The Protect America Act: One Nation under Surveillance

Shahab Mossavar-Rahmani

Recommended Citation
THE PROTECT AMERICA ACT: ONE NATION UNDER GOD SURVEILLANCE

I. INTRODUCTION

Early in the morning on December 16, 2005, people across the United States awoke to the smell of freshly brewed coffee and learned that their own government had been spying on them for over three years. A *New York Times* (Times) article revealed that President George W. Bush authorized a secret wiretapping program for the National Security Agency (NSA) in the months following the September 11, 2001 (9/11) terrorist attacks. Current and former officials from the Bush Administration discussed the story with journalists from the *Times* because these officials had legitimate concerns about the legality and oversight of the operation.

According to the *Times* article, “the intelligence agency had monitored the international telephone calls . . . of hundreds, perhaps thousands, of people inside the United States without warrants” and eavesdropped “on up to 500 people in the United States at any given time.”

In the weeks and months following the publication of the *Times* article, the Bush Administration conducted damage control, often appearing in the media to assert the program’s legality. The Bush Administration even claimed that domestic surveillance was *necessary* to combat terrorism (although this argument has not been frequently

---

2. Id.
3. Id.
4. Id.
asserted). The United States Department of Justice (DOJ) asserted two legal foundations to support the President’s authorization of the NSA program: (1) an inherent constitutional power and (2) an express power granted by Congress when it enacted the Authorization for Use of Military Force (AUMF) to combat terrorism.7

A mere eight days after it first exposed the NSA program, the Times published another article revealing that the NSA was able to monitor and gather information on millions of people because it gained the cooperation of major American telecommunications companies.8 The Times reported that these companies allowed the NSA “to obtain backdoor access to streams of domestic and international communications . . . .”9 Soon after the Times published the article, civil liberties groups flooded companies like AT&T and Verizon with lawsuits. One such group, the Electronic Frontier Foundation (EFF), alleged that AT&T had “opened its key telecommunications facilities and databases to direct access by the NSA and/or other government agencies, intercepting and disclosing to the government the contents of its customers’ communications as well as detailed communications records about millions of its customers . . . .”10 Based on the value of the claims asserted, these companies faced potential bankruptcy if left to fend for themselves.11 Initially, the Bush Administration intervened in these suits by asserting the state secrets privilege.12 Sometimes referred to as the “nuclear bomb of legal tactics,”13 the state secrets privilege effectively prevents any disclosure of evidence that the government deems a threat to national security.14 However, the

9. Id.
Bush Administration sought a more permanent solution\textsuperscript{15} after one federal court declined to apply the privilege,\textsuperscript{16} and another federal court held that the NSA violated the Constitution.\textsuperscript{17}

The ironically titled Protect America Act of 2007 (PAA)\textsuperscript{18} is the focus of the ongoing debate on whether the Bush Administration sacrificed individuals’ fundamental liberties in exchange for domestic security.\textsuperscript{19} The PAA amended the Foreign Intelligence Surveillance Act of 1978 (FISA),\textsuperscript{20} and effectively removed the system of checks and balances on the Executive Branch’s authority to wiretap international phone calls.\textsuperscript{21} Conveniently, the PAA also included an immunity provision that shielded telecommunications companies from any future lawsuits.\textsuperscript{22} Because the provision only granted immunity from future suits, the Bush Administration continued to publicly condemn Congress’ resistance to a retroactive application of the immunity provision.\textsuperscript{23} Congress eventually passed the FISA Amendments Act of 2008 (FAA), which includes a retroactive immunity clause.\textsuperscript{24}

On one hand, proponents such as Mike McConnell, Director of National Intelligence, argue that the PAA is vital to early detection of terrorist plots, and that “our intelligence professionals [are] ‘missing a significant amount of foreign intelligence’” without the legislation.\textsuperscript{25} On the other hand, critics, such as the American Civil Liberties Union

\begin{itemize}
  \item \textsuperscript{15}Press Release, Office of the Press Sec’y, Fact Sheet: Congress Must Act Now to Keep a Critical Intelligence Gap Closed (Jan. 22, 2008), http://www.whitehouse.gov/news/releases/2008/01/20080122-2.html.
  \item \textsuperscript{16}John Markoff, \textit{Judge Declines to Dismiss Privacy Suit Against AT&T}, \textit{N.Y. TIMES}, July 21, 2006, at A13.
  \item \textsuperscript{17}ACLU v. NSA, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006).
  \item \textsuperscript{19}See Risen & Lichtblau, supra note 1.
  \item \textsuperscript{21}American Civil Liberties Union, \textit{ACLU Fact Sheet on the “Police America Act”}, http://www.aclu.org/safefree/nsaspying/31203res20070807.html (last visited Sept. 14, 2007) [hereinafter Fact Sheet].
\end{itemize}
(ACLU), argue that the legislation allows for a massive collection of data without any oversight by the courts or Congress.26 Some Democrats, like Senator Russ Feingold of Wisconsin, claimed that the passage of the PAA was politically motivated27 because Democrats faced their first election year in 2008 after they gained control of Congress in 2006. One political commentator seemed to agree with Feingold's assessment when he claimed that Democrats feared "appearing weak on national security issues" and wanted to avoid spending the August recess defending themselves from Republican accusations that they "left Americans exposed to threats."28 As one Internet blogger wrote, "the Democrats can rest easily over the August recess, knowing that they haven’t left themselves vulnerable to political attacks. The rest of us can worry about whether the NSA is using its enhanced surveillance authority to spy on Americans."29

This Comment examines the scope of the PAA, the legality of telecommunications companies' participation, and the possible ramifications of passing such controversial legislation. The NSA program and cooperation of major telecommunications companies are eerily similar to the events that gave rise to FISA in 1978.30 The recurrence of these issues is forcing a new generation of Americans to find a balance between the security of the country and the protection of civil liberties.31 Although the Bush Administration believed it was protecting the nation with these laws,32 scholars argued that this type of legislation actually supports the goals terrorists seek to achieve.33 Terrorists use attacks like the ones on 9/11 as a tool to "influence the decisions of the government and the opinion of the population."34 While some experts disagree on the true objectives of

31. Id.
34. Id. at 1996.
any terrorist group, they cannot deny that terrorism has profoundly affected the diminution of Americans' civil liberties.35

Part II of this Comment discusses the legislative background of the current law and the collateral effect of the involvement of telecommunications companies, including a comparison between the events leading up to the passage of FISA and those leading up to the passage of the PAA. This section also examines how the exposure of the NSA's warrantless wiretapping program created two substantial setbacks in the government's terrorism prevention strategy, and how the PAA solved both problems. Part III examines the significance and legality of participation by telecommunications companies, and analyzes the legislative efforts to safeguard those companies from liability. This section also analyzes the potential for government abuse under the PAA given its vague language. Part III also weighs the benefits of such laws against the civil liberties that are compromised. Part IV highlights the subsequent enactment of the FISA Amendments Act of 2008 and concludes that both pieces of legislation compromised constitutionally guaranteed rights in exchange for the illusion of domestic security.

