Foreign Intelligence, Criminal Prosecutions, and Special Advocates

PATRICK WALSH*

I. INTRODUCTION

The Snowden leaks and other revelations about the bulk foreign surveillance programs have led to significant public concern that the United States was conducting illegal surveillance programs. Lost in

the scandal over the disclosure of these massive government collection programs is the truth that these programs were presumptively lawful, at least in that they were enacted while strictly following the procedures set forth by Congress, approved by the executive, and with the approval of the judicial branch. Judicial approval of these vast programs highlights a very real problem: judicial independence is difficult to achieve in cases involving national security. There is tremendous pressure to defer to the executive branch when the security of our nation is at issue. The current system provides little adversarial oversight in intelligence matters and creates a persistent danger that the judicial branch will not act independently in matters where there is no opposing voice to counterbalance government interests.

The surveillance programs disclosed by Edward Snowden were conducted in a secret proceeding in a secret court without opposing counsel, which led to the approval of surveillance programs that vastly exceeded the scope of what Congress and the public believed were appropriate.[1] The courts and Congress have responded to the public concern over these programs, and many of the specific programs that were disclosed have been altered or abandoned. However, insufficient attention has been paid to how the intelligence community and, more importantly, the courts that must provide a check against the executive, went so very wrong in the first place. Without significant changes to the procedures for reviewing and challenging government intelligence

---

* Senior Instructor, Legal Division, United States Department of Homeland Security Federal Law Enforcement Training Center; B.A., Loyola Marymount University, 1995; J.D., University of California at Berkeley School of Law, 1998; LL.M., The Judge Advocate General's Legal Center and School, 2009; LL.M., University of Virginia School of Law, 2016. The author would like to thank University of Virginia Law Professor Tom Nachbar for his review of prior drafts of this article.

1. *See* Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, WASH. POST (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html (detailing how the surveillance files provided by Snowden reveal the extent to which the data of citizens is being collected under section 702); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (revealing that President Bush had authorized the National Security Agency to conduct surveillance on both Americans and others inside the United States without requiring a court-approved warrant).

collection, there is substantial risk that the intelligence community and secret courts will again pursue a path that is inconsistent with the values of our nation by seeking and approving unlawful surveillance programs.[2]

Recent changes to the Foreign Intelligence Surveillance Act ("FISA") in the USA FREEDOM Act have tried to address the constitutional concerns, but they are insufficient to ensure that the national security apparatus does not err in the future like it has in the recent past.[3] One of the new provisions allows the Foreign Intelligence Surveillance Court ("FISC") to appoint an amicus curiae or a special advocate to assist the court in future potentially controversial cases.[4] While this new advocate has some value, as it provides the adversarial check that is essential to ensuring judicial independence, the FISC amicus curiae is insufficient to help defendants in criminal court who are trying to challenge the admission of the evidence being used against them. Further, the criminal defendants who have suffered the consequences of government searches are in the best position to review and challenge the appropriateness of the intelligence program itself but cannot meaningfully do so.[5]

Criminal defendants can be convicted on evidence obtained using secret intelligence collection programs like those approved through FISA.[6] However, criminal defendants do not have the same ability to

---

2. Foreign intelligence has changed from information that was always intended to remain classified to potentially inculpatory evidence that will be made available for use in criminal prosecutions. This transformation to using information gathered from classified intelligence tools to evidence used in criminal prosecutions creates friction with the secretive nature of intelligence. This is most acute when evidence gathered from FISA is being challenged in a criminal case.

3. *See* USA FREEDOM Act of 2015 § 401, 50 U.S.C. § 1803(i) (2015); Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1803 (2010).

4. USA FREEDOM Act of 2015 § 401, 50 U.S.C. § 1803(i) (2015) (amending Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1803 (2010)).

5. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 436–38 (9th Cir. 2016) (finding that although the government did not disclose the methods used to obtain emails between a foreign national and the defendant as required under FISA, suppression of the emails was not required and acquisition of the emails pursuant to FISA did not violate the defendant's Fourth Amendment rights).

6. *Id.* at 423, 436 (convicting the defendant of terrorism charges with the aid of evidence gathered through FISA).

review and challenge the searches and seizures that occur through intelligence programs like a defendant challenging the lawfulness of all other searches and seizures would.[7] In order to protect the secrecy of the foreign intelligence surveillance programs, criminal defendants and their attorneys are prohibited from reviewing the affidavits and orders used to secure evidence under FISA.[8] Judges can best act with independence when there is a robust adversarial process. Due to the impairment to the adversarial system at the hands of the executive branch, judicial independence suffers.

While the USA FREEDOM Act permits an amicus curiae access to these affidavits and orders, it does so only in cases before the FISC.[9] The next step in ensuring that intelligence programs are consistent with constitutional protections is to create a panel of cleared counsel who can see the same information after indictment and challenge intelligence gathering programs where they most impact individual liberties. This would ensure judicial independence at a crucial moment, when the intelligence is being used against defendants in criminal cases.[10]

To understand the background of this problem, Part II of this article reviews the history of court involvement in national security surveillance, including development of both FISA and the FISC. Part III discusses the traditional judicial process of how criminal defendants challenge the evidence against them and demonstrates how the current federal criminal procedures severely curb the adversarial process, an essential element to independent judicial decisions. Part IV discusses how the addition of cleared counsel or special advocates at the pretrial level will significantly improve the defendant's ability to challenge both individual items of evidence and the programs used to gather them. This will ensure that judges make independent decisions derived from the adversarial process and that intelligence communities under the executive branch do not stray far beyond their Congressionally approved mandate. Finally, Part V concludes that adding this program

---

7. *See e.g.*, *id.*

8. *See e.g.*, *id.*

9. 50 U.S.C. §1803(i) (2016).

10. *See* Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES (Oct. 26, 2013), http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html.

will not cause an increased risk to national security because these types of advocates are already being used in other parts of intelligence collection efforts.

