Securing Liberty: Terrorizing Fourth Amendment Protections in a Post 9/11 World

Jara Jebrock*
SECURING LIBERTY: TERRORIZING FOURTH AMENDMENT PROTECTIONS IN A POST 9/11 WORLD

DARA JEBROCK*

I. INTRODUCTION ............................................................................................................. 279

II. HISTORY OF FOURTH AMENDMENT PROTECTIONS .............................................. 282
   A. The Warrant Requirement .................................................................................. 283
       1. Probable Cause ....................................................................................... 284
       2. Judicial Approval .................................................................................. 285
   B. From Property to Privacy ............................................................................... 287

III. NATIONAL SECURITY AS A POTENTIAL EXCEPTION ............................................. 289
   A. National Security in Domestic Affairs .......................................................... 289
   B. National Security in Foreign Affairs ............................................................. 293

IV. EROSION OF THE FOURTH AMENDMENT AFTER 9/11 ........................................ 296

V. DOE V. ASHCROFT ....................................................................................................... 297
   A. The Case for Controversy ............................................................................. 297
   B. Securing Fourth Amendment Freedoms ...................................................... 298

VI. RECOMMENDATION .................................................................................................. 299
   A. Prior Judicial Approval ................................................................................. 300
   B. Post Judicial Oversight ................................................................................. 300
   C. The Keith Approach .................................................................................... 301

VII. CONCLUSION .............................................................................................................. 301

I. INTRODUCTION

On September 11, 2001, nineteen men affiliated with the al Qaeda terrorist organization hijacked four commercial airliners.¹ At approximately 8:46 a.m., American Airlines Flight 11, holding eighty-one passengers,
crashed into the North Tower of the World Trade Center. 2 "[S]omething terrible is happening,"3 Stuart Meltzer declared while on the phone with his wife from the 105th floor of the building.4 This would be the last time the two would speak.5 All of the passengers onboard Flight 11, including an unknown number of people in the building, were killed.6

Approximately eighteen minutes later, United Airlines Flight 175, with fifty-six passengers on board, slammed into the South Tower of the World Trade Center.7 "The place is filling with smoke," a person [located] in [a] New York office was heard to say [just before the phone] connection was cut off."8 Consequently, all of the passengers on board Flight 75, along with an undetermined number of people in the building, were killed.9

It is "an 'apparent terrorist attack'" on our country,10 President Bush proclaimed just before American Airlines Flight 77, traveling at approximately 530 miles per hour, smashed into the Pentagon.11 All fifty-eight passengers on board Flight 77 were killed, in addition to 125 civilian and military personnel located in the building.12

At approximately 10:00 a.m., "Alice Hoglan's son, Mark, called her from United Airlines Flight 93" and told her that the plane had been "taken over."13 Shortly thereafter, the fourth plane holding thirty-seven passengers crashed into a rural field in southern Pennsylvania.14 The hijacker's objective was to crash the fourth airliner into either the Capitol Building or the White House, but a counterattack by the passengers of United Flight 93 defeated that goal.15 Unfortunately, all of the people on board the airliner were killed.16

4. Id. (citation omitted).
5. See id. (citation omitted).
6. See EXECUTIVE SUMMARY, supra note 1, at 2.
7. Id. at 1; Chronology, supra note 2.
8. Veale, supra note 3 (citation omitted).
10. Id.
12. Chronology, supra note 2; see also COMM'N REP., supra note 11, at 10.
13. Veale, supra note 3 (citation omitted).
14. See EXECUTIVE SUMMARY, supra note 1, at 1; Chronology, supra note 2.
15. EXECUTIVE SUMMARY, supra note 1, at 1.
16. See id. at 1–2.
The deadly terrorist attacks of September 11, 2001 were unprecedented in America’s national history. There is no doubt that sophisticated technologies, especially internet communication, were essential to allow the planning and plotting of the attacks. As a result, President Bush, along with Congress, responded by enacting the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, generally known as the USA PATRIOT Act, in order to allow law enforcement and intelligence agencies greater authority in tracking and intercepting communications.

More specifically, the USA PATRIOT Act made a series of controversial amendments to the United States Code. In particular, this article focuses on 18 U.S.C. § 2709, which “authorizes the Federal Bureau of Investigation (FBI) to compel . . . internet service providers (ISPs) or telephone companies, to produce . . . customer records whenever the FBI certifies that those records are ‘relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.’” The FBI makes those demands by sending national security letters to the communication provider. Once the national security letter is formally issued, § 2709 bars the recipient from contesting the grounds for the letter and prohibits the recipient from notifying the customers that their personal information has been provided to the FBI. That means the provider is forced to turn over the requested records or else face criminal prosecution. Thus, this provision raises serious constitutional questions because § 2709, as amended, grants the FBI the extraordinary power to obtain records without obtaining a warrant supported by probable cause and judicial oversight as required by the Fourth Amendment.