II. BACKGROUND

A. Hersh, Church, and Cheney

From late 1974 through 1975, journalist Seymour Hersh wrote a series of stories in the New York Times (Times), reporting that the FBI and CIA were conducting illegal intelligence operations on tens of thousands of Americans.36 Hersh also reported that the government was conducting illegal wiretaps on the Soviet Union inside its three-mile territorial limit.37

These explosive revelations spurred the Senate to form the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.38 The "Church Committee," which

35. See id. at 1997 (presenting arguments of Jean-Francois Gayraud, David Senat, and others that international mass terrorism does not have a political goal, other than the destruction of the political sphere); but see ROBERT E. GOODIN, WHAT'S WRONG WITH TERRORISM? 49 (2006) (arguing that terrorism is "a political tactic, involving the deliberate frightening of people for political advantage").
37. Id. at 34.
derived its name from its chairman, Senator Frank Church, found that both the National Security Agency (NSA) and the Executive Branch had enlisted the help of AT&T and Western Union to aid in the wiretapping program. These companies provided access to almost all communications between American citizens and people in foreign countries. At the program’s peak, the government was reviewing 150,000 messages per month, all without a single warrant. When the House of Representatives attempted to subpoena records from AT&T, the Ford Administration intervened, stating that “the American Telephone and Telegraph Company was and is an agent of the United States acting under contract with the Executive Branch.”

While Republicans complained of national security issues, Democrats talked of the dangers to civil liberties. Edward H. Levi, the Attorney General at the time, even argued that “courts had upheld the [P]resident’s power to order surveillance for foreign intelligence without warrants.”

As Chief of Staff and Secretary of Defense, respectively, Dick Cheney and Donald Rumsfeld successfully encouraged President Gerald Ford to extend the “state secrets doctrine” to the embroiled telecommunications companies, shielding them from testifying publicly. Mr. Cheney and Mr. Rumsfeld also reviewed various legislative proposals based on the results of the Church Committee’s reports. Not surprisingly, despite the reports’ publication in 1976, prescriptive legislation on government eavesdropping was not adopted until the administration of Democrat Jimmy Carter in 1978.

With its enactment, the Foreign Intelligence Surveillance Act of 1978

39. Id.
41. DUBOSE & BERNSTEIN, supra note 36, at 36.
42. Id.
43. Id.
44. Id.
45. Shane, supra note 30.
46. Id.
48. DUBOSE & BERNSTEIN, supra note 36, at 23, 32 (explaining that while Dick Cheney served as Deputy Chief of Staff and Donald Rumsfeld served as Chief of Staff, neither appeared to be in favor of judicial oversight of electronic surveillance).
49. Id. at 37.
(FISA) struck a balance between the preservation of individual liberty and the Executive Branch’s ability to “protect the nation from security threats.” But FISA was more than just a limit on government power since it was specifically written “to restrain how telecoms cooperate with Government spying requests.” According to Cindy Cohn, Legal Director for the Electronic Frontier Foundation (EFF), since Congress knew preventing the government from eavesdropping was not enough to protect Americans’ civil liberties, “[it] had to create an independent duty for the telecom carrier[s] not to participate in illegal surveillance.” In other words, the telecommunications companies were “forbidden from handing over [their] communications and communications records to the Government without proper legal process.” Congress included this prohibition in FISA, in part, because the Church Committee’s final report revealed the complete lack of structure and oversight for eavesdropping and exposed just how vulnerable Americans were.

The Church Committee found that the companies essentially provided unfettered access to all international communications and allowed the NSA to sort through and determine which messages would be reviewed. For example, the final report stated that ITT World Communications (ITT) allowed “access to all incoming, outgoing, and transiting messages.” Additionally, the Church Committee found that the government recorded and developed all traffic before being returned to the company. Even more chilling was the report’s revelation that, aside from members of the NSA and a select few in the Truman Administration, no government official knew of the program’s existence, ostensibly indicating that the program lacked judicial and congressional oversight.

During congressional hearings on FISA, a representative of the American Privacy Foundation stated that two major telecommunications companies, RCA and ITT, had provided all of their customer

53. Id.
55. Id.
56. Id.
57. Id.
58. Id.
communications to the NSA from 1945 to 1975. He also stated that "[a]s long as [the NSA’s] activities remain essentially uncontrolled and cloaked in undue secrecy, Americans cannot be certain that their privacy is not being silently invaded."60

The practical effect of FISA was that, instead of the NSA soliciting telecommunications companies for unregulated access to private information, it now must apply for a FISA warrant through a two-part process. First, the federal officer applying for the warrant must submit "an application signed by a [Department of Justice (DOJ)] attorney" along with a signed affidavit by either an NSA or FBI official. The affidavit must contain facts that establish "probable cause to believe that... the target of the electronic surveillance is a foreign [government or agent]." Second, a high-ranking Executive Branch official must sign a certification, which states in part "that the certifying official deems the information sought to be foreign intelligence information" that the government needs. Once completed, the federal officer must file the warrant application with the FISA court, which is responsible for reviewing the warrant applications. The court is composed of eleven district judges, each of which serves a one-time, seven-year term. There is also a court of review, composed of three court of appeals or district court judges. The Chief Justice of the U.S. Supreme Court appoints all of the judges.

Fast-forward to the year 2001, a mere seven days after the attacks on September 11 (9/11), Congress granted President George W. Bush the Authorization for Use of Military Force (AUMF). The AUMF authorized


60. Id.

61. Leslie Cauley, NSA has Massive Database of Americans’ Phone Calls, USA TODAY, May 11, 2006, at IA.


63. Id.


65. Kris, supra note 62.


67. Id. § 1803.

68. Id. § 1803(a)(1).

69. Id. § 1803(d).

70. Id. § 1803(b).

71. Id. § 1803(a)–(b).

the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks . . . in order to prevent any future acts of international terrorism . . . ." 73 During AUMF debates in the United States Senate, Democrat Patrick Leahy of Vermont reassured Americans by stating: "We will maintain our democracy, and with justice, we will use our strength. We will not lose our commitment to the rule of law, no matter how much the provocation, because that rule of law has protected us throughout the centuries. It has created our democracy." 74 Despite Senator Leahy's reassurances, the hastily enacted AUMF was the cornerstone of every legal justification for the Bush Administration's actions with respect to warrantless surveillance. 75