II. FOREIGN SURVEILLANCE, SECRECY, AND DOMESTIC COURTS

Intelligence gathering receives special protections in law because, by its very nature, it requires secrecy to be effective.[11] Secrecy has given way in limited occasions to other national priorities, like oversight of the intelligence community by legislative and judicial branches and even executive priorities to disclose information or programs to prosecute individuals or defend government actions.[12] Recently, secrecy has been surrendered to leaks, government disclosures, and, now, outside counsel arguing as amicus curiae before the FISC. But this recent trend away from secrecy must be viewed in light of America's historical views on secrecy of national security programs. America has struggled with the balance between the need for secrecy to protect national security and the need for accountability to protect civil liberties. Courts often have to weigh these competing interests but often do so with limited information. The history of government surveillance demonstrates this constraint on judicial independence in national security matters.

Wiretaps to gather intelligence were conducted in secret and without judicial supervision as early as the presidency of Franklin Delano Roosevelt.[13] The Federal Bureau of Investigation ("FBI") and

---

11. *See, e.g.*, Classified Information Procedures Act (CIPA), 18 U.S.C. app. § 3 (1980); Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. §§ 1801–85c (2015).

12. *See* FREDERICK M. KAISER, CONG. RESEARCH SERV., LEGISLATIVE HISTORY OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE (1978), http://www.intelligence.senate.gov/sites/default/files/leg_history_kaiser_1978.pdf.

13. *See* Zweibon v. Mitchell, 516 F.2d 594 app. at 673–74 (D.C. Cir. 1975) (en banc) (presenting a memorandum from President Franklin D. Roosevelt to Attorney General Robert Jackson authorizing the use of "listening devices" as an investigative agent against "persons suspected of subversive activities against the Government of the United States . . . ."); *see also* Herbert Brownell, Jr., *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195, 196–98 (1954) (reviewing the Supreme Court's consideration of wiretaps in the 1930s and contending that "[n]one of these decisions . . . held that wiretapping by federal officers in and of itself was illegal. . . . This may have accounted for the continued adherence to the position taken by the

other law enforcement agencies later expanded the use of these secret wiretaps with the permission of the executive and without judicial approval.[14] However, these warrantless wiretaps remained relatively rare and seldom used as evidence in criminal cases until the 1970s.[15] There was little concern or controversy in the legislative or judicial branches regarding the executive's use of these unapproved wiretaps.[16]

Prior to 1967, the courts sanctioned warrantless telephone surveillance, even criminal wiretaps, with no national security nexus.[17] In its 1928 decision in *Olmstead v. United States*, the Supreme Court held that telephone surveillance did not need judicial approval because it

---

Justice Department until 1940 that mere interception of wire communications is not prohibited . . ."). "National Security" wiretaps, which are sometimes called "foreign intelligence" wiretaps, are a government surveillance tool conducted for reasons other than traditional law enforcement purposes. They are often cited as falling within the "special needs" exception to the Fourth Amendment's warrant requirement because they are used to gather foreign intelligence or to protect the United States from a foreign threat. *See* Owen Fiss, *Even in a Time of Terror*, 31 YALE L. & POL'Y REV. 1, 25–28 (2012).

14. Memorandum from Herbert Brownell, Attorney Gen., to J. Edgar Hoover, Dir., Fed. Bureau of Investigation 1 (May 20, 1954) (advising Hoover that he could evade the Supreme Court's rejection of wiretaps in *Irvine v. California*, 347 U.S. 128 (1954) if the information gathered through a wiretap was not to be used for prosecution); Memorandum from Nicholas Katzenbach, Attorney Gen., to J. Edgar Hoover, Dir., Fed. Bureau of Investigation (Sept. 27, 1965), *quoted in* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 287 (1976), http://www.intelligence.senate.gov/sites/default/files/94755_III.pdf (setting forth guidelines for the use of wiretaps in light of "current judicial and public attitudes"); L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343, 1383 (2013) (citing Press Release, U.S. Dep't of Justice (Sept. 12, 1973)).

15. *See* Atkinson, *supra* note 14, at 1346–47.

16. *See id.* at 1347 ("[A] clear legal framework regulated the scope of national security investigations, and records reveal a palpable opinio juris—a sense of legal obligation—that governed the constitutional boundaries of security operations.").

17. *See* Olmstead v. United States, 277 U.S. 438, 458–66 (1928) (considering the Court's Fourth Amendment jurisprudence and determining that past precedent dictated that wiretapping could not amount to a search or seizure).

did not constitute a search under the Constitution's Fourth Amendment.[18] Although this created the possibility of unrestrained government telephone surveillance, the executive and legislative branches later reduced that risk by prohibiting the use of wiretaps as evidence in court proceedings.[19] This created a civil liberties "compromise" where government agents had few limitations on their ability to use wiretaps but had little incentive to do so for any purpose other than to gather foreign intelligence.[20] Intelligence searches were secret but were of limited value, since the information could not be used for a criminal prosecution.[21] The Supreme Court revised its view on wiretaps in 1967 and brought wiretaps under the protection of the Fourth Amendment while leaving open the possibility that national security wiretaps were permissible—even without court approval—in certain circumstances.[22]

---

18. *Id.* at 465–66. In *Olmstead*, law enforcement's bug was placed on telephone wires in a public area (in this case, the basement of a large office building), thus there was no physical trespass over defendants' property. *Id.* at 456–57, 465–66.

19. *See* 47 U.S.C. § 605 (1934) (amended 1996); Nardone v. United States, 302 U.S. 379, 382 (1937) (interpreting section 605 as forbidding the introduction of the contents of an intercepted telephone message into evidence); Department of Justice Appropriation Act of March 1, 1933, 47 Stat. 1381 (prohibiting the use of wiretapping as a means of obtaining evidence of violations of the National Prohibition Act).

20. *See* Atkinson, *supra* note 14, at 1346–47 ("Well into the 1970s, the executive branch assumed that the national security exception permitted only, in the words of FBI Director J. Edgar Hoover, 'purely intelligence' focused investigations.") (citation omitted). As the evidence obtained through a wiretap was inadmissible in court, the wiretap was rendered a far less useful tool in criminal investigations. Therefore, wiretaps were primarily used only by those who gathered information for its intelligence value.

21. *See id.* at 1358–87 (detailing the use of the national security exception between the end of World War II and the passage of FISA in 1978); *see also* Katz v. United States, 389 U.S. 347, 358 n.23 (1967) (refraining from determining the existence of an exception to the Fourth Amendment's warrant requirement in a situation involving national security).

22. *Katz*, 389 U.S. at 358 n.23.