23. Id. at 475.
24. Id. (citing 18 U.S.C. § 2709(c) (2000)).
25. See § 2709.
According to President Bush, the USA PATRIOT Act provision granting the FBI such vast power was necessary in allowing the government to enforce laws "with all the urgency of a nation at war." However, this article will demonstrate that expanding the FBI's power to conduct terrorism investigations abolishes important Fourth Amendment protections. Part II of this article will provide a historical overview of Fourth Amendment jurisprudence, while Part III will examine traditional Fourth Amendment protections in light of national security operations. Part IV will discuss the erosion of Fourth Amendment freedoms after 9/11 as a result of the technologies that allowed terrorists to evade law enforcement more easily. Part V will analyze the decision rendered in Doe v. Ashcroft, because the opinion describes how Fourth Amendment protections cannot be guaranteed within the sole discretion of the FBI and, in turn, without judicial approval. Part VI will provide recommendations to revise § 2709 in order to reduce Fourth Amendment implications. Lastly, part VII will conclude with a summary of this article.

II. HISTORY OF FOURTH AMENDMENT PROTECTIONS

The Fourth Amendment affords individuals with some of the most basic protections against government intrusion. In short, the Framers of the Constitution designed the Fourth Amendment as a way to break away from British policy, which allowed for the issuance of general warrants. Those types of warrants generally allowed officials to break into an individual's home, store, or other personal place and seize goods based on minimal suspicion of criminal activity. Since there were no requirements of probable cause and judicial oversight, the use of the general warrant was widely abused and caused significant intrusions into individuals' personal lives because once the warrant was obtained, there was no limit to what the official could search or obtain a warrant based on probable cause, supported by judicial authorization, particularly describing the place to be searched and the persons or things to be seized).

27. The Fourth Amendment guarantees:
   [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
   U.S. CONST. amend. IV.
30. See U.S. CONST. amend. IV.
32. See id. at 693–94.
seize. Moreover, because there was no fact finder to determine whether the suspicion was justified, the official could easily lie to obtain a warrant.

However, the Framers' concern when drafting the Fourth Amendment was not the issuance of the warrant itself. The Framers' concern was the lack of procedural limitations placed on law enforcement's ability to invade an individual's privacy. As a result, the Fourth Amendment's warrant requirement, as examined below, was specifically written to protect individuals against unjustified police behavior.

A. The Warrant Requirement

Requiring a warrant to conduct a search or seizure was the Framers' way of protecting individuals from unwarranted government intrusions by limiting its ability to conduct investigations. One of the first cases decided concerning the scope of the warrant requirement was Ex parte Jackson. In Jackson, the United States Supreme Court clearly stated that searches and seizures of personal documents in a criminal investigation require a warrant. The Court held that:

[the constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. [Letters and sealed packages] can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.]

Thus, under Jackson, a warrantless search and seizure of an individual's private property constitutes a violation of the Fourth Amendment.

Over time, the Court broadened the scope of Fourth Amendment protection to include searches and seizures involving entry into a person's home, as
well as the curtilage surrounding the property.\textsuperscript{43} That augmentation was significant because it furthered the premise that individuals should be protected from unwarranted government intrusion not only in the privacy of their own home, but also in a limited, judicially-defined area surrounding their home.\textsuperscript{44} Moreover, in \textit{Camara v. Municipal Court},\textsuperscript{45} the Court then extended those principles to include routine administrative searches of a home.\textsuperscript{46} In \textit{Camara}, the petitioner leased the ground floor of a building to use as his personal residence.\textsuperscript{47} The case arose when the petitioner did not allow an inspector of the Division of Housing to perform a routine administrative search of his home.\textsuperscript{48} As a result, the petitioner was charged with "refusing to permit a lawful inspection in violation" of a city ordinance.\textsuperscript{49} On appeal, the petitioner alleged that a search of private property is unreasonable unless it has been authorized by a search warrant.\textsuperscript{50} The Court agreed, holding that administrative searches authorized and conducted without a warrant are significant intrusions upon privacy interests protected by the Fourth Amendment.\textsuperscript{51} Thus, the Court reversed the conviction, reinforced the importance of the Fourth Amendment warrant requirement, and expanded the scope of this amendment’s protections.\textsuperscript{52}

1. Probable Cause

The Fourth Amendment generally requires a showing of probable cause before law enforcement may obtain a warrant to conduct a search or seizure

\begin{itemize}
\item \textsuperscript{43} E.g., \textit{Hester v. United States}, 265 U.S. 57, 59 (1924) (recognizing that Fourth Amendment protection extends not only to houses, but also to the area surrounding the residence, generally known as “curtilage”); \textit{United States v. Dunn}, 480 U.S. 294, 296 (1987); \textit{Oliver v. United States}, 466 U.S. 170, 180 (1984).
\item \textsuperscript{44} \textit{See Oliver}, 466 U.S. at 180.
\item \textsuperscript{45} 387 U.S. 523 (1967).
\item \textsuperscript{46} \textit{Id.} at 534. In general, an administrative search is an inspection made by a government official in regards to municipal fire, health, and housing evaluation programs. \textit{BLACK’S LAW DICTIONARY} 1378 (8th ed. 2004).
\item \textsuperscript{47} \textit{Camara}, 387 U.S. at 526.
\item \textsuperscript{48} \textit{Id.}
\item \textsuperscript{49} \textit{Id.} at 527. This case dealt with section 503 of the Housing Code which permits: [a]uthorized employees of the City departments or City agencies, so far as may be necessary for the performance of their duties, shall, upon presentation of proper credentials, have the right to enter, at reasonable times, any building, structure, or premises in the City to perform any duty imposed upon them by the Municipal Code.
\item \textit{Id.} at 526.
\item \textsuperscript{50} \textit{See id.} at 525.
\item \textsuperscript{51} \textit{Camara}, 387 U.S. at 534.
\item \textsuperscript{52} \textit{See id.} at 534, 546.
\end{itemize}
of property. Under the probable cause rule, law enforcement cannot search a person's home or seize private documents unless they have specific facts to believe that the subject of the search or seizure is connected with criminal activity. The purpose of that requirement is to lessen the possibility that law enforcement will commit perjury to create a reason for discovering incriminating evidence. For that reason, warrants lacking probable cause usually violate the Fourth Amendment.

