Open Access Library Journal
2025, Volume 12, e14179
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Foreign Intelligence Surveillance Act in Light of the United States Fourth Amendment

Seyed Milad Kashefi Pour Dezfuli

College of Law, Florida International University, Miami, USA
Email: skash009@fiu.edu

How to cite this paper: Dezfuli, S.M.K.P. (2025) Foreign Intelligence Surveillance Act in Light of the United States Fourth Amendment. *Open Access Library Journal*, **12**: e14179.
https://doi.org/10.4236/oalib.1114179

Received: August 28, 2025
Accepted: October 14, 2025
Published: October 17, 2025

Copyright © 2025 by author(s) and Open Access Library Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

This paper examines the evolving relationship between the Fourth Amendment's protection against unreasonable searches and seizures and the U.S. government's use of electronic surveillance in the name of national security. It traces the historical expansion of surveillance authority, beginning with early wiretapping cases and culminating in the enactment and evolution of the Foreign Intelligence Surveillance Act (FISA). The analysis highlights the legal tension between the executive branch's national security prerogatives and constitutional safeguards for U.S. persons, focusing on how courts have justified exceptions to warrant requirements through doctrines such as "special needs." It explores key cases like *Katz*, *Keith*, *Truong*, and *In re Sealed Case*, which shaped the balance between privacy rights and intelligence gathering. The paper also discusses the post-9/11 amendments to FISA under the USA PATRIOT Act, which shifted the threshold for permissible surveillance by lowering the requirement from "primary purpose" to "significant purpose" in foreign intelligence investigations. Finally, it considers ongoing legal controversies regarding warrantless surveillance programs and the implications of these developments for the future of constitutional privacy protections.

Subject Areas

Law

Keywords

United States Fourth Amendment, Electronic Surveillance, Foreign Intelligence Surveillance Act [FISA], National Security Law

1. Introduction

The Fourth Amendment to the United States Constitution prohibits the govern-

ment's unreasonable searches and seizures. Historically, the Amendment has been understood as requiring the government to obtain a warrant prior to making arrests or conducting searches in criminal investigations. An independent magistrate should issue a warrant for arrest or search based on a probable cause determination. Probable cause means that law enforcement agents have a reasonable belief that someone is engaged in criminal activities or evidence of crime will be found in the place to be searched.

The 1960s and 1970s witnessed the crux of the United States Supreme Court's rulemaking surrounding the Fourth Amendment's reasonable search and seizure protections. In *Mapp v. Ohio*, the Court provided for a remedy against government violation of constitutional protections by excluding evidence obtained through unreasonable searches and seizures. While the Court also recognized several categories of exceptions to the warrant requirement, its landmark decisions during these two decades established a strong analytical framework that still governs criminal investigations in the country.

The foreign intelligence collection is presumed to be an exception to the warrant requirement under the Fourth Amendment. Congress passed the Foreign Intelligence Surveillance Act [FISA] in 1978 in recognition of the government's compelling interest in surveilling the operations of foreign-connected persons in the United States. While Congress acknowledged that the government's interest must be balanced against the privacy rights of U.S. persons, the Act devised a legal framework different from the constitutional protections for ordinary criminal investigations in cases of foreign intelligence gathering.

FISA and its amendments, including the U.S. Patriot Act of 2001 [the Patriot Act], and FISA Amendment Act of 2008, provide for a much slimmed-down procedure for the judicial oversight of the government's surveillance operations against foreign-connected persons [including U.S. persons]. In recent years, many Americans and civil rights activists have been concerned about the government's intrusion into privacy in the name of national security. Following 9/11 the government enacted laws amending FISA and implemented policies that the critics argue would seriously impinge on the privacy rights and civil liberties of U.S. persons [1].

Chief among concerns is that the Patriot Act strikingly expands the government's surveillance powers. The Act authorized the government to carry out searches and gather intelligence on U.S. persons without obtaining a warrant, without a probable cause determination, and simply by showing that access to the information is related to an unspecified investigation. The critics point out the repercussions of the Act on the Fourth Amendment protections and the due process requirements [2].