A. Domestic Surveillance Begins to Need a Judge's Approval

This early need for secrecy extended to keeping intelligence surveillance activities away from the courts. That changed in 1967 when the Supreme Court altered its position on wiretaps and held that they are "searches" and must be conducted in a manner consistent with the Fourth Amendment.[23] In *Katz v. United States*, the Supreme Court determined that the FBI violated the Fourth Amendment when it obtained a telephone wiretap without first seeking a judicially authorized warrant.[24] The Court further held that searches without judicially-authorized search warrants "are per se unreasonable under the Fourth Amendment — subject only to a few specifically established and well delineated exceptions."[25] The same year as *Katz*, the Supreme Court issued two other opinions reinforcing its commitment to the principle that searches without warrants carry a presumption of unreasonableness unless they fit into a narrow group of exceptions.[26]

Katz involved a wiretap for a criminal investigation into illegal gambling that had no national security implications.[27] Nonetheless, the Court addressed national security wiretaps through dicta in its well-known "footnote twenty-three."[28] This footnote specifically raised the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involv-

---

23. *Id.* at 353.

24. *Id.* at 359. The Supreme Court overruled its prior decision in *Olmstead* when it determined that the Fourth Amendment could be violated without a physical trespass. *Id.* at 367 ("[U]ntil today this Court has refused to say that eavesdropping comes within the ambit of Fourth Amendment restrictions.").

25. *Id.* at 357.

26. *Id.*; *see* Cooper v. California, 386 U.S. 58, 59–60 (1967) (noting that a warrantless search of an automobile may be reasonable due to an automobile's mobility); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–300 (1967) (holding that a warrantless search in pursuit of an armed robber was valid as "the exigencies of the situation made that course imperative").

27. *Katz*, 389 U.S. at 354.

28. *Id.* at 358 n.23. This footnote is well-known in the national security arena because it planted the seed for the modern national security exception to the Fourth Amendment's warrant requirement. *See* Atkinson, *supra* note 14, at 1379–80 (discussing the historical significance of footnote twenty-three).

ing the national security" but did not provide an answer as the "question [was] not presented by this case."[29] This footnote suggested the possibility that agents could conduct national security and foreign intelligence searches without obtaining approval from the courts.[30]

The Court's specific mention of national security searches in a criminal case was a nod to the prior history and affirmed the belief that the need for secrecy in national security or foreign intelligence cases may outweigh the traditional need for court approval. The Court was comfortable in setting a bright line rule (that searches without warrants carry a presumption of unreasonableness) only when it carved out a potential exception for cases involving national security.[31]

A year after *Katz,* Congress provided additional support for the proposition that non-judicially sanctioned searches are still constitutional if done for intelligence or national security reasons. It enacted a broad framework for criminal wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[32] The Act specifically addressed, but did not definitively resolve, whether the executive branch could obtain wiretaps outside the Title III criminal framework for intelligence or national security reasons.[33] Congress stated that Title III was not intended to "limit the constitutional power of the President . . . to protect the Nation against actual or potential attack . . . to obtain foreign intelligence information . . . [or] to protect the United States against . . . any other clear and present danger to the structure or existence of the Government."[34] This ambiguous language allowed the executive, legislative, and judicial branches of government to each develop its own interpretation of Title III as a limitation on the executive's power to conduct warrantless surveillance.

---

29. *Katz*, 389 U.S. at 358 n.23.

30. *See* Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 273–75 (2009) (detailing how footnote twenty-three led to legislation that "seemed to suggest that 'national security' wiretaps in both domestic and international investigations could continue . . . .").

31. *Katz*, 389 U.S. at 358 n.23.

32. 18 U.S.C. § 2511 (1968).

33. *Id.* at § 2511(3) (1968), *amended by* Pub. L. No. 95-511, § 201(c), 92 Stat. 1783 (1978).

34. *Id.*

The executive branch interpreted *Katz*'s footnote twenty-three and Congress' Title III statement as tacit approval of an evolving national security exception to the warrant requirement, which was necessary to protect foreign intelligence and keep classified information secret.[35] While it is not certain, the legislative branch likely intended only to reserve this issue for later consideration, not to concede the executive had this authority.[36] The judicial branch at first showed an inclination to agree with the executive branch's analysis.[37] In *United States v. Clay*, the Fifth Circuit Court of Appeals permitted a warrantless wiretap "for the purpose of obtaining foreign intelligence information."[38] But this issue remained largely unresolved until 1972, when the Supreme Court severely limited the potential scope of a national security exception for intelligence searches.[39]

B. Keith *and the Concerns of Foreign Intelligence in Domestic Courts*

The Supreme Court intervened again to ensure that secrecy did not trump individual liberties in 1972. In *United States v. U.S. District Court (Keith)*, the Supreme Court squarely addressed the issue of whether domestic wiretaps for national security purposes required prior judicial approval. In a case now commonly referred to as *Keith*

35. Letter from John C. Keeney, Assistant Attorney Gen., U.S. Dep't of Justice, to Hugh E. Kline, Clerk of the Court, D.C. Cir. (May 9, 1975), *quoted in* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS OF INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 369–70 (1976), http://www.intelligence.senate.gov/sites/default/files/94755_III.pdf (defending the President's constitutional authority to conduct warrantless surveillance).

36. United States v. U.S. Dist. Court (Keith) 407 U.S. 297, 303–04 (1972) (interpreting Congress's intention with Title III as "[leaving] presidential powers where it found them").

37. *See* United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970) (declining to read Title III as "forbidding the President, or his representative, from ordering wiretap surveillance to obtain foreign intelligence in the national interest"), *rev'd on other grounds*, 403 U.S. 698 (1971).

38. *Id.* at 170.

39. *Keith*, 407 U.S. at 303–04.

(named after the federal district judge who wrote the lower court opinion),[40] the Supreme Court found that a national security wiretap conducted inside the United States and without a search warrant violated the Fourth Amendment.[41] In doing so, the Court created the possibility that it would permit warrantless foreign intelligence searches in future cases.

Under the facts of *Keith*, the government charged three members of the White Panther Party with the bombing of a Central Intelligence Agency ("CIA") office in Michigan.[42] The prosecution's evidence included warrantless wiretaps of one of the defendant's telephone conversations.[43] The government claimed these conversations were lawfully obtained without judicial approval because the Attorney General authorized the surveillance "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."[44]

The Supreme Court disagreed and held that "prior *judicial* approval is required for . . . domestic security surveillance."[45] However, the Court did not foreclose all warrantless national security searches, as it limited its decision to searches within the United States that did

---

40. *See id.* at 298.

