/LAW/11/19/fbi.watch.list/index.html (last visited July 24, 2003). This list, which was originally distributed to law enforcement agencies and select businesses, has spread via the Internet, among other carriers. *Id.*

140. *Id.*

141. *Id.* Various industries can now use this list to screen potential employees. *Id.*

142. *In re All Matters*, (FISC May 17, 2002) at 26-7.

143. *Id.* at 14-15.

our privacy rights,[144] and slow the erosion of Fourth Amendment rights.[145] This step is especially needed because the new Attorney General Guidelines constitute an end-run around the FISC opinion and modifications.[146] Since these Guidelines are essential to the lawful implementation of existing criminal and anti-terrorist statutes, the Constitution mandates that Congress enact legislation to ensure their proper execution.[147]

The augmented 1995 Guidelines[148] provide a less-intrusive solution to the issues presented by the Attorney General in his appellate brief to the FISC of Review.[149] In its opinion, the FISC outlines the elements of the 1995 Guidelines that effectively coordinate criminal and foreign intelligence investigators, while guaranteeing that proper minimization procedures are followed.[150] For example, they mandate that "reasonable indications of significant federal crimes" discovered during a FISA investigation are reported to criminal investigators.[151] However, the Guidelines forbid FISA investigations from being directed primarily to advance the goals of criminal investigators.[152]

In addition to enacting the FISC modifications into law, Congress should also add a provision mandating that future modifications be submitted to Congress, or a legislatively created administrative agency, at least ninety days in advance of implementation for review, comment, and public input.[153] To ensure compliance with this mandate, a section including remedial measures and emergency provisions is necessary. Remedies should take the form of "appropriations language limiting the implementation" of the

144. *See* STRUM, *supra* note 6, at 7-10 (describing the historical basis of the Fourth Amendment); *see also* Guidelines, *supra* note 17, at 21-22 (describing new Attorney General Guidelines regarding counter-terrorism activities that invoke the specter of general warrants, lowering the evidentiary standard for obtaining a warrant or wiretap across the board).

145. *See In re All Matters*, (FISC May 17, 2002) at 17 (detailing the erosion of Fourth Amendment protections resulting from "inaccurate FBI affidavits," and "misstatements in . . . FISA applications").

146. *See Guidelines*, *supra* note 17, at 17 (allowing the investigation of any individual only thought "likely" to be involved in supposedly "terrorist" activities).

147. U.S. CONST. art. I, § 8, cl. 18. The Necessary and Proper Clause gives Congress the power to, "make all Laws which shall be necessary and proper for carrying into Execution . . . all other Powers vested by this Constitution in the Government of the United States." *Id.* Therefore, in order to properly execute the Fourth Amendment, Congress must pass laws to balance the execution of its criminal and anti-terrorist statutes with this enumerated right.

148. *In Re All Matters*, (FISC May 17, 2002) at 14-15.

149. *See* Brief for the United States, *supra* note 112 (describing the Attorney General's desire for expanded powers of investigation under FISA).

150. *In Re All Matters*, (FISC May 17, 2002) at 14-15.

151. *Id.* at 14.

152. *Id.* at 14-15.

153. *See* Berman & Dempsey, *supra* note 3 (proposing increased congressional oversight of the FISA warrant process and the FBI's activities in general). This provision would enable Congress to stay abreast of the impact that investigative procedures would have on its constituents. Additionally, it would allow Congress time to draft further legislation amending the proposed Act to prevent future erosion of Fourth Amendment rights.

modified guidelines until they have been submitted for review,[154] and a refusal to expend funds "implementing any future changes in Attorney General Guidelines . . . unless such proposed guidelines have been transmitted to Congress for review."[155]

C. Solving the Problems of Statutory Interpretation

The dissenting opinion in *Konop* discusses the problematic and conflicting interpretations of "intercept" as it applies to electronic communications.[156] While this opinion discusses the law prior to the passage of the USA PATRIOT Act,[157] the issues presented are still applicable to this proposal.[158] If the precedent of the *Konop* majority is allowed to stand, a viable threat to Fourth Amendment protections exists.[159]

For instance, as the Internet proliferates, increasingly large numbers of people are communicating via stored electronic and wire communications. While it is not necessary to re-define what a stored communication is, it is necessary to ensure that what constitutes an "interception" within the meaning of the ECPA and the Wiretap Act is uniform for both wired and electronic communications.[160] If the current interpretations are applied, the privacy rights of all Internet users will be severely compromised.