Perhaps the most widely known piece of legislation passed by Congress since 9/11 is the USA PATRIOT Act of 2001 (Patriot Act), which came only thirty-eight days after the AUMF, and amended FISA in two important ways. 76 First, under section 206, the Patriot Act abolished the need for federal officials to seek a warrant for each communication device that a suspect was using. 77 Instead it "allows a single wiretap to legally 'roam' from device to device, to tap the person rather than the phone." 78 Second, under section 218, collecting intelligence information on a suspect no longer had to be "the purpose" of the investigation; it just has to be "a significant purpose." 79

The NSA's program involves massive amounts of data collection 80 with scarcely any oversight or accountability. 81 When asked about telecommunications companies' cooperation with the NSA program, one technology expert stated that the NSA has the "capability of an enormous vacuum operation to sweep up data." 82 Conversely, if the government knows a terrorist's identity or uncovers that an individual conducted some

73. Id.
76. See, e.g., DOJ WHITEPAPER, supra note 7, at 1–3.
79. Id. at 3, 7 (emphasis added).
80. Cauley, supra note 61.
81. Risen & Lichtblau, supra note 1.
82. Lichtblau & Risen, Spy Agency, supra note 8.
type of illegal activity, then perhaps additional surveillance to ascertain their whereabouts would be justified. Instead, the Bush Administration weakened the requirements for conducting surveillance on Americans without justifying why it targeted certain individuals.83

Even more disconcerting is the fact that, according to national security and telecommunications experts, “even if the NSA seeks to adhere closely to the rules that Mr. Bush has set, the logistics of the program may make it difficult to ensure that the rules are being followed.”84 Robert Morris, a former NSA scientist, stated that the complication arises because it is difficult to determine where a call begins and ends, especially with roaming cell phones and voice-over-Internet technology.85 With the rise of digital and computerized systems, even basic concepts such as how communications get from origin to destination have changed.86 Instead of taking the shortest direct route to a destination, “[c]omputerized systems determine the most efficient routes for digital ‘packets’ of electronic communications depending on the speed and congestion on the networks.”87 Consequently, “switches carrying calls from Cleveland to Chicago, for example, may also be carrying calls from Islamabad to Jakarta.”88 As a result, in order to effectively monitor communications, the NSA must check nearly every voice communication that passes through the United States to ensure that it gets all domestic to foreign traffic, and vice versa.89

B. History Repeats Itself

Even before the dust settled at Ground Zero after the 9/11 terrorist attacks, Congress granted President Bush broad powers to address the terrorist threat in the name of domestic security.90 Therefore, when the NSA was at the center of a wiretapping scandal involving American

83. Podesta, supra note 78, at 3, 7.
85. Id.
87. Id. at 50.
88. Id.
89. Id. at 49–50.
citizens, the Bush Administration quickly asserted its legal authority to determine the validity of the program.\textsuperscript{91} Some Republicans complained of the need to modernize intelligence-gathering methods, while Democrats, like House Representative Adam Schiff of California, tried to introduce legislation to block financing of the NSA program.\textsuperscript{92} Dick Cheney, emboldened by his status as Vice President, stated that, with regard to FISA, "[t]he [P]resident of the United States needs to have his constitutional powers unimpaired... in terms of the conduct of national security policy."\textsuperscript{93} Vice President Cheney also stated that the DOJ repeatedly reviewed the program to ensure its constitutionality and the constitutionality of the Patriot Act—sentiments echoed by then-serving Attorney General Alberto Gonzales.\textsuperscript{95}

According to DOJ attorneys, the primary basis for this presidential power is in the Constitution.\textsuperscript{96} Courts have broadly construed the President’s power as Commander-in-Chief, empowering the President to defend the nation and its citizens.\textsuperscript{97} In United States v. Curtiss-Wright Export Corp., the Supreme Court held that the President is the "sole organ of the federal government in the field of international relations."\textsuperscript{98} Therefore, DOJ attorneys argued that the President’s power to create the NSA program stemmed from his inherent constitutional power to act against foreign powers during a time of war.\textsuperscript{99}

The second basis under which President Bush claimed to derive the power to order warrantless surveillance came from authority granted to him under the AUMF.\textsuperscript{100} The AUMF was the cornerstone of the Bush Administration’s justification for the surveillance program because it

\textsuperscript{91} See DOJ WHITEPAPER, supra note 7, at 6–7 (explaining the DOJ’s oversight and analysis of the legal basis for the NSA activities described by the President).

\textsuperscript{92} Eric Lichtblau, Critics of Wiretapping Oppose a Plan for a Decision on the Program by a Secret Court, N.Y. TIMES, July 15, 2006, at A10.

\textsuperscript{93} Shane, supra note 30.


\textsuperscript{95} Eric Lichtblau, Gonzales Invokes Actions of Other Presidents in Defense of U.S. Spying, N.Y. TIMES, Jan. 25, 2006, at A19.

\textsuperscript{96} DOJ WHITEPAPER, supra note 7, at 1, 6.

\textsuperscript{97} See JOHN YOO, WAR BY OTHER MEANS: AN INSIDER’S ACCOUNT OF THE WAR ON TERROR 103 (2006).


\textsuperscript{99} See DOJ WHITEPAPER, supra note 7, at 1, 6 (explaining that the president had such powers and his actions were constitutional); but see Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 579 (1952) (holding that the president did not have constitutional authority to seize steel mills during a nationwide strike of steelworkers that jeopardized national defense).

\textsuperscript{100} DOJ WHITEPAPER, supra note 7, at 2.
specifically authorized the President to "use all necessary and appropriate force" to prevent "any future acts of international terrorism against the United States." DOJ attorneys under the Bush Administration also claimed that presidential action under AUMF satisfied the statutory exception clause in FISA, which states that a person is guilty of violating FISA if he or she engages in electronic surveillance, unless that surveillance is expressly authorized by statute. Accordingly, President Bush claimed that he followed FISA requirements when he created the NSA program.

Finally, under Justice Jackson's oft-cited "tripartite framework" from the Court's 1952 plurality decision in Youngstown Sheet & Tube Co. v. Sawyer, the Bush Administration asserted that President Bush was actually at the "zenith" of his powers because he acted with congressional approval via AUMF. In his concurring opinion in Youngstown, Justice Jackson established the judicial framework that determines the President's inherent emergency powers based on the level of congressional acquiescence. The President is authorized to act as long as Congress has either approved the action or remained silent on the issue. Conversely, if the President acts against the express or implied will of Congress, then "he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."