41. *Id.* at 320–21; *see also* Atkinson, *supra* note 14, at 1381–84 (describing *Keith* as maintaining a "limited security exception").

42. *Keith*, 407 U.S. at 299; *see also* United States v. U.S. Dist. Court, 444 F.2d 651, 653 (6th Cir. 1971) (lower court opinion); Samuel C. Damren, *The* Keith *Case*, 11 CT. LEGACY (Historical Society for the U.S. Dist. Ct. for the E.D. Mich.), Nov. 2003, 1 (2003) (detailing a history of the facts of the case).

43. *Keith*, 407 U.S. at 300–01.

44. *Id.* at 300. This argument mirrored similar language included in Title III. *See* 18 U.S.C. § 2511(3) (1968) (amended 1978) ("Nothing contained in this chapter . . . shall limit the constitutional power of the President 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 contained in this chapter be deemed to 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.").

45. *Keith*, 407 U.S. at 324 (emphasis added). The Court softened its holding by limiting the warrant requirement to the type of domestic surveillance at issue in the case and by inviting Congress to propose "reasonable standards" that may apply in domestic national security searches. *Id.*

not involve foreign powers.[46] The Court "express[ed] no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents."[47] Once again, the need for secrecy to protect national security gave the courts reason to pause and limit their ruling to cases that did not involve intelligence gathering. *Keith* accordingly left unanswered the issue of whether a search warrant is required for a national security search involving a foreign spy or an agent of a foreign government. By refraining from addressing searches that involve foreign countries or their spies, the Court suggested that a reduced level of judicial scrutiny may be permissible in cases involving extraterritorial national security threats. After noting this potential exception, the Court clarified that, if a national security exception to the Fourth Amendment's warrant requirement does exist, it does not apply to purely domestic national security wiretaps.[48]

After *Keith*, the Nixon Administration continued to sanction foreign intelligence searches without judicial approval and applied the "national security exception" implied in *Keith* to cases involving foreign powers.[49] Lower courts also continued to affirm warrantless searches under this national security exception throughout the 1970s.[50] The Fourth Circuit went further, expanding the national security exception by sanctioning a warrantless physical search in the name of foreign intelligence gathering—even though the search was conducted pursuant to a trespass that would have been unconstitutional under *Olmstead*.[51]

---

46. *Id.* at 321–22.

47. *Id.*

48. *Id.* at 321–24.

49. Atkinson, *supra* note 14, at 1383 (citing Press Release, U.S. Dep't of Justice (Sept. 12, 1973)).

50. *See, e.g.*, United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (approving warrantless search conducted for the purpose of gathering foreign intelligence information); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) ("[T]he President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence."). *But see* Zweibon v. Mitchell, 516 F.2d 594, 651 (D.C. Cir. 1975) (en banc) (plurality opinion) ("[A]bsent exigent circumstances, *no* wiretapping in the area of foreign affairs should be exempt from prior judicial scrutiny, irrespective of the justification for the surveillance or the importance of the information sought.").

51. United States v. Truong Dinh Hung, 629 F.2d 908, 912–17 (4th Cir. 1980).

These cases establish that the courts recognized the need for flexibility in foreign intelligence cases to permit the government to protect national security and preserve the secrecy of foreign intelligence programs. These cases also demonstrate that courts can and will alter established precedent, even in national security cases. This is especially true when the adversarial process provides the court with an opportunity to review how the intelligence community is using its tools to conduct searches and seizures. These notions survived even after Congress significantly altered the foreign intelligence-gathering framework with the enactment of FISA.[52]

C. The Foreign Intelligence Surveillance Act: Preserving Secrecy with a Secret Court

In 1978, Congress passed the FISA in part to answer the *Keith* court's invitation to address the issue of developing a system to oversee government use of foreign intelligence programs while still preserving secrecy.[53] In FISA, Congress created a comprehensive statutory framework for the executive branch to obtain judicially sanctioned wiretaps to gather foreign intelligence and provide for national security.[54]

Under FISA, intelligence searches require judicial authorization by the FISC.[55] If the government wishes to intercept a communication of a targeted person inside the United States, it needs to obtain a court order from the FISC permitting the surveillance or search.[56] Colloquially, these are referred to as traditional "FISA warrants" because they function in a manner similar to standard criminal search warrants.[57]

---

52. 50 U.S.C. § 1801 (1978) (amended 2015).

53. *See* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1211, 1226–27 (2007) (detailing the historical context in which FISA was enacted). The FISA was also enacted to respond to government abuse of intelligence programs as identified by the Church Committee. *Id.*

54. § 1801. A detailed review of judicially authorized wiretaps under FISA is beyond the scope of this article, which will focus on the constitutionality of wiretaps conducted without a judicial warrant.

55. *See id.* at § 1803; Blum, *supra* note 30, at 277–80 (summarizing the procedures of the FISC and FISA Court of Review).

56. *See* 50 U.S.C. §§ 1801, 1804–05.

57. *Id.* at § 1803; Blum, *supra* note 30, at 277–80.

However, FISA does not use the word "warrant," instead calling them court "orders" or "authorizations."[58]

In order to issue a FISA order to search or surveil, the FISC judge reviewing the application must find that there is probable cause to believe the target of the surveillance is an agent of a foreign power and that the target is using the facilities that law enforcement intends to surveil.[59] The judge must also find that the minimization procedures are appropriate and that the application has the proper statements and certifications.[60] Additional requirements are necessary if the target is a "United States person."[61] The judge can issue an order that permits surveillance from ninety days to one hundred twenty days, depending on whether the target is a U.S. person.[62] Subsequent orders can be extended for up to one year.[63]

All of these orders to surveil or search are applied for ex parte, without the presence of opposing counsel. The process, an ex parte application to a judge, mirrors the process for obtaining traditional criminal search warrants and Title III electronic surveillance.[64] In traditional criminal cases, a prosecutor or law enforcement officer applies ex parte to the court through an affidavit stating that there is probable cause to believe that evidence of a crime will be located in the place to be searched.[65] The judge must make a finding that probable cause exists and approves the nature and scope of the search.[66] Electronic surveillance works in a similar manner in federal court, but in addition to the applications, the federal prosecutor must obtain approvals and cer-

---

58. *See* 50 U.S.C. §§ 1802 (authorizations), 1804 (orders).