In the years immediately after the 9/11 attacks, the National Security Agency (NSA) started a warrantless program to wiretap phone calls and emails both inside and outside the U.S. territory. The government argued that the program was necessary for its counterterrorism efforts but the fact that most of the data collection

operation was conducted beyond even the slightest measure of judicial oversight was concerning. The same agency ran another warrantless program called PRISM in which it collected vast amounts of information [emails, text messages, social media chats, photos, and other personal information] from major U.S. tech companies without probable cause determination or judicial oversight [3].

Finally, a host of new technologies and police practices such as police body cameras, closed-circuit television (CCTV) cameras, and surveillance drones, though necessary for effective law enforcement and security, have created new sources of worry for the Fourth Amendment protections against unreasonable searches and seizures and the U.S. citizens' privacy rights. One notable objection to such modern practices is that they allow "suspicion-less" searches that violate even the lowest standards applicable under lawful exceptions to the Fourth Amendment's warrant requirement [4].

Although, in some cases, the government operated completely outside judicial oversight, in many other cases, it complied with the requirement of informing undergoing investigations to the Foreign Intelligence Surveillance Court [FISC]. The critics argue that meager procedural arrangements provided for by the FISA Act of 1978 under which the FISC courts were established are barely sufficient to ensure that constitutional protections of the Fourth Amendment are respected [5].

This paper investigates the changes to foreign intelligence-gathering operations in the aftermath of the 9/11 attacks in light of the U.S. Patriot Act and recent practices. The paper begins by investigating the historical development of the rules surrounding the Fourth Amendment protections against unreasonable searches and seizures. The second section studies the Congress FISA Act in 1978 which applied an analytical framework on foreign intelligence-gathering operations substantially different from the one applicable to ordinary criminal investigations. The section later reviews some of the courts' decisions under FISA prior to 9/11. The stringent separation that FISA and subsequent courts' decisions created between counterintelligence operations and the criminal investigation was believed to be a major impediment that thwarted effective response to the 9/11 attacks [6]. The U.S. Patriot Act was designed as a response to that deficiency. The final section of this paper looks into the Patriot Act and surveys the courts' rulings in the aftermath of the Act. The purpose will be to understand how the framework established by FISA changed following the enactment of the Patriot Act.

2. Historical Development

The Fourth Amendment to the United States Constitution states:

> "The 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."

The courts will determine the constitutionality of searches conducted by government actors by assessing whether it was reasonable in light of the circumstances in which it was conducted. A search pursuant to a warrant issued by a neutral magistrate after a determination of probable cause is presumptively reasonable.

However, places and objects protected by constitutional rights were largely confined to physical ones before the 1930s. During the 1920s, for example, the Court refused to exclude evidence obtained by warrantless wiretapping of the defendants' phone conversations in a case involving violations under the prohibition laws. The massive expansion in the government's wiretapping activities led the Court in the late 1930s, to recognize wiretapping as an unreasonable search and seizure. The case made an exception for permissible intrusions in matters of national security by limiting the rule against wiretapping to ordinary criminal investigations.

Fears of Communist sabotage, espionage, subversion attempts, and cooperation with foreign hostile powers at the end of World War II provided much impetus for the government to invoke national security in justifying information gathering from U.S. persons by way of wiretapping or other electronic methods.

The theoretical justification of excluding matters of national security from constitutional protections against unreasonable searches rested on a presumptive difference between the role of the President as the chief executive responsible for upholding the laws of the United States and also the commander-in-chief tasked with defending the nation against threats [7]. Congress yielded to urgency by avoiding tying the President's hand in matters of national security through legislation, thus, placing the issue well within the realm of the second prong in Justice Jackson's famous framework. The U.S. intelligence agencies seized the opportunity by unleashing their full force against U.S. persons suspected of collaborating with foreign Communist powers in the 1950s and early 1960s.

The mid and late 1960s witnessed a surge in the Supreme Court's rulemaking in regard to constitutional protections against unreasonable searches and seizures. The seminal Katz decision restricted the use of the government's electronic surveillance by recognizing it as a violation of the Fourth Amendment protections. But Justice White wrote in his concurring opinion that: "if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.", an investigation into matters of national security should not require a warrant.