At first blush, the arguments set forth by the DOJ attorneys for the Bush Administration appeared to be based upon sound legal precedent and backed by congressional approval. But a closer look at the Bush Administration's legal reasoning reveals unfounded assumptions and circular logic. There are three flaws with the arguments set forth: first, the President's inherent constitutional powers cannot be used to conduct

102. DOJ WHITEPAPER, supra note 7, at 17–18.
104. DOJ WHITEPAPER, supra note 7, at 17.
106. DOJ WHITEPAPER, supra note 7, at 2, 11.
108. Id. at 635–37.
109. Id. at 637.
electronic surveillance on American citizens domestically; second, the Senate did not intend to support a domestic warrantless wiretapping program when it passed the AUMF; and third, the program violated FISA.

Although the Bush Administration correctly argued that the President’s power is inherent in the Constitution, such a power only applies in the context of foreign surveillance. Nevertheless, former Attorney General Alberto Gonzales and other members of the Bush Administration admitted that there had been instances of domestic spying. Commentators suggested that the Constitution did not grant the President the authority to enact programs that spy on Americans. In fact, past presidential abuse is one of the main reasons why FISA was enacted. When the Church Committee gave its final report to Congress, revelations of domestic wiretapping by the Nixon Administration led Congress to pass legislation to limit such surveillance actions. Moreover, in drafting FISA, Congress stated that its intention was to “circumscribe any claim of inherent presidential authority to conduct electronic surveillance . . . .” In fact, language that specifically recognized such inherent presidential authority was deleted from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), a law that set rules for obtaining

110. See Neff, supra note 50, at 908–10.
112. Although the district court initially found the program in violation of FISA, on appeal the Sixth Circuit reversed because the plaintiffs failed to show that the “NSA’s surveillance program include[s] the sort of conduct that would satisfy FISA’s definition of ‘electronic surveillance’ . . . .” ACLU v. NSA, 493 F.3d 644, 682 (6th Cir. 2007). While the Sixth Circuit’s decision was particular to the plaintiffs, the district court’s decision focused on the underlying statutory policy. See Adam Liptak & Eric Lichtblau, U.S. Judge Finds Wiretap Actions Violate the Law, N.Y. TIMES, Aug. 18, 2006, at A1. It is on this broader basis the author asserts the illegality of the NSA program with respect to FISA.
113. See Neff, supra note 50, at 904–10.
114. See, e.g., Norris, supra note 6; Risen & Lichtblau, supra note 1.
116. See Neff, supra note 50, at 914.
117. Id. (stating that “[t]he legislative history of FISA reveals that the statute’s purpose was to balance concerns about the presidential abuse of power through unilateral determination[s] of when national security justifies domestic spying against the need for the legitimate use of electronic surveillance to obtain foreign intelligence information”); see also Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Attorneys, Am. Law Div., Cong. Research Serv., Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information 13 (Jan. 5, 2006), available at http://www.fas.org/sgp/crs/intel/m010506.pdf [hereinafter Bazan & Elsea].
118. Bazan & Elsea, supra note 117, at 27.
wiretaps within the United States.\textsuperscript{119}

The Bush Administration also asserted that the President acted at his zenith of power because Congress supported the NSA program when it enacted the AUMF.\textsuperscript{120} However, this argument was also flawed. Under the third category of Justice Jackson's framework in \textit{Youngstown}, the President cannot utilize his inherent powers if his actions expressly or inherently conflict with the will of Congress.\textsuperscript{121} In response to the Bush Administration’s continued reliance on the AUMF as justification for the program, members of the Senate passed Resolution 350 on January 20, 2006.\textsuperscript{122} The resolution stated that the Senate did not authorize warrantless domestic surveillance of United States citizens when it voted to enact the AUMF.\textsuperscript{123} Upon the passage of Resolution 350, Senator Leahy condemned the program, stating that “[t]he Framers built checks and balances into our system specifically to counter such abuses and undue assertions of power . . . Once lost or eroded, liberty is difficult if not impossible to restore.”\textsuperscript{124} Therefore, under the third category from \textit{Youngstown}, the President had no inherent constitutional authority to create the NSA program because he acted in the face of congressional disapproval. Although this one-house resolution did not have a legal effect on the previously enacted law, it implied that the President essentially created his inherent authority by interpreting the language in AUMF to authorize the NSA program.\textsuperscript{125}

The third flaw in the Bush Administration’s reasoning was that the program completely disregards the congressionally approved procedures set forth under FISA. Attorneys from the Congressional Research Service (CRS) contended that the AUMF did not give the President power to authorize the NSA program because Congress expressly stated that FISA and Title III should be “the exclusive means by which electronic surveillance . . . may be conducted.”\textsuperscript{126} Without the AUMF to satisfy the statutory exception clause within FISA, the exception can no longer apply. Therefore, the Bush Administration unjustly ignored a federal law that specifically deals with wiretapping regulations.\textsuperscript{127} Former Attorney General Alberto Gonzales acknowledged that he was well aware the Bush

\begin{itemize}
  \item 120. DOJ WHITEPAPER, supra note 7, at 17.
  \item 121. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952).
  \item 123. Id.
  \item 124. Id.
  \item 125. Id.
  \item 126. Bazan & Elsea, supra note 117, at 15.
  \item 127. See Neff, supra note 50, at 901–02.
\end{itemize}
Administration was legally bound to follow FISA, stating “[w]e have had discussions with Congress in the past . . . as to whether or not FISA could be amended to allow us to adequately deal with this kind of threat, and we were advised that that would be difficult, if not impossible.” Realizing that the ratification of amendments to FISA was unlikely, the Bush Administration circumvented the statute by asserting executive power under AUMF. The statute did not provide an adequate legal basis for the President to create a warrantless surveillance program, yet he did just that.

III. TELECOM IMMUNITY

A. The Threat of Checks and Balances

Along with the legal challenges discussed in Part II above, the New York Times’ (Times) exposure of the National Security Agency (NSA) wiretapping program also created a wave of lawsuits against both the NSA and major telecommunications companies that assisted the Bush Administration. The first cases came less than a month after the Times article exposed the hidden program. However, unlike the companies at the center of the Church Committee investigations in the 1970s, the companies implicated in the NSA scandal did not appear to have any guaranteed immunity. Perhaps even more alarming, at least for AT&T, was the defection of former employees who had inside knowledge of the program and were willing to testify.

In Hepting v. AT&T Corp., one of the first major suits filed against AT&T, the Electronic Frontier Foundation (EFF) asserted that companies like AT&T made the NSA program possible and that they should not simply succumb to the will of the President. According to Mark Klein, a

128. Gonzales & Hayden, supra note 5.
129. See id.
130. See id.
132. See, e.g., Hepting, 439 F. Supp. 2d at 974.
133. See Snider, supra note 40.
134. See John Markoff & Scott Shane, Documents Show Link Between AT&T and Agency in Eavesdropping Case, N.Y. TIMES, Apr. 13, 2006, at A17.
witness and former AT&T technician, AT&T created a special room in its San Francisco facility to be supervised by the NSA. AT&T used a device called a “splitter” to make a copy of all Internet activity and emails from customers, and then diverted the information to the NSA room. AT&T used equipment inside this room to analyze contents and traffic patterns of communications. Mr. Klein also testified that only people with NSA clearance had access to the room. The EFF eventually obtained evidence of at least fifteen of these sites, meaning “probably well over half of AT&T’s purely domestic traffic was diverted to the NSA.”