2. Judicial Approval

In addition, the warrant requirement generally mandates that an independent judicial officer determine whether probable cause exists to conduct a search or seizure. In *Johnson v. United States*, the United States Supreme Court stated that a warrant can only be issued by a "neutral and detached magistrate." Writing for the majority, Justice Jackson reasoned that:

[...]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers. Crime, even in the privacy of one's own quarters, is, of course, of grave concern to society, and the law allows such crime to be reached on proper showing. The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably

53. *Id.*
55. *See Camara*, 387 U.S. at 528; Giordenello v. United States, 357 U.S. 480, 486 (1958); McDonald v. United States, 335 U.S. 451, 455 (1948).
58. 333 U.S. 10 (1948).
59. *Id.* at 14.
yield to the right of search is, as a rule, to be decided by a judicial
officer, not by a policeman or government enforcement agent. 60

Moreover, the Court emphasized that the Fourth Amendment was designed
to prevent the depreciation of personal freedom, personal security, and prop-
erty interests because those rights "are to be regarded as of the very essence
of constitutional liberty." 61 Accordingly, the Court recognized that allowing
law enforcement to seek personal information without judicial oversight vio-
lates the core principles of the Fourth Amendment. 62

Subsequently, in Coolidge v. New Hampshire, 63 the Court held that it is
unconstitutional under the Fourth Amendment for a government official to
issue a warrant, even if authorized to do so as a justice of the peace, when
that official is engaged in the criminal investigation. 64 In Coolidge, police
went to the defendant’s home to question him about a murder. 65 Thereafter,
the police presented the results of their inquiry to the State Attorney General
because he was leading the murder investigation. 66 After concluding there
was sufficient evidence to charge the defendant, the Attorney General, acting
as a justice of the peace, 67 issued a warrant to search the defendant’s prop-
erty. 68 At trial, the defendant was convicted of murder based on evidence
obtained from the searches. 69 The defendant appealed, alleging that such
evidence should not have been admitted at trial because it was obtained in
violation of the Fourth Amendment. 70 The Court agreed, holding that a war-
rant issued by a government official involved in law enforcement activities
does not constitute a "neutral and detached magistrate" in accordance with
the warrant procedure of the Fourth Amendment. 71

60. Id. at 13–14 (footnotes omitted).
61. Id. at 17 n.8 (quoting Gouled v. United States, 255 U.S. 298, 304 (1921)).
62. See id. at 17.
63. 403 U.S. 443 (1971).
64. Id. at 453.
65. Id. at 445.
66. Id. at 446–47.
67. "Under New Hampshire law in force at that time, all justices of the peace were au-
thorized to issue search warrants." Id. at 447.
68. Coolidge, 403 U.S. at 447.
69. See id. at 448.
70. Id. at 449.
71. Id.
B. From Property to Privacy

The invention of surveillance technologies provided law enforcement with the ability to surreptitiously observe and record an individual's private telephone conversations. The warrantless use of such technology to aid securing criminal convictions was challenged for the first time in *Olmstead v. United States*. In *Olmstead*, the defendants were convicted of conspiracy to violate the National Prohibition Act. Federal officers obtained the evidence that led to their conviction by inserting small wires along the ordinary wires of a telephone company which was connected to the defendants' residences. Using the taps on the telephone wires, federal officials surreptitiously listened to the defendants' conversations and took stenographic notes. As a result, federal officials procured evidence to indict and eventually convict the defendants of conspiracy. In 1928, the Supreme Court granted certiorari to determine whether the use of evidence obtained from wiretapping the defendants' private conversations constituted a violation of the Fourth Amendment. On a five-to-four vote, the Court held that the use of wiretapping to obtain evidence without a search warrant was not within the confines of the Fourth Amendment because there was no physical encroachment onto the defendants' property.

After *Olmstead*, the measure of Fourth Amendment protection was determined on a property-based analysis. However, in 1967, the Supreme Court redefined the Amendment's scope by recognizing "that the principal object of the Fourth Amendment is the protection of privacy rather than [the further protection of] property." In *Katz v. United States*, the Supreme Court held that the "Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures," and that its reach "cannot turn upon the presence or absence of a physical intrusion into any given enclosure." In *Katz*, the petitioner, a bookkeeper, was suspected of using a public telephone booth to conduct business transactions in violation

---

73. Id. at 438.
74. Id. at 455.
75. Id. at 456-57.
76. Id. at 457.
77. *Olmstead*, 277 U.S. at 455, 457.
78. Id. at 455.
79. Id. at 466.
82. Id. at 353.
of a federal statute. To confirm those suspicions, the FBI placed an electronic eavesdropping device on the outside of the telephone booth, which recorded the petitioner’s conversations. As a result, the petitioner was charged and convicted of transmitting gambling information by telephone across state lines. On appeal, the petitioner alleged that the recordings had been obtained in violation of the Fourth Amendment. However, the Ninth Circuit Court of Appeals disagreed, holding that no violation occurred because the FBI agents did not physically enter the telephone booth.