Shortly after the *Katz* decision, Congress passed the Omnibus Crime Control and Safe Streets Act which regulated the process of obtaining warrants for electronic surveillance in criminal investigations. However, Congress demonstrated its reluctance to constrain the government in matters of national security in Title III of the Act. Title III endorsed, as a matter of policy, the presidential powers by permitting warrantless electronic surveillance in matters:

> "1) necessary to protect the nation against actual or potential attack or any other hostile action of a foreign power; 2) necessary to obtain foreign intelligence information deemed essential to the security of the United States; 3) necessary to protect national security information against foreign intelligence activities; 4) necessary to protect the United States against the overthrow of the Government by force or other unlawful means; or 5) necessary to protect the United States against a clear or present danger to the structure or the existence of its Government.".

In the years following the Omnibus Act and amid public outcry over the war in Vietnam, a number of controversial cases revealed dissatisfaction with the government's targeting of U.S. citizens' rights to privacy in the name of national security. The determination in *United States v. Clay*, that federal courts lack sufficient information to decide about matters of national security did not end public anger over the recording and overhearing of Mohammad Ali Clay's conversations by FBI agents. In another case, *United States v. Enten*, the court held that only the executive branch possesses the knowledge to assess the reasonability of electronic surveillance conducted in matters of national security.

Such extreme opinions resulted in a judicial backlash aimed at distinguishing between electronic surveillance when conducted in response to perceived domestic threats and when carried out to deal with foreign threats. In *United States v. Smith*, the court held that when the issue at stake is domestic political activity, "the government can act only in limited ways.". The matters came to a head with *United States v. Sinclair*, in which Judge Keith ruled that when domestic groups are targets of a national security investigation, they shall be given the protections of the Fourth Amendment. When the issue went up to the Supreme Court, the justices of the Court affirmed Judge Keith's decision by refusing to recognize an exception to the warrant requirement in national security cases. The Supreme Court decision specifically left foreign intelligence gathering outside the realm of the Fourth Amendment.

The *Keith* decision set the stage for later developments of the law in regard to foreign intelligence gathering by foreign-connected agents. Since the Attorney General was the official responsible for reviewing requests for warrantless electronic surveillance in such situations, the Department of Justice introduced factors such as financing, control, or active collaboration by a foreign government in granting requests for electronic surveillance. Several cases in the early and mid-1970s consolidated the trend established and reproduced the arguments made by *Keith*.

In *United States v. Brown*, the court found that the President's constitutional duty to lead foreign affairs and protect the nation removes the requirement for obtaining a warrant in foreign intelligence gathering matters. In *United States v. Butenko*, the court maintained that the defendant's conviction based on evidence obtained through warrantless surveillance was lawful because he was a spy gathering intelligence for a foreign government. *United States v. Buck*, expressly found

an exception to the Fourth Amendment's warrant requirement for foreign intelligence gathering cases. Finally, in *United States v. Troung Dinh Hung*, the last major case decided before the passage of the Foreign Intelligence Surveillance Act [FISA] and under a separation of power argument, the court held that obtaining a warrant for foreign intelligence gathering investigations would "unduly frustrate" the executive branch efforts in protecting the nation. However, in its use of the phrase "unduly frustrate", the *Troung* Court also paved the way for a quite different argument in favor of excluding foreign intelligence gathering from the warrant requirement of the Fourth Amendment.

3. Special Needs Doctrine

Generally speaking, the exceptions to the warrant requirement that the Supreme Court began to recognize after the mid-1960s fell within two major categories. Most of the exceptions still required standards comparable (reasonable belief) or less stringent than probable cause (reasonable suspicion). In another, smaller category of exceptions, what the Supreme Court later referred to as "constitutionally permitted suspicion-less searches" justified exclusion from the normal requirements of the Fourth Amendment.

The special needs doctrine permits searches where no particular suspicion exists and where the search's purpose is something beyond law enforcement's normal functions (crime detection). The doctrine has been traditionally invoked to allow for government administrative or public safety searches. The argument in such cases is that requiring a warrant would be impracticable because it "unduly frustrates" the government's proposed search. The doctrine, furthermore, argues that suspicionless searches are different from the usual constitutionally regulated searches since the primary purpose in administrative or public safety investigations is not to turn over the evidence uncovered to law enforcement agencies in order to bring criminal charges against the violators.

The cases above were decided pursuant to a precedent established by the Supreme Court in *Camara v. Mun. Ct*. There, the Court found that states' interest in preventing public hazards would allow administrative searches for non-law enforcement purposes without the constitutional requirements of a warrant or probable cause determination. In *Camera*, the Court tried to distinguish between warrantless administrative searches and the usual criminal investigations by expressly providing that the former cannot be conducted to obtain evidence for crimes.