In response, the government asserted the “state secrets privilege,” a legal doctrine that excludes evidence based on the government’s assertion that revealing such evidence may endanger national security. As constitutional law and civil rights attorney, Glenn Greenwald, stated, “[o]ne of the odd—and dangerous—features of this privilege doctrine is that, in many cases, courts allow the Government to assert the privilege without even submitting the documents in question to a judge for the judge to review in secrecy . . . .” This means that the “Executive Branch can decree that the documents should not be disclosed because disclosure will harm national security,” and it is usually “blindly accepted without anyone reviewing its truthfulness or propriety.” From the time the privilege was created in 1953, until 1976, it was invoked a grand total of four times. After the September 11, 2001 (9/11) attacks, the Bush Administration invoked the privilege a whopping twenty-three times, five of those in 2006 alone.

The first major legal blow to the Bush Administration on the surveillance issue came in July 2006 when Judge Vaughn Walker of the

137. Id.
138. Id.
139. Id.
140. Id.
141. See Markoff & Shane, supra note 134; see also Lyons, supra note 14.
143. Id.
144. See United States v. Reynolds, 345 U.S. 1, 6 (1953).
146. Id.
Northern District of California denied both the government’s state secrecy claim and AT&T’s immunity claim in *Hepting*.\(^{147}\) In rejecting the secrecy claim, Judge Walker stated that “[b]ecause of the public disclosures by the government and AT&T, the court cannot conclude that merely maintaining this action creates a ‘reasonable danger’ of harming national security.”\(^{148}\) The court also denied AT&T’s motion to dismiss.\(^{149}\) The motion was based in part on AT&T’s assertion that “telecommunications providers are immune from suit if they receive a government certification authorizing them to conduct electronic surveillance.”\(^{150}\) AT&T further asserted that the burden rests upon the EFF, as the plaintiff, to plead that AT&T lacks such certification.\(^{151}\) The court cleverly skirted this issue stating that it “need not decide whether plaintiffs must plead affirmatively the absence of a certification because the present complaint, liberally construed, alleges that AT&T acted outside the scope of any government certification it might have received.”\(^{152}\)

AT&T also contended that the complaint should be dismissed because the EFF failed to plead the absence of AT&T’s common law immunity.\(^{153}\) AT&T asserted that its immunity “grew out of recognition that telecommunications carriers should not be subject to civil liability for cooperating with government officials conducting surveillance activities. That is true whether or not the surveillance was lawful.”\(^{154}\) Again, the court rejected this argument, stating that application of such immunity would undermine the language of the Foreign Intelligence Surveillance Act of 1978’s (FISA) certification provision.\(^{155}\) Specifically, the certification provision requires authorized written certification from a government official.\(^{156}\) Therefore, applying this common law immunity would “in essence be nullifying the procedural requirements of that statutory provision . . . .”\(^{157}\)

Although the EFF prevailed in the lower court, AT&T appealed the case to the Ninth Circuit, which released a two sentence order stating: “In light of the FISA Amendments Act of 2008, Pub. L. No. 110-

---

147. See *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 1006, 1010–11 (N.D. Cal. 2006); see also Markoff, *Judge Declines*, supra note 16.


149. *Id.* at 1011.

150. *Id.* at 1001.

151. *Id.*

152. *Id.* at 1002.

153. *Id.* at 1003.


155. *Id.* at 1005–06.

156. *Id.*

157. *Id.* at 1006.
261, we remand this case to the district court. We retain jurisdiction over any further appeals.”

Cindy Cohn, Legal Director for the EFF, hailed the decision as a victory because it affirmed that the government must verify the participation of specific companies in the NSA program in order to establish immunity under the FISA Amendments Act of 2008 (FAA). Accordingly, the government may no longer claim that a particular company’s participation in the NSA program is a state secret. Thus, if the retroactive immunity provision of the FAA is later struck down, the forfeiture of the state secrets doctrine leaves open the opportunity for a renewed suit.

However, the Bush Administration was able to successfully assert the state secrets privilege in *Terkel v. AT&T Corp.* The major distinction between *Hepting* and *Terkel* is that, in the former, the plaintiffs challenged “the interception of the contents of communications,” whereas the plaintiffs in the latter limited their challenge to “the alleged disclosure of records regarding customer communications.” In *Hepting*, Judge Walker noted Attorney General Gonzales' public statement that the government intercepted communications where one party to the communication was outside the United States and the government reasonably believed one party was a suspected terrorist, regardless of whether the other party was in the United States. Due to this acknowledgment, the state secrets privilege could bar a claim that an interception of the contents of communications occurred; simply put, it was no longer a secret. In contrast, the plaintiffs in *Terkel* conceded that no Executive Branch official had “officially confirmed or denied the existence of any program to obtain large quantities of customer telephone records . . . .” Since neither AT&T nor the government confirmed or denied the allegations that AT&T disclosed records, the court held that the government’s assertion of the state

---

158. Order in Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (9th Cir. 2008) (No. 06-17137).
160. Opposition of Plaintiffs-Appellees to the Government’s Motion to Hold Appeals in Abeyance and Plaintiffs-Appellees’ Cross-Motion to Dismiss the Appeals at 9–10, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (9th Cir. 2008) (Nos. 06-17132, 06-17137).
161. Singel, supra note 159.
162. Terkel v. AT&T Corp., 441 F. Supp. 2d 899 (N.D. Ill. 2006).
163. *Id.* at 900.
165. *Id.* at 994.
secrets privilege was a matter of national security.\textsuperscript{167}

The Terkel victory was short-lived for the Bush Administration.\textsuperscript{168} Less than a month later, the Bush Administration took another legal hit in \textit{ACLU v. NSA} when Judge Anna Diggs Taylor of the Eastern District of Michigan ruled that the NSA had violated both the Fourth Amendment and FISA.\textsuperscript{169} Judge Taylor wrote, "[i]t was never the intent of the framers to give the president such unfettered control, particularly when his actions blatantly disregard the parameters clearly enumerated in the Bill of Rights."\textsuperscript{170} Despite the ruling, President Bush and his administration continued to advocate the legality and necessity of the program, stating that they would do everything in their power to have the decision overturned on appeal.\textsuperscript{171} True to their promise, they were successful in getting the case overturned by a two-to-one vote in the Sixth Circuit Court of Appeals because the plaintiffs did not have standing.\textsuperscript{172} The court stated that implicit in the plaintiffs' alleged injuries was the "underlying possibility—which the plaintiffs label a 'well founded belief' and seek to treat as a probability or even a certainty—that the NSA is presently intercepting, or will eventually intercept, communications to or from one or more of these particular plaintiffs."\textsuperscript{173}