In light of that ruling, the United States Supreme Court granted certiorari to consider whether electronic surveillance was subject to the Fourth Amendment prohibition against unreasonable searches and seizures. Writing for the majority, Justice Stewart declared that:

the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

For those reasons, the Court ruled that a violation of the Fourth Amendment occurs when FBI agents conduct electronic surveillance of an individual without presenting “their estimate of probable cause for detached scrutiny by a neutral magistrate,” even when there is no interference with property. Consequently, the petitioner’s conviction was reversed because he had not been provided with the procedural safeguards of the Fourth Amendment. Thus, the Court’s decision is significant because it recognizes the importance of protecting Fourth Amendment liberties, especially when technological innovations threaten personal privacy.

83. Id. at 348. 18 U.S.C. § 1084 made it a crime to “knowingly [use] a wire communication facility for the transmission in interstate . . . commerce of bets or wagers . . . on any sporting event or contest, . . . which entitles the recipient to receive money or credit as a result of bets or wagers.” Id. at 348 n.1 (citation omitted).
84. Id. at 348.
86. Id. at 348–49.
87. Id. at 349.
88. Id. at 349–50.
89. Id. at 351–52 (citations omitted).
91. Id. at 359.
92. See id. at 349–53.
III. NATIONAL SECURITY AS A POTENTIAL EXCEPTION

In *Katz*, the majority declined to consider whether national security investigations should be exempt from the Fourth Amendment warrant requirement. However, Justice White noted in his concurring opinion that the warrant requirement and the objective judgment of a magistrate would be unnecessary "if the President of the United States or his chief legal officer, the Attorney General," authorized electronic surveillance in national security situations.

Alternatively, Justice Douglas in his concurring opinion proclaimed that:

> Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and disinterested. Rather it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases.

In his conclusion, Justice Douglas acknowledged that throughout history the Fourth Amendment has never been construed to distinguish between different types of crimes. Thus, those opinions suggest that there are constitutional limitations on the government’s ability to obtain intelligence information even in the name of national security.

A. National Security in Domestic Affairs

Following *Katz*, courts had difficulty determining whether there is in fact a national security exception to the Fourth Amendment warrant requirement. For example, in *United States v. Smith*, the defendant was found guilty of violating a federal statute and sentenced to two years in prison. The defendant appealed his conviction and while "pending, the government

---

93. *Id.* at 358 n.23.
94. *Id.* at 364 (White, J., concurring).
96. *Id.* at 360.
98. *Id.* at 424.
disclosed to the Court of Appeals that it monitored the defendant’s conversations by electronic surveillance to gather information regarding a national security investigation. Accordingly, the Court of Appeals remanded the case to the United States District Court of the Central District of California to consider whether it was constitutional under the Fourth Amendment for the government to conduct warrantless electronic surveillance without judicial approval, even though such surveillance had been authorized by the Attorney General for national security purposes. At the proceeding, the government argued that although a warrant was not obtained prior to conducting the surveillance, it was constitutional because it had been expressly authorized by the Attorney General to gather information necessary to protect the nation. More specifically, that the surveillance was reasonable because “the President, acting through the Attorney General, has the inherent constitutional power” to authorize electronic surveillance without a judicially approved warrant in national security cases and to unilaterally determine whether a situation constitutes a national security matter. However, the district court disagreed, holding that in domestic situations there is no national security exception to the Fourth Amendment warrant requirement. Moreover, “the President is . . . subject to the constitutional limitations imposed upon him by the Fourth Amendment,” which means that he cannot judicially determine the restrictions on his power to protect the security of the nation. The court reasoned that the Constitution was drafted “to strike a balance between the protection of political freedom and the protection of the national security

99. Id.
100. Id. at 424, 426.
101. Id. at 426. To support its argument, the government relied on the Omnibus Crime Control and Safe Streets Act of 1968, which stated in relevant part:

[T]he constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything . . . limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

102. Id. at 426.
103. Id. at 429.
104. Id. at 425.
105. See Id. at 425–30.
interest." Thus, "to sacrifice those freedoms in order to defend them" would undermine the democratic system. Consequently, the electronic surveillance violated the defendant's Fourth Amendment rights because it had been authorized without judicial oversight.

Likewise, in United States v. Sinclair, the United States District Court of the Eastern District of Michigan furthered the Smith rationale by holding that the President, acting through the Attorney General, does not have the inherent constitutional power to authorize, without a judicial warrant, electronic surveillance in national security investigations. In Sinclair, the defendant was indicted based on evidence which was obtained when the FBI conducted warrantless electronic surveillance of the defendant's telephone conversations.

The dispute arose when the defendant made a motion to suppress such evidence, alleging that it was acquired in violation of the Fourth Amendment warrant requirement because it lacked judicial approval. In response, the government asserted that the electronic monitoring of the defendant's conversations was lawful because the Attorney General, acting as an agent of the President, authorized the surveillance in the interest of national security. Particularly, the government argued that the evidence should not be suppressed because the President has the inherent constitutional power to authorize warrantless electronic surveillance when gaining such information is essential to the security of the nation.