Public safety is another justification commonly invoked to justify warrantless searches without probable cause. In *Chandler v. Miller*, the Court provided that substantial and real risks would make warrantless searches reasonable under the Fourth Amendment; however, the constitutional protections will not be precluded if the risks are not genuine. In *Skinner v. Ry. Labor Execs.' Ass'n*, the Court recognized the danger of railway crashes as one such example of substantial and real risks under the special need doctrine. The doctrine requires a significant non-law enforcement purpose to carry out searches. In *Skinner*, the Court acknowledged

that the purpose of taking blood tests from the employees in the railway industry is not "to assist in the prosecution", but rather "to prevent accidents and casualties in railroad operations that result from impairment of employees by alcohol or drugs".

4. Foreign Intelligence Surveillance Act of 1978

The Supreme Court in the *Keith* decision indicated a willingness to recognize an exception to the Fourth Amendment requirements for foreign intelligence gathering by stating that lower standards than probable cause might be reasonable where the subject of investigations is foreign-connected agents. At the heart of the Act lies a lower standard than probable cause and the warrant requirement of the Fourth Amendment in conducting electronic surveillance against foreign-connected agents, including U.S. persons suspected of acting on behalf of foreign governments and organizations.

Prior to FISA disagreements existed about whether the foreign intelligence gathering exception should be justified entirely by a constitutional argument based on Article II and the separation of powers or based on a statutory ground recognizing an exception to the requirements of the Fourth Amendment. Congress, in passing FISA, responded to the dispute. Although the Act refused to explicitly incorporate a special needs doctrine language, it provided for a limited measure of judicial oversight in cases involving foreign intelligence gathering.

FISA created a special procedure for application by the government and approval by the judiciary of orders authorizing the use of electronic information gathering against targets suspected of working on behalf of foreign governments and organizations. The Act accomplished its objective, in part, by establishing a standard of review for FISA applications and issuance of orders for electronic surveillance. In reviewing the applications submitted by the Attorney General, the courts should have ensured 1) whether the government believes that "the target of the electronic surveillance is a foreign power or an agent of a foreign power", 2) "each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent"; and 3) "the information cannot be obtained through normal investigative techniques.".

The FISA standard of review departs from a Fourth Amendment standard by removing the necessity to show that a criminal activity has been committed or is about to be committed. An application to order electronic surveillance under FISA will be granted if probable cause exists to show that the target of the surveillance "is a foreign power or an agent of a foreign power." If the target is a U.S. person, FISA requires an additional showing of a nexus to criminal activity. FISA also created Federal Intelligence Surveillance Courts (FISC) to hear applications for electronic surveillance; if these courts were to refuse the application, the government could appeal their decision to the Federal Intelligence Surveillance Courts of Review (FISCR). Finally, the Act authorized the Attorney General to order emergency surveillance in cases where obtaining a judicial order would frus-

trate imminent response to national security threats.

FISA represented a legislative solution between the constitutional rights of U.S. citizens to privacy (protection against unreasonable searches and seizures) on the one hand and the government's compelling interest in gathering intelligence from foreign-connected agents on the other. The Act refused to use any language besides the unique and complex nature of national security matters in justifying a different standard of review in cases involving foreign intelligence gathering. Subsequent judicial interpretations of the FISA standard of review, however, combined this reasoning with arguments reminiscent of the "special needs doctrine". According to these judicial interpretations, the government was required to demonstrate, on a case-by-case basis, that the "primary purpose" of investigations was intelligence gathering rather than a law enforcement objective (crime detection) [8].

In the years following the passage of FISA, challenges to the constitutionality of the Act were not sustained in non-FISC courts. The courts have generally argued that since FISA strikes a reasonable balance between the government's compelling security interests and the citizens' rights to privacy, its respective standard of review does not violate the Fourth Amendment requirements.