59. *See* §§ 1805(a)(2) (for electronic surveillance), 1824(a)(2) (for physical searches).

60. *See* §§ 1805(a)(3)–(4) (for electronic surveillance), 1824(a)(3)–(4) (for physical searches).

61. *See* United States v. Mubayyid, 521 F. Supp. 2d 125, 138 (D. Mass. 2007).

62. *See* 50 U.S.C. §§ 1805(d)(1)–(2) (electronic surveillance), 1824(d)(1) (physical searches).

63. *See* §§ 1805(d)(2) (electronic surveillance), 1824(d)(2) (physical searches).

64. *See* 18 U.S.C. § 2518 (1998) (procedure for Title III wiretaps).

65. *See* § 2518(3)(a).

66. *See* U.S. CONST. amend. IV; FED. R. CRIM. P. 41.

tifications from the Department of Justice's Office of Enforcement Operations.[67] All of these procedures in federal court are ex parte procedures.[68] Traditional FISA applications thus mirror the procedures found in traditional criminal cases. However, Congress approved a new procedure in 2008 to obtain foreign intelligence information without following this traditional path of judicial approval.

D. The FISA Amendments Act of 2008: Keeping Judicial Input for Foreign Intelligence Programs

Congress sought a compromise between the executive's desire for wide latitude to surveil foreigners outside the United States and the public's concern for oversight of government programs that may intrude into American civil liberties. These concerns over government misconduct with foreign intelligence tools led to another change in FISA. Congress created a statutory process in FISA for use by the executive branch to obtain foreign intelligence. However, after the September 11, 2001, attacks on the United States, President George W. Bush authorized an alternative way for government intelligence agents to wiretap communications from Al Qaeda members to individuals within the United States.[69] In a classified executive order, the Terrorist Surveillance Program ("TSP") required high-level findings by the executive branch that the target was a member of a terrorist organization but did not require approval from a judge.[70] The TSP was conducted in secret for several years until its existence was publicly revealed by the New York Times.[71]

---

67. *See* 50 U.S.C. §§ 1802, 1804–05.

68. *See id.* at § 1805; FED. R. CRIM. P. 41.

69. *See* Public Declaration of James R. Clapper, Dir. of Nat'l Intelligence ¶ 6; Jewel v. NSA, No. 08-cv-04373, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal. Dec. 20, 2013). *See generally* Risen & Lichtblau, *supra* note 1.

70. Public Declaration of James R. Clapper, *supra* note 69, ¶¶ 35–36.

71. *See* Risen & Lichtblau, *supra* note 1 (noting that the White House had asked the New York Times not to publish its article revealing the existence of the administration's secret program); *see also* Public Declaration of James R. Clapper, *supra* note 69, ¶ 6 (stating that the existence of TSP collection activities was declassified by President Bush on December 20, 2013).

Members of Congress and the public criticized the program, characterizing it as violating federal law and the Constitution.[72] Moreover, the ACLU filed a lawsuit in federal district court. In *ACLU v. NSA*, the district court held that the TSP violated both the Fourth Amendment and federal statutes.[73] The district court found that the TSP had "undisputedly been implemented without regard to FISA and of course the more stringent standards of Title III, and obviously in violation of the Fourth Amendment."[74] Although an appellate court granted review, it never reached the issue of the TSP's constitutionality, as it held that the plaintiffs lacked standing to bring the claim.[75]

In the wake of *ACLU v. NSA* and a FISC opinion that also raised concerns about the TSP, the executive branch, in an effort to bolster its legitimacy and constitutionality, sought Congressional approval for a similar surveillance program.[76] Congress agreed and passed the FISA Amendment Act of 2008 ("FAA").[77] The FAA eliminates the relevance of the statutory violation noted by the district court, but any search pursuant to the FAA must still comply with the Fourth Amendment.

---

72. *See* John Diamond & David Jackson, *Surveillance Program Protects Country, Bush Says*, USA TODAY (Jan. 23, 2006), http://usatoday30.usatoday.com/news/washington/2006-01-23-bush_x.htm; s*ee also* Risen & Lichtblau, *supra* note 1; Ellen Nakashima & Joby Warrick, *House Approves Wiretap Measure*, WASH. POST (Aug. 5, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/08/04/AR2007080401744.html.

73. *See* ACLU v. NSA, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006), *vacated*, 493 F.3d 644 (6th Cir. 2007).

74. *Id.* at 775.

75. ACLU v. NSA, 493 F.3d 644, 687–88 (6th Cir. 2007).

76. *Id.* (reversing the lower court ruling on procedural grounds due to lack of standing, which highlighted the risk that a future court would rule the program unconstitutional if a petitioner had standing to bring a claim); *see also* Nakashima & Warrick, *supra* note 72.

77. Pub. L. No. 110-261, 122 Stat. 2436 (2008). In 2007, Congress passed the Protect America Act as an amendment to FISA. Pub. L. No. 110-55, 121 Stat. 552 (2007). This was viewed as a "stopgap measure" that allowed Congress to debate and then enact the FAA in 2008. *See In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1007 (FISA Ct. Review 2008). The FAA, which remains current law, partially repealed the Protect America Act. § 403, Pub. L. No. 110-55, 121 Stat. 552 (2007).

On July 10, 2008, the President signed the FAA, which legislated an alternative to FISA warrants for surveillance of non-U.S. persons located outside the United States.[78] Under this legislation, the Attorney General and the Director of National Intelligence can authorize wiretaps of foreign persons outside the United States to obtain foreign intelligence.[79] The authorizations permit interception for up to one year and require limited judicial oversight.[80]

Before interception begins, the executive branch is required to obtain approval from the FISC, but this approval is for a very limited purpose.[81] Specifically, the FISC reviews the "targeting procedures" to ensure that the government will only target "persons reasonably believed to be located outside the United States," not purely domestic communications.[82] The FISC must also ensure that the government undertakes proper minimization procedures and that the Director of National Intelligence and Attorney General have certified that a "significant purpose" of the surveillance is to obtain "foreign intelligence information."[83] These procedures are all conducted in secret and ex parte.