Nevertheless, the district court disagreed, stating that the purpose of the Fourth Amendment warrant procedure is to maintain a system of checks and balances between the citizens and the government. Therefore, independent judicial review of whether or not probable cause exists to issue a warrant is essential because it protects citizens' "constitutional right to be free from unreasonable searches and seizures." Further, the court explained that if the executive branch were granted unchecked investigative power in domestic situations, citizens' Fourth Amendment protections would be threat-

107. Id.
108. See id.
109. See id.
111. Id. at 1077.
112. Id. at 1075–76.
113. Id. at 1076.
114. Id.
116. Id. at 1077.
117. Id.
ened.118 For those reasons, the court held that the evidence should be suppressed because there is no exception to the Fourth Amendment warrant requirement in domestic situations involving national security.119

Following Smith and Sinclair, the Supreme Court ruled that in domestic situations the executive branch is not exempt from obtaining a judicially approved warrant when seeking information in a national security investigation.120 In United States v. United States District Court (Keith),121 the government "charged three defendants with conspiracy to destroy [g]overnment property in violation of" a federal statute.122 During pretrial proceedings, the defendants filed a motion to determine whether certain surveillance information obtained by the government complied with the defendants’ Fourth Amendment rights.123 In response, the government alleged that such information was obtained lawfully because the surveillance conducted without judicial approval was authorized by the Attorney General "‘to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government.’"124 More specifically, the government argued that requiring judicial oversight would create a danger of leaks, threaten the need for secrecy, and endanger the lives of informants and agents.125 However, the District Court disagreed and the Court of Appeals affirmed, holding that the surveillance violated the Fourth Amendment.126

In response to that decision, the Supreme Court granted certiorari to determine "‘[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving . . . national security.’"127 To answer this question, the Supreme Court began by noting that under Article II, Section 1 of the Constitution, the President has the duty "‘to preserve, protect and defend the Constitution of the United States,’"128 especially against those who try to depose the government.129 Writing for the majority, Justice Powell expressed his apprehension towards allowing electronic surveillance in national security matters because it provides the gov-

118. See id. at 1079.
119. Id. at 1079–80.
121. Id. at 297.
122. Id. at 299.
123. See id. at 299–300.
124. Id. at 300 (citation omitted).
126. Id. at 301.
127. Id. at 309 (quoting Katz v. United States, 389 U.S. 347, 358 n.23 (1967)).
128. Id. at 310 (quoting U.S. Const. art. II, § 1).
129. Id.
government with the capability to intrude upon individuals' Fourth Amendment rights. However, Justice Powell recognized that technological developments have resulted in new ways to depose the government. For that reason, Justice Powell stated that it would be contrary to public interest to deny the government use of such technology, since it is necessary to counteract the practice of techniques which threaten democracy. As a result, the Court acknowledged that the conflict between the government's need to act when safeguarding the nation's security and individual rights will be implicated in any situation concerning electronic surveillance of a person's private activities. Consequently, the Court balanced those values, concluding that the guarantee that an individual's privacy can only be invaded upon the issuance of a warrant by a neutral and detached magistrate founded on probable cause prevails over the government's duty to preserve national security. Moreover, domestic security surveillances conducted entirely within the discretion of the Executive Branch is inconsistent with the Fourth Amendment because those officials are not neutral and detached. Finally, the role of judicial approval cannot be dispensed because it "accords with [the] basic constitutional doctrine that individual freedoms will best be preserved through [the] separation of powers and division of functions among the different branches and levels of [g]overnment."

B. National Security in Foreign Affairs

Based on the Court's decision in Keith, it is clear that there is no national security exception to the Fourth Amendment in situations involving domestic investigations. However, the Court expressly refused to define the constitutional limitations on the Executive Branch's power to meet foreign threats to the nation. As a result, the scope of Fourth Amendment protections still remain uncertain in situations involving the Executive Branch and foreign security surveillance.

In Noro v. United States, the Fifth Circuit Court of Appeals considered whether the search and seizure of account books owned by Japanese

130. See Keith, 407 U.S. at 312.
131. See id. at 312.
132. Id.
133. See id. at 312-13.
134. See id. at 312-17.
136. Id. at 317.
137. See id. at 321.
138. Id. at 321-22.
139. 148 F.2d 696 (5th Cir. 1945).
citizens living in the United States was a violation of the Fourth Amendment. In Noro, the defendants were Japanese citizens who established a business in the United States, which had been licensed by the Secretary of the Treasury. Following the attack on Pearl Harbor, the President ordered customs officers to remove books, files, and accounts of all Japanese enterprises licensed in the United States. As a result, customs officers seized account books from the defendants’ business without obtaining a judicially approved warrant. After searching the books, the government discovered that the defendants completed false income tax returns. Based on that discovery, the defendants were charged with tax evasion and were convicted at trial. On appeal, the defendants argued that the entry into their place of business and the seizure of their account books violated the Fourth Amendment because such documents were obtained without a judicially authorized warrant. However, the court disagreed stating that no violation occurred because “searches in the sudden emergency of war [are] necessary to be made . . . with all speed and efficiency, under the urgent orders of the President and Secretary of the Treasury.” Thus, the court recognized that the Executive Branch has the power to authorize searches and seizures without judicial oversight in situations that involve foreign threats to the security of the nation.