To prevent this severe erosion of the Fourth Amendment, Congress should amend the pertinent statutes to specifically include stored electronic and wire communications within the list of communications that can be intercepted. As technology has advanced, the methods used to store wire and electronic communications have become "technologically equivalent."[161] A clear statutory statement indicating an intention to protect the "access to" and "acquisition of" stored electronic communications would prevent further misinterpretations of the ECPA and Wiretap Act.[162]

---

154. *Id.*

155. *Id.*; *see also* U.S. CONST. art. I, § 8, cl. 1 (describing the power of Congress to "lay and collect Taxes"). When combined with the Necessary and Proper Clause, it is clear that Congress possesses the power to refuse to allocate funds, as well as the power to allocate them. U.S. CONST. art. I, § 8, cl. 18.

156. *Konop*, 302 F.3d at 887-88 (Reinhardt, J., dissenting).

157. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18, 28, and 50 U.S.C.).

158. *See Konop*, 302 F.3d at 887-88 (Reinhardt, J., dissenting) (discussing the interception and investigation of stored electronic information).

159. *See id.* at 890 (discussing the fears computer operators may have about the confidentiality of their private communications). Taken in conjunction with the Attorney General Guidelines not modified by FISC, all stored wire and electronic communications would be exempt from the warrant requirements of the ECPA and the Wiretap Act. *See* Guidelines, *supra* note 17, at 22 (describing the freedom investigators would have to use online resources in their investigations).

160. *See Konop*, 302 F.3d at 887-88 (Reinhardt, J., dissenting) (indicating that this term's statutory meaning has not been firmly established by the courts). Justice Reinhardt's dissent points out that the varying definitions of "interception" "have rendered the intercept prohibition . . . meaningless." *Id.* at 887.

161. *Id.* at 888. Justice Reinhardt continues on to discuss the legislative intent behind the ECPA and the Wiretap Act. *Id.* at 888-91.

162. *Id.* at 889.

The protection of privacy rights is a constant balancing act that deserves the utmost vigilance. In addition to the proposal contained in this Comment, other initiatives can be offered to further protect privacy rights.[163]

IV. CONCLUSION

The attacks on September 11, 2001 shocked the country. The Executive Branch, whose duty it is to enforce the laws of the Nation,[164] must temper its zeal to protect the nation with a commitment to protect the rights of the People. However, without participation by all three branches of government, this goal becomes difficult to achieve.

The reasonable expectation of privacy first posited by Justice Brandeis,[165] and later refined by the *Katz* Court,[166] must be maintained, regardless of the proliferation of investigative technologies. Balancing privacy and national security is a difficult job. However, those accepting the responsibility of this balancing act must always be vigilant to prevent a permanent and destructive erosion of privacy rights. Our nation cannot lose sight of the freedoms it seeks to protect.

163. For instance, in order to prevent abuse of FISA's in camera, ex parte consideration of wiretap and warrant requests, Congress could appoint special Federal Defense attorneys, with the security clearance to review and contest the warrants should a criminal proceeding be brought against the target of an investigation. *See also* Podesta & Swire, *supra* note 76 (describing the pitfalls of the current system of review for FISA warrants, and proposing a "Committee on Privacy, Personal Liberty and Homeland Security"). However, this becomes an issue of criminal procedure and due process, which is beyond the scope of this Comment.

164. U.S. CONST. art. II, § 1, cl. 1. "The executive Power shall be vested in a President of the United States of America." *Id.* Possessing the power to execute the Laws, the Executive also takes an oath to uphold the Constitution. *Id.* at art. II, § 8. "[H]e shall take the following Oath or Affirmation: "I do solemnly swear (or affirm) that I . . . will to the best of my Ability, preserve, protect, and defend the Constitution of the United States." *Id.*

165. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting). "[Every] unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." *Id.*

166. *See Katz*, 389 U.S. at 361 (Harlan J., concurring) (indicating that the Fourth Amendment extends to the individual via a reasonable expectation of privacy).