Since the Bush Administration prevailed only on standing, it still faced the possibility of legal consequences.\textsuperscript{174} This threat, coupled with the controversy that surrounded the legal justifications asserted in support of the NSA program, required a permanent solution: clear legislation on the issue.\textsuperscript{175} It is no coincidence that less than a month after the Sixth Circuit ruling, President Bush forced through the Protect America Act of 2007 (PAA)—an act that legalized eavesdropping on domestic calls and provided immunity to telecommunications companies.\textsuperscript{176} Before Judge Walker's decision, there was no sense of urgency to close the gap in intelligence gathering, as the President had continuously asserted,\textsuperscript{177}

\begin{itemize}
  \item \textsuperscript{167} Id. at 917.
  \item \textsuperscript{168} See ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).
  \item \textsuperscript{169} Id. at 782; Liptak & Lichtblau, supra note 112.
  \item \textsuperscript{170} Liptak & Lichtblau, supra note 112.
  \item \textsuperscript{171} Id.
  \item \textsuperscript{172} ACLU, 493 F.3d at 657 (stating that "the injury that would support a declaratory judgment action . . . is too speculative").
  \item \textsuperscript{173} Id. at 655.
  \item \textsuperscript{174} Id. at 657.
  \item \textsuperscript{175} Press Release, supra note 25.
because there was no threat of legal consequences.\textsuperscript{178} However, after Judge Walker denied the government’s motion to dismiss based on the state secrecy privilege, President Bush spoke of an important intelligence gap that needed to be filled immediately.\textsuperscript{179} Hence, the PAA provided immunity to telecommunications companies who aided the government in data collection and wiretapping.\textsuperscript{180} The Bush Administration was determined to have legislation produced before Congress’ month-long recess gave it an opportunity to oppose the concept of legalized wiretapping.\textsuperscript{181} President Bush even threatened to keep Congress in an “emergency session” until something was produced.\textsuperscript{182} It was under this political climate that the PAA was created.\textsuperscript{183}

When the PAA was passed, the Bush Administration’s inclusion of the immunity provision did more than just shield a useful ally in the war on terror; it fundamentally disrupted the system of checks and balances.\textsuperscript{184} Senator Edward “Ted” Kennedy of Massachusetts, one of the drafters of the original FISA, stated that telecommunications company immunity would “violate basic principles of fairness and justice.”\textsuperscript{185} He argued that it is “precisely because fairness and justice are so important to the American system of government that we ask an independent branch—the judiciary—
to resolve such legal disputes.”

But there was more at stake for the Bush Administration than notions of fairness and justice because the NSA needed telecommunications companies to cooperate. Before current technology was widely available, the NSA could ascertain much of the data it needed via satellites and microwave transmissions. But because these “communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia,” they now bypass the traditional means used by the NSA. The NSA could not access such data without the assistance of these companies. However, with their assistance, the NSA could analyze “the length of a call, the time it was placed, and the origin and destination of electronic transmissions.”

B. “... With [Redacted] and Justice for All”

The boiling frog syndrome states that if a frog is placed in a pot of boiling water it will jump out, but if the frog is placed in a pot of cold water that is gradually warmed up, it will sit still until it dies. This same concept holds true with regard to laws like the PAA. Like the frog placed in cold water that does not notice its slow death, American citizens are not likely to recognize how the PAA will incrementally violate their civil liberties all in the name of national security. “This cycle of terrorist attack followed by government curtailment of civil liberties must be broken—or our society will eventually lose the key attribute that has made it great: freedom.”

The debate in Congress about whether to pass the PAA began only three days before a month-long congressional recess. The Senate considered two versions of the PAA, one sponsored by Republicans and the

186. Id.
187. See id.
189. Id.
190. Id.
191. Id.
192. Id.
196. Id.
other by Democrats.\textsuperscript{198} Despite additional safeguards against abuse in the latter version,\textsuperscript{199} the Republican version of the Act passed.\textsuperscript{200} After affirmation in the Senate, the House of Representatives opened up its floor to debate the merits of the PAA.\textsuperscript{201} Republicans and Democrats were immediately polarized.\textsuperscript{202} Republicans urged the House to take swift action and close what they referred to as "a loophole" in the system.\textsuperscript{203} They appeared to have two main goals: to pass the act before the one-month recess and to attack the only Democrat-sponsored aspect—a 180-day sunset provision.\textsuperscript{204} Congressman Rush Holt, a Democrat from New Jersey, spoke of the tactics his Republican colleagues used in their attempt to achieve these goals:

Do not believe these scare tactics. Legislation should not be passed to respond to fear-mongering. Of course, we need good intelligence to protect Americans, but we are being asked to enter a "just trust us" form of legislation. Just trust an Attorney General who has provided demonstrably false or misleading testimony before Congress on this very issue. We are being asked to just trust this Attorney General with unlimited authority to authorize spying on Americans through this legislation without oversight of the courts, even after his own Inspector General has revealed massive abuses of civil liberties through his department's unchecked use of national security letters.\textsuperscript{205}

Representative Lamar Smith of Texas set the conservative tone by emphasizing that, although the PAA would sunset in 180 days, "terrorists do not sunset their plots to kill Americans."\textsuperscript{206} Representative Trent Franks of Arizona similarly reasoned that "[i]f we do not address the critical loopholes in our foreign surveillance system tonight, our children may

---

198. Id.
200. By examining the statements of the Republican members of the U.S. Senate, it is evident that their version passed. See generally 153 CONG. REC. S10861, 10861–72 (daily ed. Aug. 3, 2007).
202. In the final vote on this bill, only two Republican Congressman voted against it, while over forty Democrats voted for it. See 153 CONG. REC. H9965–66 (daily ed. Aug. 4, 2007).
204. Id.
205. 153 CONG. REC. H9956-57 (daily ed. Aug. 4, 2007) (statement of Rep. Holt). At the time this statement was made, Alberto Gonzales was serving as the Attorney General; however, he was replaced on Aug. 31, 2007.
some day face a nuclear jihad . . . "207 Ultimately, these scare tactics caused the Democrats to supply the necessary votes to tip the scales of justice in favor of the Act’s passage.208 Ironically, such use of fear-based reasoning—the belief that we must do anything and everything to secure our freedom—compromises the very freedom we seek to protect.209