Likewise, in United States v. Brown, the Fifth Circuit Court of Appeals held that warrantless electronic surveillance authorized by the President for the purpose of gathering foreign intelligence information without prior judicial approval was constitutional under the Fourth Amendment. In Brown, the defendant was charged and convicted of transporting a firearm in violation of a federal statute. The defendant appealed his conviction and, while the appeal was pending, federal officials monitored and recorded the defendant’s telephone conversations without judicial authorization. On appeal, the defendant argued that the warrantless wiretaps violated his Fourth

140. Id. at 697.
141. Id. at 697–98.
142. Id.
143. Id. at 697.
144. Noro, 148 F.2d at 697.
145. Id.
146. Id.
147. Id. at 698.
148. Id. at 698–99.
149. 484 F.2d 418 (5th Cir. 1973).
150. Id. at 426 (citing United States v. Clay, 430 F.2d 165, 170–72 (5th Cir. 1970)).
151. Id. at 420.
152. Id. at 421.
Amendment rights. In response, the government contended that no violation occurred because the wiretaps had been authorized by the Attorney General, acting as an agent of the President, for the purpose of gathering foreign intelligence. Consequently, the court agreed with the government, explaining that the President has the inherent authority to protect national security in the context of foreign affairs. Thus, the court recognized that it is constitutionally permissible for the Executive Branch to conduct searches or seizures without a judicially approved warrant when "safeguard[ing] the nation from possible foreign encroachment."

Similarly, in United States v. Butenko, the Third Circuit Court of Appeals held that the President's authority to authorize warrantless searches in foreign intelligence investigations does not contravene the safeguards of the Fourth Amendment. At trial, one of the defendants, a Soviet national, was convicted of conspiring to transmit foreign government information relating to the national defense of the United States. Federal officials obtained the evidence that led to this conviction by conducting warrantless electronic wiretaps of the defendant's conversations which were authorized by the Attorney General for purposes of gathering foreign intelligence information. The defendant appealed his conviction on the basis that his Fourth Amendment rights were violated because the material collected through the electronic surveillance was obtained without a judicially authorized warrant. However, the court noted that under these circumstances the Fourth Amendment requires post-search judicial review in order for electronic surveillance to be lawful because post-judicial oversight ensures that the primary purpose of the government's investigation is to obtain foreign intelligence information.

153. Id. at 425.
154. Brown, 484 F.2d at 425.
155. Id. at 426.
156. Id. (citations omitted).
157. 494 F.2d 593 (3d Cir. 1974).
158. Id. at 603–06.
159. Id. at 596.
160. Id. at 596–601.
161. Id. at 596.
162. Butenko, 494 F.2d at 603–06.
163. Id. at 605–06.
IV. EROSION OF THE FOURTH AMENDMENT AFTER 9/11

Following September 11, 2001, securing the nation demanded heightened vigilance because technological innovations allowed terrorists to evade law enforcement more easily. On October 26, 2001, Congress enacted the USA PATRIOT Act\textsuperscript{164} to provide government officials with greater authority when conducting terrorism investigations.\textsuperscript{165} In particular, the USA PATRIOT Act revised 18 U.S.C. § 2709 in order to expand the FBI’s power to obtain customer information from internet service providers and telephone companies.\textsuperscript{166}

Originally, § 2709 was enacted as a part of the Electronic Communications Privacy Act (ECPA) of 1986,\textsuperscript{167} which was designed to protect communications customers from unwarranted invasions into privacy, while at the same time allowing law enforcement access to records after satisfying the warrant requirement.\textsuperscript{168} Under the ECPA, § 2709 operated as an exception to the warrant requirement in order to permit the FBI to seek records upon issuing a national security letter to an internet service provider or telephone company by certifying that 1) the requested “information was ‘relevant to an authorized foreign counterintelligence investigation[]’” and 2) that there was probable cause to believe that the customer to whom the information sought was connected to a “‘foreign power or an agent of a foreign power.’”\textsuperscript{169} Subsequently, Congress further revised § 2709 to allow the FBI to obtain customer records where there is a contact with a suspected terrorist or where circumstances of the conversations indicate that the customer may have information regarding terrorist activities.\textsuperscript{170} Recently, in 2001, § 505 of the USA PATRIOT Act dispensed § 2709’s foreign nexus requirement, “replacing that prerequisite with a broad standard of relevance to investigations of terrorism or clandestine intelligence activities.”\textsuperscript{171} Under the current provision,\textsuperscript{172} law enforcement officials have unchecked power to obtain a person’s

\textsuperscript{165} See Kerr, supra note 18, at 607.
\textsuperscript{168} Ashcroft, 334 F. Supp. 2d at 480 (citation omitted).
\textsuperscript{169} Id. at 481 (quoting 18 U.S.C. § 2709 (2000)).
\textsuperscript{170} Id. at 482 (citation omitted).
\textsuperscript{172} The amended version of § 2709 states:
(a) DUTY TO PROVIDE. – A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic
private information from an internet service provider or telephone company without a warrant, and, in turn, without judicial authorization. As discussed below in the case of Doe v. Ashcroft, to allow the government to obtain private information in the manner provided by § 2709 is arguably an unjustified encroachment upon an individual’s Fourth Amendment rights.