The FISC approves general procedures but does not issue warrants based on individualized findings for any specific target.[84] Rather, the FAA permits targeting of non-U.S. persons outside the United States to gather "foreign intelligence" based on individualized deci-

78. *See* 50 U.S.C. § 1881 (2015).

79. *See id.* at § 1881a(a).

80. *Id.*; *see In re* Proceedings Required by 702(i) of FISA Amendments Act of 2008, Misc. No. 08-01, 2008 WL 9487946, at *2 (FISA Ct., Aug. 27, 2008) [hereinafter 702(i) Proceedings] (describing judicial review under Section 702).

81. § 1881a(i)(2)(B).

82. *Id.*

83. *Id.* at §§ 1881a(i)(2)(C), 1881a(g)(2)(A)(v); *see also* NAT'L SEC. AGENCY, CIVIL LIBERTIES & PRIVACY OFFICE, REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 (2014), http://www.lawfareblog.com/2014/04/readings-nsa-report-on-the-702-program/ (describing the procedures through which FISC approval is obtained). Minimization procedures are protocols to reduce the amount of information collected that is not relevant to the purpose of the search and also to detail what to do with information collected that is not relevant to the purpose of the search. 50 U.S.C. § 1801(h) (2015).

84. *See* 702(i) Proceedings, *supra* note 80 at *2.

sions made by senior members of the executive branch with no involvement of the judicial branch.[85] In short, the executive branch is not required to tell the judiciary which individuals it is targeting, on what phone or electronic device, or, importantly, whether it will intercept the communication within or outside the United States.[86]

These procedures under the FAA are conducted in secret and ex parte. After the revelations of the expansive intelligence bulk collection programs, Congress sought to insert some type of opposing counsel into the ex parte proceedings to safeguard civil liberties by arguing against the government in limited circumstances.[87] This idea of a "special advocate" at the FISC was enacted in the USA FREEDOM Act.

E. USA FREEDOM Act and the Amicus Curiae

In 2015, Congress again amended FISA, also in response to concerns about how the government and the FISC were interpreting current provisions.[88] The USA FREEDOM Act ended a once highly classified program that permitted the bulk collection and storage of all call detail information from Verizon and perhaps other cellular telephone companies.[89] Publicly disclosed by Edward Snowden, the bulk collection program collected all call data (also called "metadata") and stored it so that it may be searched in the future pursuant to a terrorism investigation.[90] Since the collection and storage was for all data, for all subscribers, and without any showing of a foreign intelligence connection to the data collected, there was significant public concern

---

85. § 1881a(g).

86. *See* NAT'L SEC. AGENCY, CIVIL LIBERTIES & PRIVACY OFFICE, *supra* note 83.

87. Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 280 (June 2, 2015) [hereinafter USA FREEDOM Act].

88. *See id.*

89. Ellen Nakashima, *NSA's Bulk Collection of Americans' Phone Records Ends Sunday*, WASH. POST (Nov. 27, 2015), https://www.washingtonpost.com/world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html.

90. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 16, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

about the program.[91] The debate continued for two years, until Congress finally amended FISA to prohibit the bulk collection of information.[92]

The USA FREEDOM Act requires all applications for business records in foreign intelligence searches to include a "specific selection term" and specifically prohibits bulk collection programs.[93] The Act created other limits and restrictions in FISA and modified the FISC procedures.[94] These changes included permitting the appointment of amicus curiae and providing a process where decisions, orders, and opinions were reviewed and declassified.[95]

Congress amended FISA to permit the appointment of an amicus curiae to appear before the court in "appropriate" matters and present "legal arguments that advance the protection of individual privacy and civil liberties," address "information related to intelligence collection," or review "a novel or significant interpretation of the law."[96] At least five individuals are appointed to participate in this process.[97] The individuals will receive security clearances and access to the necessary documents, information, and FISC precedent to perform their duties.[98]

The amicus curiae is a response to many who have long argued that there should be some type of "special advocate" to argue against the government in cases before the FISC.[99] Those same critics have

---

91. Glenn Greenwald, *As Europe Erupts over US Spying, NSA Chief Says Government Must Stop Media*, THE GUARDIAN (Oct. 25, 2013), http://www.theguardian.com/commentisfree/2013/oct/25/europe-erupts-nsa-spying-chief-government; Greenwald, *supra* note 90.

92. USA FREEDOM Act, § 103.

93. *Id.*

94. *Id.* at §§ 103, 401–02.

95. *Id.*

96. 50 U.S.C. § 1803(i)(4)(A)–(B), (i)(2)(A) (2015).

97. *Id.* at § 1803(i)(1).

98. *Id.* at § 1803(i)(3)(B).

99. *See* Stephen I. Vladeck, *The Case for a FISA 'Special Advocate',* 2 TEX. A&M L. REV. (forthcoming); FISA Court Reform Act of 2013, S. 1467, 113th Cong. (1st Sess. 2013), § 3(a); Merton Bernstein, *One-Sided FISA Court Procedure Widely Distrusted As Unfair and Unreliable* (Aug. 20, 2013), http://www.huffingtonpost.com/merton-bernstein/onesided-fisa-court-proce_b_3785797.html; Orin Kerr, *A Proposal to Reform FISA Court Decisionmaking*, THE VOLOKH CONSPIRACY (July 8, 2013), http://www.volokh.com/2013/07/08/a-proposal-to-reform-fisa-court-decisionmaking/.

argued that the amicus curiae is insufficient to prevent the government from asking for, and the FISC from approving, intelligence collection programs that are not consistent with Congress' intentions and the public trust.[100] Two exceptions created in the USA FREEDOM Act limit the scope of the amicus curiae.[101] First, the FISC can determine that the use of an amicus curiae in any particular case is not "appropriate."[102] The FISC would be required to make a "finding" that an amicus is inappropriate for a particular case and could then decide the case without external input.[103] A second exception is that the FISC can determine that a particular case does not present a "novel or significant issue."[104] The FISC, in its sole discretion, determines what is "novel or significant."[105] Therefore, the FISC has significant latitude to decide whether to employ an amicus curiae in any case.