When challenges to the constitutionality of FISA failed, arguments shifted toward questioning the validity of the government's actions in light of the Congressional intent, and especially their conformity with the requirements of the special needs doctrine as previously established by judicial precedents. The *Troung* case mentioned above was particularly important in this respect. Although the 4th Circuit decided the case two years after the passage of FISA, it was still based on a pre-FISA context. There, the court held that foreign intelligence surveillance on U.S. persons was constitutionally permissible if the U.S. person was an agent or collaborator of a foreign power. The *Troung* court combined elements of pre-FISA Article II arguments with those of a special need doctrine. Foreign intelligence gathering was an exception to the Fourth Amendment because requiring the government to obtain a warrant in advance of the surveillance would create procedural hurdles, reduce the flexibility of counter-intelligence operations, delay the executive response to foreign threats, and increase the risk of leaks in sensitive intelligence operations. Thus, a warrant requirement would "unduly frustrate" the President in fulfilling his constitutional duties. The court also went on to add elements of the "special needs doctrine" to its analysis. It stated that in foreign intelligence gathering, the "primary purpose" of surveillance is to deal with the threats of foreign intelligence activities rather than to obtain evidence of a crime. *Troung* court's argument that foreign intelligence gathering investigations, like administrative or public safety searches, are conducted primarily for purposes beyond law enforcement, affected many subsequent decisions. Thus, it became usual practice for FISC courts to consider the nature of the intrusion imposed by foreign intelligence surveillance in assessing whether to grant applications for electronic surveillance. In more than two decades after the passage of the FISA, very few cases

have come up in which the use of the evidence obtained by FISA orders in criminal investigations became an issue. One such case is notable to mention.

In *United States v. Megahey*, the defendants moved to suppress evidence obtained through a FISA order. They argued that evidence so obtained should be used only for the purpose of foreign intelligence gathering rather than criminal prosecution. The court, however, rejected the claim that the fruits of FISA electronic surveillance cannot be used for criminal investigations since Congress, in passing FISA, was aware that evidence obtained through warrantless FISA surveillance may be used for criminal proceedings as well and did not provide for their exclusion.

The *Megahey* Court ruled that FISA surveillance did not need to stop on gathering foreign intelligence and they may well use the fruits of their investigation for criminal purposes. But by the beginning of the new millennium, the practice was well-established. The executive branch committed itself to following the special procedure outlined in FISA, which placed significant challenges on the ability to share information and the consultation between the intelligence community and the federal prosecutors. The result was the prevailing of a FISA interpretation jealously protecting the so-called wall between intelligence and law enforcement capacities through "minimization procedures" that prohibited criminal prosecutors from instructing intelligence agents on how to operate or use the fruits of their FISA electronic surveillance.

5. Post-9/11 FISA Amendments

Although Congress has amended FISA several times in the past nearly half-century, the most important changes came with the 9/11 attacks. The authors of the Congress-mandated National Commission on Terrorist Attacks Upon the United States believed that the FISA-created wall between intelligence gathering and law enforcement was a major contribution to the failures of security agencies [9]. The Commission also proposed that the international war on terrorism created a need for collecting intelligence from domestic targets, and the President should be able to employ a wide variety of tools, including prosecution for domestic crimes, in the war against foreign terrorist organizations.

Pre-9/11 prevailing interpretation of FISA had allowed for warrantless surveillance only where the "primary purpose" of the investigations was to gather foreign intelligence. After 9/11 an amendment to FISA under the U.S.A. Patriot Act permitted greater ease in securing FISA surveillance orders by removing the requirement of showing that the primary purpose of surveillance was to gather foreign intelligence. The change in wording from "a primary purpose" to "a significant purpose" opened the possibility of using the information obtained by FISA surveillance for criminal prosecutions. The Act also allowed the sharing and disclosing of information obtained through FISA surveillance to federal officials and grand juries

Under the Patriot Act, a FISA order could now "be used primarily for a law

enforcement purpose, so long as a significant foreign intelligence purpose remain[ed]." Permitting criminal prosecutions with a probable cause standard wildly thinner than what the Constitution required was bound to be challenged in courts.