During the August 2007 congressional recess, Bush Administration officials attempted to downplay the significance of the PAA, stating that there would be "strict rules in place to minimize the extent to which Americans would be caught up in the surveillance."210 However, many Democratic lawmakers, like Congressman Rush Holt, were unconvinced that the Bush Administration would impose any limitations on itself with respect to domestic surveillance.211 Congressman Holt stated: "The countries we detest around the world are the ones that spy on their own people. Usually they say they do it for the sake of public safety and security."212

The PAA amended FISA in a number of important ways.213 Under section 105A, the very definition of electronic surveillance was amended to exclude any person “reasonably believed to be located outside the United States.”214 Both the White House and the Director of National Intelligence (DIR), John Michael “Mike” McConnell, asserted that this was a crucial fix in FISA’s outdated language.215 Prior to the passage of the PAA, Mr. McConnell claimed there was a substantial amount of expert resources that were being allocated toward the application process required by the FISA court—a secret federal court that oversees requests for surveillance warrants.216 He argued that this process created a temporal gap that

212. Id.
214. § 105A, 121 Stat. at 552 (emphasis added).
hindered intelligence-gathering abilities.\textsuperscript{218} Furthermore, Mr. McConnell stated that eavesdropping on foreign targets in foreign countries should never require court approval because that was not Congress' original intent when it first passed FISA.\textsuperscript{219}

Under section 105B, "[n]otwithstanding any other law, the [DIR] and the Attorney General may, for periods of time up to one year, authorize the acquisition of foreign intelligence."\textsuperscript{220} Despite the implication that the government could interpret this section to extend to the Constitution, Mr. McConnell believed that the PAA provided sufficient oversight by all three branches of government, and therefore had a low capacity for abuse.\textsuperscript{221} Under section 105C(a), the Attorney General is required to submit a summary of procedures to the Foreign Intelligence Surveillance Court (FISC) within 120 days, and renew it annually thereafter.\textsuperscript{222} Furthermore, the Office of Inspector General (part of the Executive Branch) must conduct internal agency reviews, and the intelligence community must notify the congressional intelligence committees about every authorization made.\textsuperscript{223}

The PAA also includes sections 105B(e) and 105B(e)(1), which allow the government to require the assistance, knowledge, or expertise of virtually any individual and any information database.\textsuperscript{224} More importantly, these sections prevent those individuals or entities from being sued, regardless of whether or not the forced compliance results in unlawful activity.\textsuperscript{225} The latter section was included to address the rising number of suits against telecommunications moguls such as AT&T and Verizon, alleging that they provided private information to the government without first obtaining individual consent from customers.\textsuperscript{226} Although section 105B(1) grants immunity to anyone acting in compliance with the PAA, these companies still faced lawsuits for their alleged actions prior to

\textsuperscript{218} McConnell, \textit{Hearing, supra} note 215, at 21–22.

\textsuperscript{219} \textit{Id.} at 22.


\textsuperscript{222} § 105C(a), 121 Stat. at 555.


\textsuperscript{224} See §§ 105B(e)-105B(e)(1), 121 Stat. at 553. In section 105B(e), the PAA allows the Director of National Intelligence or the Attorney General to direct a person to "immediately provide the government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy." \textit{Id.}

\textsuperscript{225} § 105B(1), 121 Stat. at 554–55.

its passage because Congress refused to make the PAA retroactive.\textsuperscript{227}

Despite Mr. McConnell's assurances that the PAA is sufficiently overseen and not overbroad in its language,\textsuperscript{228} some of its language is ambiguous, and thus creates potential for abuse.\textsuperscript{229} For example, under the definition of "electronic surveillance" in Section 105A, the definition of "reasonableness" was not expanded.\textsuperscript{230} The result was that the Bush Administration was given free reign to conduct surveillance on almost anyone that it could classify as reasonably believed to be outside the United States, without any judicial oversight whatsoever.\textsuperscript{231} Even more alarming, the law remained silent on what action federal officials should take regarding phone calls in which one party is located inside the United States.\textsuperscript{232} Therefore, the Bush Administration was responsible for a process that largely remains a mystery to this day: the collection and storage of such private communications.\textsuperscript{233}

After the PAA expired on February 16, 2008, the Democrats stalled on renewing the legislation, and President Bush increased pressure on Congress to come up with an immediate solution.\textsuperscript{234} Eventually, both the House and Senate approved the FAA, retaining a retroactive immunity provision\textsuperscript{235} that the House had rejected in a previous version of the bill.\textsuperscript{236} The immunity provision was central to finding a legislative solution, with President Bush insisting on granting immunity to the companies.\textsuperscript{237} With the provision included, the FAA effectively rendered moot all pending litigation against telecommunications companies,\textsuperscript{238} as evidenced by the recent decision in \textit{Hepting}.\textsuperscript{239} Attorneys involved in suits against telecommunications companies vowed to appeal the immunity provision in

\begin{itemize}
\item \textsuperscript{227} Eric Lichtblau, \textit{Role of Telecom Firms in Wiretaps is Confirmed}, N.Y. TIMES, Aug. 24, 2007, at A13.
\item \textsuperscript{228} See McConnell, \textit{Hearing}, supra note 215, at 13–14.
\item \textsuperscript{230} Id.
\item \textsuperscript{231} Fact Sheet, supra note 21.
\item \textsuperscript{232} Id.
\item \textsuperscript{233} See Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 909 (N.D. Ill. 2006); see also Fact Sheet, supra note 21.
\item \textsuperscript{234} Branigin, supra note 226.
\item \textsuperscript{238} See Lichtblau, supra note 237 (explaining that "[t]he final deal . . . effectively ends those lawsuits").
\item \textsuperscript{239} See Hepting v. AT&T Corp., 539 F.3d 1157, 1157 (9th Cir. 2008).
\end{itemize}
They believed that the FAA only passed because 2008 was an election year and Democrats did not want to look weak on national security issues. In June 2008, Senator Barack Obama—then campaigning to become the Democratic nominee for President—issued a statement that supported updates to FISA; however, he did not support the telecommunications immunity provision. Senator Obama stated that the Bush Administration, with the cooperation of the telecommunications companies, "abused [its] authority and undermined the Constitution by intercepting the communications of innocent Americans without their knowledge or the required court orders." On the other hand, Republican presidential nominee Senator John McCain expressed support for updates to FISA, but not to renewal of the telecommunications immunity provision. Nevertheless, in June 2008, Senator McCain stated that "neither the Administration nor the telecoms need apologize for actions that most people, except for the [American Civil Liberties Union (ACLU)] and the trial lawyers, understand were Constitutional and appropriate . . . ." These polarized views on telecommunications company immunity illustrate the ongoing debate over the proper role of the private sector in national security issues.