The amicus curiae is also limited in the scope of information available to her.[106] The amicus is entitled to access information "that the court determines [is] relevant."[107] Access to classified information is also permitted for amicus with appropriate security clearance "to the extent consistent with the national security of the United States."[108] Additionally, the government is permitted to exclude "privileged" information, although it is not clear what privileges are included.[109]

---

100. *See* Steve Vladeck, *The USA FREEDOM Act and a FISA "Special Advocate,"* LAWFARE BLOG (May 20, 2014, 4:19 PM), https://www.lawfareblog.com/usa-freedom-act-and-fisa-special-advocate.

101. 50 U.S.C. §§ 1803(i)(2)–(4).

102. *Id.*; *see also* Chad Squitieri, *The Limits of the Freedom Act's Amicus Curiae*, 11 WASH. J.L. TECH & ARTS 197, 204–05 (2015). The FISC did this in the first case they considered after the amicus was created. Memorandum Opinion and Order (FISC Jun. 18, 2015).

103. *See* Letter from The Constitution Project to Speaker of the House et al. 3 (May 20, 2014), http://justsecurity.org/wp-content/uploads/ 2014/05/TCP-Letter-to-House-members-on-FISA-Special-Advocate-FINAL-SIGNED.pdf.

104. § 1803(i)(2).

105. *See id.*

106. *See id*. at § 1803(i)(6).

107. *See id.* at § 1803(i)(6)(A)(i).

108. *See id.* at § 1803(i)(6)(C).

109. *See id.* at § 1803(i)(6)(D). This could include state secret privilege in addition to traditional attorney-client privileges, which might completely restrict the amicus curiae's ability to access almost all classified information.

Therefore, both the government and the FISC can condone withholding information from the amicus curiae, reducing the effectiveness of this position.[110]

There are also limits on judicial review, which can further impact the protections afforded the public by having an advocate inside FISC hearings.[111] The amicus curiae does not have the authority to assist the FISC in considering whether certification to the Foreign Intelligence Surveillance Court of Review ("FISCR") is appropriate.[112] In appeals from the FISCR to the Supreme Court, there is no provision for the original amicus curiae to participate, as would the attorney for a party to the lawsuit.[113] Therefore, the amicus curiae in the USA FREEDOM Act has limited value to intercede in FISC proceedings and ensure that the secret court does not approve improper programs. Two declassified FISC opinions demonstrate the limited value that the USA FREEDOM Act's amicus curiae provision has for curbing improper intelligence programs.[114]

First, in a June 18, 2015, memorandum, the FISC considered but did not appoint an amicus curiae to assist with the case.[115] Written two weeks after the passage of the USA FREEDOM Act, the court reviewed a request for an emergency authorization of a pen register and "trap and trace" under one of the newly enacted changes to FISA.[116] The FISC determined that the "application in this matter 'presents a novel or significant interpretation of the law'" under the amicus curiae provision of the USA FREEDOM Act.[117] Despite determining

---

110. *See* Squitieri, *supra* note 102.

111. Jodie Liu, *So What Does the USA Freedom Act Do Anyway*?, LAWFARE BLOG (June 3, 2015, 5:29 PM), http://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway.

112. *See* Benjamin Wittes & Jodie Liu, *So What's in the New USA Freedom Act, Anyway?*, LAWFARE BLOG (May 14, 2015, 11:51 PM), http://www.lawfareblog.com/so-whats-new-usa-freedom-act-anyway; Liu, *supra* note 111. The FISCR is the appellate court that can review any appeals from the FISC.

113. The Supreme Court has the authority to determine if the appointment of an amicus is warranted, just like it does with amici in any other Supreme Court case. 50 U.S.C. § 1803(i).

114. Memorandum Opinion and Order (FISC June 18, 2015); Memorandum Opinion and Order (FISC Nov. 6, 2015).

115. Memorandum Opinion and Order (FISC Jun. 18, 2015).

116. *Id.* at 1.

117. *Id.* at 3 (citing 50 U.S.C. § 1803(i)(1).

that this case was of the exact type for which the amicus curiae was created, the FISC determined that it was "not appropriate" to appoint an amicus curiae in this matter.[118]

In explaining its decision, the FISC noted that the USA FREEDOM Act was less than two weeks old.[119] The FISC had not yet had sufficient time to review and select potential amicus curiae.[120] However, the FISC acknowledged that they had the authority to appoint an individual specifically to hear this matter, yet declined to do so.[121] The FISC determined that the emergent nature of this novel and significant issue was such that it would be inappropriate to slow the process down to permit an amicus to participate.[122] The FISC's conclusion that an amicus is not appropriate in a situation in which a speedy decision is necessary is concerning. Many novel and significant questions will also be time-sensitive as they concern matters of national security, preventing terrorism, and obtaining foreign intelligence. Therefore, the FISC will have the ability to exclude an amicus in most cases before it.

Second, in November 2015, the FISC again considered appointing amicus curiae.[123] The FISC determined that this case, which involved searches under FISA section 702, involved "one or more novel or significant interpretations of the law."[124] While the court found that the use of the amicus in that case was beneficial, the case illustrates the significant limitations on the use of an amicus in the FISC. These procedural limitations include the government's ability to effectively prevent an amicus from being appointed in many cases and the FISC's ability to limit the specific issues that the amicus curiae can consider in an individual case.[125]

The government can effectively foreclose the use of amicus curiae in any particular matter. In the November 2015 FISC decision, the court noted that the matter involved "novel or significant" legal

---

118. *Id.* at 3.

119. *Id*. at 3.

120. *Id*. at 3; *see also* 50 U.S.C. § 1803(i)(1).

121. Memorandum Opinion and Order 3 (FISC Jun. 18, 2015) (citing 50 U.S.C. § 1803(i)(2)(B).

122. *Id.* at 3.

123. Memorandum Opinion and Order (FISC Nov. 6, 2015).

124. *Id.* at 5.