Despite doubts about the constitutionality of the amendments made by the Patriot Act, FISC courts continued to issue and uphold surveillance orders that could be used to gather admissible criminal evidence. In re *Sealed Case*, FISC acknowledged that the procedure established under FISA might not meet the Fourth Amendment minimum requirements but concluded that it is still constitutional. The FISC court held that FISA provides safeguards in the form of determination of probable cause by a neutral magistrate based on the particular description of what to be searched; FISC acquiesced that these safeguards are different from the ones established by the Fourth Amendment but held that they are still and come close to constitutional criminal warrants. Criticizing the "wall" that had been created between intelligence gathering and law enforcement functions by the pre-9/11 interpretation of FISA, the FISC found that the use of evidence obtained by FISA surveillance orders was even constitutional under the original text of FISA. In light of the changes made by the Patriot Act [gathering foreign intelligence being a significant, rather than a primary purpose], the fruits of FISA surveillance can certainly be used for the purpose of criminal proceedings.

The overarching conclusion of the *Sealed Case* was to eliminate many bureaucratic and procedural bulwarks created by earlier rulings of FISC courts. In an environment characterized by heightened security concerns, FISC made a strong case for better communication between the intelligence community and law enforcement, and it also allowed the use of evidence for criminal investigations in national security cases that had not been obtained by regular means warranted by the Fourth Amendment.

When challenges to the constitutionality of the Patriot Act provisions found their way into federal courts, they, too, refused to entertain such arguments. *Mayfield v. United States*, was a rare exception among rulings in federal courts that briefly considered some of the arguments about the constitutionality of the Patriot Act. There, the plaintiffs moved to suppress fingerprint evidence obtained by FISA surveillance order that included a physical search of one of the plaintiff's home as well as electronic surveillance. The *Mayfield* court started its analysis by acknowledging that the purpose of the post-9/11 amendments to FISA was to do away with barriers between law enforcement and intelligence gathering. However, the court refused to uphold the government's arguments based on the special needs doctrine by pointing out that national security is not one of the grave concerns that justifies an exemption from the Fourth Amendment warrant requirements. The Mayfield court's decision was vacated in the appeals court. However, the Ninth Circuit did not challenge the decision on merits; it simply used a settlement agreement between the plaintiffs and the government to argue that the plaintiffs did not have any standing to bring the case.

6. Later Developments

The courts' position that the Patriot Act does not violate the Fourth Amendment's minimum requirements did not stop controversies over the constitutionality of the special procedure for foreign intelligence gathering established by FISA and its amendments.

In 2005 American media reported that the United States government had been engaged, for some years, in a massive surveillance program targeting the international communications of American citizens without obtaining warrants under FISA or its later amendments [10].

The government defended the program by raising two arguments. First, the government invoked an Article II argument by stating that the President has a constitutional duty, as commander-in-chief, to protect the nation; the President's constitutional duty warrants gathering foreign intelligence at a time of war even through unregulated surveillance. Second, the government insisted that the FISA text does not bar the government from gathering foreign intelligence in ways not specifically provided for in FISA [11].

Despite heated political controversy over the program and the dubious nature of the government's arguments, neither Congress nor the judiciary showed any willingness to curb the actions of the executive branch. Congress did not move to challenge the legality of massive surveillance programs in further amendments of FISA in 2008. The FISC courts, too, reiterated their earlier position that a lighter probable cause standard in foreign intelligence gathering cases is reasonable given the special characteristics of such cases that "take [them] out of the strict rigors of a warrant requirement".

The cases have not fared better in federal courts. Given the secret nature of surveillance programs conducted by the government, it is difficult to prove injuries that establish standing for the plaintiffs. In at least one exception, the plaintiffs argued that the National Security Agency's warrantless electronic surveillance program violated the Congressional intent because FISA required the government to obtain FISC orders to gather foreign intelligence. The lower court held that there was insufficient evidence to uphold charges against the plaintiffs. However, the Sixth Circuit overturned the ruling on a standing argument. The Appeals court argued that the plaintiffs could not show that they had been subject to the alleged electronic surveillance programs.

7. Conclusions

The idea that the President's power to gather foreign intelligence should not be limited by constitutional requirements has always found strong support in Congress and among judges. The beginning of a war with a treacherous enemy equipped with a global network rooted across and beyond national borders only strengthened the urge not to tie the President's hand. Thus, the Patriot Act combined the President's powers as both the commander-in-chief and the chief law enforcement officer.