V. Doe v. Ashcroft

A. The Case for Controversy

The controversy began when John Doe received a telephone call from the FBI informing him that he would be served with a national security letter. Shortly thereafter, Doe received a document stating that pursuant to 18 U.S.C. § 2709, he was required to provide certain intelligence information to the FBI. Printed on FBI letterhead, the national security letter was certified in compliance with the terms of § 2709. Specifically it stated, “that the information sought was relevant to an authorized investigation to pro-

173. See Ashcroft, 334 F. Supp. 2d at 495-96.
174. “John Doe” is a fictitious name used to describe an internet service provider. Id. at 475.
175. Id. at 478.
176. Id.
177. Id.
tect against international terrorism or clandestine intelligence activities.\textsuperscript{178} Moreover, Doe was warned not to disclose anything about the national security letter, not even that he received it.\textsuperscript{179} Accordingly, Doe contacted the American Civil Liberties Union (ACLU)\textsuperscript{180} and the American Civil Liberties Foundation (ACLF) seeking legal advice about whether the FBI had the authority to demand records from him.\textsuperscript{181}

In April 2004, the ACLU and the ACLF, acting as counsel for John Doe, filed a lawsuit challenging the FBI’s authority to issue national security letters instructing communication firms to disclose customer records.\textsuperscript{182} In the complaint, the plaintiffs alleged that § 2709 violates the Fourth Amendment because it allows the FBI to obtain private information without any form of judicial oversight.\textsuperscript{183} In response, the government argued that the congressional purpose of the provision was to allow the FBI greater investigative powers because there is a need for secrecy in national security investigations.\textsuperscript{184}

B. \textit{Securing Fourth Amendment Freedoms}

Unwilling to sacrifice liberty for security, Judge Marrero of the United States District Court of the Southern District of New York ruled that the provision authorizing the FBI to demand customer records from internet service providers and telephone companies “whenever the FBI certifies that those records are ‘relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,’”\textsuperscript{185} violates the Fourth Amendment.\textsuperscript{186} Judge Marrero began his analysis by recognizing that “[n]ational security is a paramount value, unquestionably one of the highest purposes for which any sovereign government is ordained. Equally scaled . . . is personal security, . . . [a] guarantee . . . to be free from imposition by [the] government.”\textsuperscript{187} Moreover, Judge Marrero acknowledged that in order “[t]o

\begin{itemize}
\item \textsuperscript{178} Ashcroft, 334 F. Supp. 2d at 478–79 (citation omitted).
\item \textsuperscript{179} Id. at 479.
\item \textsuperscript{180} The ACLU is an organization that advocates for individual rights and liberties. \textit{See} American Civil Liberties Union, About Us, http://www.aclu.org/about/index.html (last visited Feb. 14, 2006) [hereinafter Challenge to NSL Authority].
\item \textsuperscript{181} \textit{See} Ashcroft, 334 F. Supp. 2d at 475, 479.
\item \textsuperscript{182} Id.; American Civil Liberties Union, Challenge to National Security Letter Authority, (Sept. 29, 2004), http://www.aclu.org/safefree/patriot/17458res20040929.html.
\item \textsuperscript{183} Ashcroft, 334 F. Supp. 2d at 495–96.
\item \textsuperscript{184} Id. at 500.
\item \textsuperscript{185} Id. at 475 (quoting 18 U.S.C. § 2709 (Supp. 2003)).
\item \textsuperscript{186} Id. at 506.
\item \textsuperscript{187} Id. at 476.
\end{itemize}
perform its national security functions properly, government must be empowered to respond promptly and effectively to public exigencies as they arise,” while at the same time “maintain a reasonable measure of secrecy” when conducting its investigations. Consequently, such a race will inevitably cause a collision between securing the nation and protecting Fourth Amendment freedoms.

Expounding on those principles, Judge Marrero recognized that the temptation to dispense with such freedoms was arguably grounded given the emotional aftermath of 9/11. However, in addressing the Government’s reach to combat terrorism, Judge Marrero declared that the “state of war is not a blank check” to dispense those rights so clearly grounded in the core of the Constitution. Therefore, because “longstanding Supreme Court doctrine makes clear” that Fourth Amendment guarantees are fundamental to the democratic system, § 2709 “must be invalidated because . . . it has the effect of authorizing coercive searches effectively immune from any judicial process.” Thus, the decision rendered in Ashcroft suggests that expanding the FBI’s investigative power to seek personal information without judicial oversight, even during times when national security is at its apex, is likely unconstitutional since such authority allows for abuse of Fourth Amendment rights.

VI. RECOMMENDATION

Applying the abovementioned Supreme Court jurisprudence to § 2709, as amended by the USA PATRIOT Act, clearly infringes on our Fourth Amendment rights. However, the technological innovations used by the terrorists to plan and plot the events of 9/11 clearly were not within contemplation of the Supreme Court at the time it rendered those pre-9/11 decisions. Yet what is clear from the Court’s rulings is that it is necessary to preserve both liberty and security and not compromise one for the other.

188. Ashcroft, 334 F. Supp. 2d at 476.
189. See id. at 477.
190. See id. at 477–78.
191. Id. at 477 (quoting Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004)).
192. Id. at 495.
193. Ashcroft, 334 F. Supp. 2d at 506.
194. See id. at 501.
195. See supra Parts II-V.
197. See id.; see also Ashcroft, 334 F. Supp. 2d at 495, 506 (concluding that § 2709 violates the Fourth Amendment as applied).
Based on that premise, this article proposes several possible checks which could be placed on the FBI in fighting the war against terrorism, while at the same time preventing erosion of Fourth Amendment protections.