The FAA also contains a provision that expands the length of time in which government officials can invoke "emergency wiretapping procedures." The government can now wiretap without a warrant for seven days, as opposed to the previous three-day limit. Moreover, it allows the government to legally conduct warrantless surveillance on Americans as long as the Attorney General certifies the existence of probable cause that an individual is linked to terrorism. Despite these massive privacy intrusions, Democrats were able to slip in provisions that require a special court to approve wiretapping procedures and generally

240. Lichtblau, supra note 237.
243. Id.
245. Id.
246. See Moran, Posting, supra note 242; see also Letter, supra note 244.
247. Lichtblau, supra note 237.
248. 50 U.S.C. §§ 1801-1881; Lichtblau, supra note 238.
249. 50 U.S.C. §§ 1801-1881; Lichtblau, supra note 238.
prohibit eavesdropping on Americans without a warrant. The FAA is a significant improvement over the PAA, however, because of the continual lack of effective oversight, Congress must strike the immunity provision from the FAA to allow injured parties to have their day in court.

C. It Could Happen to You

Scholars have noted that al-Qaeda has evolved into a movement that has proven its ability to survive. Some scholars suggested that the Bush Administration made "poor short-term decisions that sacrificed our long-term security interests." To more effectively combat the terrorist threat, the federal government needs to understand why terrorists are willing to destroy themselves to harm Americans. However, the goal of politicians is oriented towards reelection. Concerns over appearing weak on terrorism and domestic security, instead of understanding the underlying causes of terrorism, are the driving factors behind the decisions the government has made. For example, the desire for reelection explains why Democrats handed the Bush Administration the PAA legislation, which disregards the Fourth Amendment. The PAA allows privately owned telecommunications companies to release detailed information about its customers without legal consequences.

Reelection is one fundamental reason why Congress has overwhelmingly chosen short-term solutions over a long-term plan to eradicate terrorism. Furthermore, scholars explain that "the political costs associated with allowing a terrorist to go free dramatically outweigh the costs of infringing on the rights of innocents." More importantly, "the costs of a false negative (failing to lock up a terrorist) are often much

250. See 50 U.S.C. §§ 1801-1881; Miller, supra note 226.
252. See Lichtblau, supra note 237.
254. Id.
255. Hulse & Andrews, supra note 28 (stating that politicians are worried about political repercussions).
256. See Nakashima & Warrick, supra note 211; see also COLE & LOBEL, supra note 253, at 195.
257. Hulse & Andrews, supra note 28 (stating that Democrats do not support the surveillance initiative because it grants "the administration too much latitude without judicial review"); see also Nakashima & Warrick, supra note 211.
258. See COLE & LOBEL, supra note 253, at 195.
259. Id.
more visible than the costs of a false positive (locking up an innocent).”

Legislation like the FAA and the PAA are blatantly ineffective to combat terrorism. Some scholars argue terrorists kill people to coerce the actions of a government, and that is exactly what happened in the United States after 9/11.

Sadly, Americans have lost many liberties and freedoms since 9/11. The story of Brandon Mayfield is one example. Mayfield was an attorney residing with his family in Oregon when the Madrid train bombing occurred in 2004. Despite notifications by the Spanish National Police that fingerprints found on a bag of detonators at the scene did not match Mayfield’s, the FBI arrested and jailed Mayfield for over two weeks. An FBI report released afterward stated that, while Mayfield’s status as a Muslim convert “was not a factor in his initial identification, it contributed to the FBI’s reluctance to reexamine its conclusions after the challenges from Spanish police.” Fortunately, the error was discovered in time, and the government agreed to pay Mayfield and his family approximately $2,000,000 in damages. Mistakes, like those in Mayfield’s case, are more likely to occur when a government views its citizens as suspects and there is a failure to properly weigh the evidence.

The very fact that such a mistake occurred in this country should cause concern. The terrorists have achieved part of their goal with respect to the United States. Americans unwittingly allowed the government to increase its prominence in private lives, thus curtailing American freedom. Congressman Mel Watt spoke against legislation such as the PAA, observing: “[W]orry about what [the terrorists] might be thinking tonight, because they must be thinking: You know, we might have won the battle, because we have the United States reacting and giving up its constitutional rights.” To date, it is unclear on whom the government

260. Id.
263. Id.
264. Id.
265. Id.
266. Id.
eavesdropped, whether these individuals had anything to do with terrorism, and what happens to the collected information. In its effort to preserve national security, the government has disregarded constitutionally guaranteed liberties known only to the trial lawyers and ACLU who have actually studied the law.

IV. CONCLUSION

Justice Warren once wrote: "Implicit in the term 'national defense' is the notion of defending those values and ideals which set this Nation apart ... It would indeed be ironic if, in the name of national defense, we would sanction the subversion of ... those liberties ... which makes the defense of the Nation worthwhile." A system of information collection that continuously chips away at the rights of Americans, while simultaneously impeding any possible legal remedy, turned our democratic system into an Orwellian one.

In addressing the Senate regarding the FISA Amendments Act of 2008 (FAA), Senator Kennedy stated: "In a democracy, it is the job of the legislature to amend laws to fit new circumstances. It is not the job of the legislature to rubber-stamp illegal conduct by the Executive." The Protect America Act of 2007 was the Bush Administration's attempt to legislate its way out of its own illegal conduct. And when it expired, the Bush Administration pressured Congress into passing a more invasive act that has the added sting of retroactive telecommunications immunity. "In the name of making us safer, the Administration's reckless disregard for the law has made us less safe, and countless Americans fear their rights have been endangered. That sorry record demands accountability—not immunity."

Congress must repeal the FAA. This is the only way to effectively ensure that the Executive Branch cannot legally collect vast amounts of personal data and that telecommunications companies should be held liable


271. See id. (stating that "neither the Administration nor the Telecoms need apologize for actions that most people, except for the ACLU and the trial lawyers, understand were Constitutional and appropriate in the wake of the attacks on September 11, 2001").


274. Press Release, Kennedy on FISA, supra note 185.


276. Press Release, Kennedy on FISA, supra note 185.
for their assistance in the National Security Agency program.\textsuperscript{277} Equally as important, Americans must never allow the threat of terrorist attacks to compromise the fundamental liberties that are inherent in American government. What Benjamin Franklin said has particular resonance today: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."\textsuperscript{278}

\textit{Shahab Mossavar-Rahmani*}

\textsuperscript{277} See 50 U.S.C. §§ 1801–1881.


* J.D. Candidate, May 2009, Loyola Law School, Los Angeles; B.A. University of California, San Diego. I would like to thank my mother, Maryam, for her constant love and support; my father, Farhang, for his guidance and valuable insight; my editors, Gary Wax, who gave form and structure to what once seemed like just a jumble of thoughts and potential, and Mark Robertson, for his dedication and painstaking attention to detail. Finally, I want to thank Michelle Raji for her seemingly endless patience and love.