The problem occurs when the proponents of the idea fail to base it on sound constitutional grounds. The government lawyers and the procedures established to obtain warrants for surveillance invoke the tenants and the language of the "special needs doctrine" liberally, while the text of the law or the rulings of the courts refuse to acknowledge foreign intelligence gathering as something similar to other categories subject to the doctrine. Their reluctance to sustain arguments based on the "special needs doctrine" seems to be sound given the fact that nothing in the procedure required under FISA or the nature of the foreign intelligence gathering cases themselves meets the doctrine's standards, including the need to provide notice before conducting searches, or the need for a purpose beyond criminal prosecution.

Under such circumstances, invoking the President's constitutional power and duty to defend the nation appears to be the most logical solution. The critics of FISA and its later amendments, however, argue that the law, especially in its application to U.S. persons, gives the President too much power at the expense of individuals' constitutional rights and protections. The concern is that FISA courts will become "a rubber stamp for the Justice Department, potentially eroding both privacy and the separation of powers."

Another concern with an Article II argument to justify the presidential powers in gathering foreign intelligence is that such a power is not enumerated in the Constitution. In fact, the absence of such a power led to the passage of FISA in 1978 in which Congress provided a proper statutory ground for electronic surveillance conducted with a warrant requirement and probable cause standard widely different from the Fourth Amendment's. Furthermore, many specific governmental actions in the wake of the 9/11 attacks have violated even the minimal standards established by FISA and its later amendments.

In light of Congress's or the judiciary's unwillingness to constrain the presidential exercise of power in foreign intelligence gathering even in the face of serious violations after 9/11, it appears unlikely that concerns over the individuals' privacy rights or constitutional protections would prevail in the absence of a major political or security paradigmatic shift.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] American Civil Liberties Union (2001) Surveillance under the USA/Patriot Act. https://www.aclu.org/documents/surveillance-under-usapatriot-act

[2] Electronic Privacy Information Center: USA Patriot Act: Overview & Legal Analysis. https://epic.org/issues/surveillance-oversight/patriot-act/

[3] Greenwald, G. (2013) NSA Collecting Phone Records of Millions of Verizon Customers Daily. The Guardian. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[4] Kerr, O.S. (2004) The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. *Michigan Law Review*, **102**, 801-888. https://doi.org/10.2307/4141982

[5] Balkin, J.M. (2008) The Constitution in the National Surveillance State. *Minnesota Law Review*, **93**, 1-25.

[6] (2004). The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States. https://govinfo.library.unt.edu/911/report/911Report.pdf

[7] Gonzalez, J.A. (2005) Constitutional Aspects of Foreign Affairs: How the War on Terror Has Changed the Intelligence Gathering Paradigm. *Naval Law Review*, **51**, 289-294.

[8] Cinquegrana, A.R. (1989) The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978. *University of Pennsylvania Law Review*, **137**, 793-828. https://doi.org/10.2307/3312277

[9] 9/11 Commission Report. https://govinfo.library.unt.edu/911/report/911Report.pdf

[10] Risen, J. and Lichtblau, E. (2005) Bush Lets U.S. Spy on Callers without Courts. TIMES. http://www.nytimes.com/2005/12/16/politics/16program.html?page-wanted=all&_r=0

[11] Gonzales, A. (2006) Legal Authorities Supporting the Activities of the National Security Agency Described by the President. U.S.DEP'T of Just.

Appendix

Cases

Weeks v. United States, 232 U.S. 383, 390 (1914).

Johnson v. United States, 333 U.S. 10, 14 (1948).

Jones v. United States, 362 U.S. 257, 260 (1960).

Brinegar v. United States, 338 U.S. 160, 175 (1949).

Terry v. Ohio, 392 U.S. 1, 64 (1968) (Douglas, J., dissenting) (defining probable cause as a belief that a crime was committed, or in the process of committing, or is about to be committed).

Map v. Ohio, 367 U.S. 643, 649 (1961).

Arizona v. Gant, 556 U.S. 332, 339 (2009) (search incidental to a lawful arrest).

Lange v. California, 594 U.S. 295, 299 (2021) (exigent circumstances).

United States v. Ross, 456 U.S. 798, 799 (1982) (vehicle search).

Horton v. California, 496 U.S. 128, 134 (1990) (plain view doctrine).

Georgia v. Randolph, 547 U.S. 103, 110 (2006) (consent).

United States v. Moalin, Brief of Amicus Curiae Brennan Center for Justice, et.al. in support of the defendant-appellant, No. 13-501572, 2015.

Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).