A. Prior Judicial Approval

First, Congress could redraft § 2709 to limit the FBI’s current unchecked ability to issue national security letters. One way of accomplishing this goal would be to include a provision which allows for judicial approval of national security letters before the FBI issues them. Although doing so would inhibit the FBI’s need for secrecy in terrorism investigations because of the likelihood that the information will be overheard by the judge’s clerks or staff, it would better protect Fourth Amendment rights. Under this approach, the “coercive searches” that Judge Marrero mentioned would be at a complete minimum, since a neutral judge or magistrate could objectively determine whether or not there was probable cause to demand customer records from communications firms.

B. Post Judicial Oversight

Alternatively, Congress could also draft the provision to mandate judicial oversight after the national security letter is received. Although there is a heightened possibility of infringing upon Fourth Amendment rights because of the possibility that the information could be leaked by the judge’s employees, this approach at least ensures that the primary purpose of the government’s investigation is to secure intelligence information relating to terrorism investigations. Moreover, such a requirement would make certain that the government is not using the national security letters as a means of obtaining information solely to conduct domestic intelligence investigations.


201. See id. at 606.

C. The Keith Approach

In Keith, as mentioned above, the Supreme Court recognized that the warrant requirement “may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.” In dicta, the Court suggested that it may be willing to approve a different standard by which to obtain probable cause in domestic security situations. Thus, because in terrorism investigations it is unclear whether the government’s interest is truly “domestic” or “foreign,” lowering the probable cause standard may meet the reasonable needs of the FBI. Like the Prior Judicial Approval approach, the Keith approach would prevent “coercive searches,” since judicial approval would still be required, just at a lower standard of reasonableness. Moreover, like the Post Judicial Oversight approach, this approach would ensure that the issuance of national security letters truly pertained to terrorism investigations.

VII. CONCLUSION

Prior to 9/11, “[t]errorism was not the overriding national security concern for the U.S. government.” The government never had a need to develop the tools necessary to thwart plots of overthrowing the government and in turn, the democratic system. As a result, the attacks of 9/11 transformed the nation and eventually transformed the FBI’s communications to counteract terrorism operations. Congress responded by enacting the USA

---

206. Id. Specifically, the Court stated:
   It may be that Congress, for example, would judge that the application and affidavit showing
   probable cause need not follow the exact requirements ... but should allege other circum-
   stances more appropriate to domestic security cases; that the request for prior court authoriza-
   tion could, in sensitive cases, be made to any member of a specially designated court ... and
   that the time and reporting requirements need not be so strict ....

208. See, e.g., Butenko, 494 F.2d at 606; United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); Noro v. United States, 148 F.2d 696, 699 (5th Cir. 1945).
209. See Keith, 407 U.S. at 323.
211. See Keith, 407 U.S. at 323.
212. See Butenko, 494 F.2d at 603-06; Keith, 407 U.S. at 323. But see Smith, 321 F. Supp. at 424.
213. EXECUTIVE SUMMARY, supra note 1, at 10.
214. See id. at 6-10.
215. See id. at 13.
PATRIOT Act which provided the FBI with investigative tools to shield the nation from another 9/11 experience.\(^{216}\) However, the government may have gone too far because it took away certain liberties in order to protect such freedoms in the name of national security.

When Congress amended 18 U.S.C. § 2709 through the USA PATRIOT Act, it gave the FBI unchecked power to infringe on Fourth Amendment rights.\(^{217}\) Specifically, § 2709 authorized the FBI to issue national security letters to obtain a person's private information from an internet service provider or telephone company without satisfying Fourth Amendment requirements of probable cause and judicial authorization.\(^{218}\) At the time, Congress' reasons for compromising Fourth Amendment protections seemed justified, considering the state of the nation after 9/11.\(^{219}\)

Three years after 9/11 and the enactment of the USA PATRIOT Act, the ACLU and an unknown internet service provider fought to protect the dissemination of Fourth Amendment rights by challenging the constitutionality of § 2709.\(^{220}\) Standing up for those rights, Judge Victor Marrero ruled that Fourth Amendment protections cannot be guaranteed solely within the discretion of the FBI because Supreme Court doctrines demonstrate that the "state of war is not a blank check"\(^{221}\) to infringe upon the rights of American citizens.\(^{222}\)

In a post-9/11 world, technological innovations will continue to threaten personal privacy. Therefore, it is clear that Congress needs to set boundaries concerning law enforcement's ability to secure the nation from future terrorist attacks. The suggestions mentioned above will provide an effective way to conduct terrorism investigations, while at the same time protect against future attacks on Fourth Amendment rights.

\(^{216}\) Remarks by President Bush at PATRIOT Act Signing, supra note 20.


\(^{218}\) See id. at 495–97.

\(^{219}\) See id. at 477–78.

\(^{220}\) Challenge to NSL Authority, supra note 180.

\(^{221}\) Ashcroft, 334 F. Supp. 2d at 477 (quoting Hamdi v. Rumsfeld, 524 U.S. 507, 536 (2004)).

\(^{222}\) Id.