Olmstead v. United States, 277 U.S. 438, (1928).

Nardone v. United States, 308 U.S. 338, (1939).

Socialist Workers Party v. Att'y Gen. of United States, 642 F. Supp. 1357 (S.D.N.Y. 1986) (giving a historical overview of domestic intelligence gathering in the United States).

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 611 (1952) (Jackson, J., concurring).

Katz v. United States, 389 U.S. 347, (1967).

Katz v. United States, 389 U.S. 347, 363 (1967) (White, J., concurring).

United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970).

United States v. Enten, 388 F. Supp. 97, 98 (E.D. D.C. 1971).

United States v. Smith, 321 F. Supp. 424 (C.D. Ca. 1971).

United States v. Sinclair, 321 F. Supp 1074, 1080 (E.D. Mich. 1971).

United States v. United States District Court, 407 U.S. 297, 302 (1972) [the case is also known as the *Keith* case].

United States v. Brown, 484 F.2d 418 (5th Cir. 1973).

United States v. Butenko, 494 F.2d 593, 604 (3d Cir. 1974).

United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977).

United States v. Troung Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

Chandler v. Miller, 520 U.S. 305, 309 (1997).

New Jersey v. T.L.O, 469 U.S. 325, 351 (1985).

Vernonia Sch. Dist. v. Acton, 515 US 646, 657-60 (1995); and *Ferguson v. City of Charleston*, 532 U.S. 67, 79 (2001).

Camara v. Mun. Ct., 387 U.S. 523 (1967).

Colonnade Catering Corp. v. United States, 397 U.S. 72, 90 S. Ct. 774 (1970) (finding that suspicionless searches of closely regulated businesses are a type of permissible administrative searches).

Illinois v. Lidster, 540 U.S. 419, 420 (2004) (ruling that search checkpoints at airports are permissible).

Chandler v. Miller, 520 U.S. 305, 323 (1997).

Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 620-21 (1989).

Nat'l Treasury Emps. v. Von Raab, 489 U.S. 656, 666 (1988) (finding that deterring drug use among the employees of U.S. Customs Service whose responsibilities are related to illegal substance detection is a special need that requires mandatory blood tests without probable cause).

United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987) (arguing that FISA's probable cause standard satisfies the requirements of the Fourth Amendment).

United States v. Duggan, 743 F.2d 59, 73 (2d Cir.1984) (finding that FISA procedures are a constitutionally adequate balancing of the citizens' constitutionally protected rights to privacy against the nation's need to obtain foreign intelligence gathering).

United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987).

United States v. Nicholson, 955 F. Supp 588 (E.D. Va. 1997).

United States v. Isa, 923 F.2d 1300 (8th Cir. 1991).

United States v. Ott, 827 F.2d 473 (9th Cir. 1987).

United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982).

United States v. Ott, 637 F. Supp. 62 (E.D. Cal. 1986).

In the *Matter of Kevork*, 788 F.2d 566 (9th Cir.1986).

United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982).

United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982).

United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982).

In re *Sealed Case* No. 02-001, 310 F.3d 717, 746 (FISA Ct. App. 2002).

United States v. Stewart, 590 F.3d 93, 126 (2d Cir. 2009) (holding that if the purpose of FISA surveillance order was to gather foreign intelligence, evidence of crimes obtained by surveillance can be submitted to domestic courts).

United States v. Damrah, 621 F.3d 474 (6th Cir. 2005).

United States v. Benkahla, 437 F. Supp. 2d 541 (E.D. Va. 2006).

United States v. Ahmed, 1:06-cr-0147-WSD-GGB (N.D. Ga. 2009).

Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007).

Mayfield v. United States, 588 F.3d. 1252, 1254 (9th Cir. 2009).

re *Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010-16 (FISA Ct. Rev. 2008).

ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

ACLU v. NSA, 493 F. 3d 644 (6th Cir. 2007).

Statutes

50 U.S.C. §§ 1801-1811.

107 P.L. 156, 115 Stat. 272 (2001).

110 P. L. 261, 122 Stat. 2436 (2008).

18 U.S.C. § 2511.

18 U.S.C. § 2511(3).

USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 203-18, 115 Stat. 272 (2001).

Pub. L. No. 110-261, §§701-3, 122 Stat. 2436 (codified at 50 U.S.C. § 1881 (2008)).