125. *Id.* at 5–6.

issues, and that the use of an amicus would assist the court.[126] However, the court also noted that there was insufficient time to appoint an amicus because the statute permits the court only a thirty-day review period.[127] The court asked the government for input on whether an extension was "necessary for good cause in a manner consistent with national security."[128] Fortunately, the government concluded that a delay would not be inconsistent with national security, but this procedural requirement limits the circumstances when the amicus curiae can participate in matters.[129] The government would not want delay in foreign intelligence and national security cases for several reasons, many legitimate but some improper. Perhaps, the most significant and novel issues will also be the ones with the highest government need to act quickly to protect the security of the United States. In these important cases, the speed to issue a decision would "as a practical matter, foreclose amicus participation."[130]

Even in cases in which the FISC chooses to employ an amicus, the court can limit the issues in which an amicus can participate. In the November 2015 decision, the court directed the amicus to address two important but narrow issues relating to whether specific minimization procedures the government sought to use for their section 702 searches were consistent with the Fourth Amendment.[131] While the court found the assistance of the amicus informative, the court's authority to exclude the amicus from considering all but a few narrow issues is a further limitation of the effectiveness of the USA FREEDOM Act's amicus provision.[132]

The amicus curiae can be an effective advocate to ensure the government and FISC authorize programs consistent with current law and balancing civil liberties. However, the effectiveness of the amicus is limited in numerous ways. The FISC chooses the individuals to become amicus curiae.[133] The government can exclude amicus in cases

126. *Id.* at 5.

127. *Id.*; *see also* 18 U.S.C. § 1881a(i)(1)(B) (proscribing a thirty-day review period).

128. Memorandum Opinion and Order (FISC Nov. 6, 2015).

129. *Id.* at 5–6.

130. *Id.* at 5.

131. *Id.* at 6.

132. *Id.* at 6 n.6

133. 50 U.S.C. § 1803(i)(1) (amended 2015).

where "national security" requires a speedy decision.[134] The FISC can limit the use of an amicus only to the cases where the FISC deems there to be "novel or significant" legal issues and only when the FISC determines the use of an amicus is "appropriate."[135] Further, the FISC can cabin the amicus's responsibilities to narrowly defined issues within a particular case. Using these limiting procedures, the government and the FISC can prevent an amicus in serving on almost any case they choose.

The procedures that restrict the use of the amicus place much of the authority into the hands of the same executive and judicial authorities that approved the prior bulk collection programs. The purpose of the amicus was in part to prevent the FISC and government counsel from exceeding the authority granted to them by Congress. However, both the government and the FISC have multiple procedures by which they can preclude amicus involvement, increasing the risk that both will again adopt intelligence programs that are inconsistent with the desires of Congress. While these efforts are a step forward, more is needed.

These concerns and limitations on the ability to use amicus curiae before the FISC demonstrate that additional protections are needed to ensure the intelligence programs authorized by the FISC remain consistent with the intent of Congress. These limitations do not mean that the amicus curiae provisions before the FISC do not have some value. In fact, there are two significant benefits to this addition to FISA. First, the amicus provision, for the first time, permits non-government officials to be included in the discussion of the most sensitive intelligence collection programs. Second, the use of an amicus at the initiation of intelligence collection programs will help judges review government requests with a balanced eye; this adversarial process will promote judicial independence. Aside from the inherent value of these two benefits, the amendments open the possibility of further improvements to FISA to ensure the government uses appropriate national security programs, protects civil liberties, and promotes judicial independence through a robust adversarial process.

---

134. *See id.* at § 1881a(j)(2).

135. *Id.* at § 1803(i)(2)(A).

The inclusion of a special advocate that can intervene in the ex parte proceedings of the FISC and review sensitive government collection programs is groundbreaking. Whether the current amicus curiae provision will actually change government policy is yet to be determined, but the mere fact that there is a provision to include an outsider in the review and approval of government intelligence programs is significant. The fact that an amicus may be included at the inception of collection may open the door to including other advocates at later stages of government programs.

Early intervention into government surveillance programs also has tremendous value for civil liberties. An effective amicus can potentially prevent constitutional violations before they happen by providing the court an opposing view that promotes civil liberties over government's request for national security protections. This early intervention, if effective, is a powerful catalyst to ensure independent judicial decisions.

However, there is a downside to this early intervention. Review of intelligence collection programs prior to their employment lacks the clarity present in post-search or collection reviews. Because there is concrete value in looking at the government conduct after it has occurred to determine whether it was constitutional, courts tend to be reluctant to review prospective action in many ordinary cases. Put another way, some intelligence programs may appear to be appropriate at the outset, but after the government collects intelligence, it becomes clear that the searches were not constitutional. An advocate has the value of hindsight when performing a full and careful review of what actions the government has already performed.

In addition to the early intervention provided by the FISC amicus curiae, it is also necessary to employ a special advocate after the searches are concluded in order to ensure that the courts and government are acting consistently with national values. Considering that an amicus can now participate in the beginning of the review of these programs, it is also appropriate to permit them to review searches after they conclude, especially when the government wishes to use the fruits of those searches in criminal cases against defendants. Unfortunately, current court procedures do not allow special advocates to review at trial the information that the USA FREEDOM Act's amicus can review before collection.

III. Challenging Evidence Derived from Foreign Intelligence

The addition of an amicus into the FISC proceedings is a dramatic shift away from the secrecy sought in the past and a significant step toward ensuring the adversarial process that is essential to judicial independence. The use of an amicus before intelligence programs are approved is a monumental change from other procedures involving the review and challenge of evidence derived from FISA. This same process can be used in criminal prosecutions, with the same benefit to judicial independence. The use of an advocate during criminal prosecutions will ensure that intelligence collections programs are appropriate. Moreover, they will ensure the same concrete protections afforded criminal defendants in all other criminal cases.

Foreign intelligence gathering has developed from something not regulated by the courts to something regulated heavily and in secret by a specialized court. At the same time, foreign intelligence has changed from information that was always intended to remain classified to potentially inculpatory evidence that will be made available for use in criminal prosecutions. This transformation to using information gathered from classified intelligence tools to evidence used in criminal prosecutions creates friction with the secretive nature of intelligence. This is most acute when evidence gathered from FISA is being challenged in a criminal case. Before we explain how challenging FISA evidence works, we must briefly examine how non-classified evidence is challenged.

A. Challenging Traditional Warrants: Attacking What the Defendant Can See

The procedure to challenge the admission of evidence in ordinary criminal cases is well known. A defendant has the right in every criminal case to file a motion to suppress the evidence being introduced to convict him.[136] The Defendant is notified when the government presents the evidence pursuant to its discovery obligations.[137] The defendant and his attorney can review the evidence the prosecutor intends to introduce at trial, read the search warrants and affidavits that support

136. Fed. R. Crim. P. 41(h).

137. *See* Fed. R. Crim. P. 16(a).

them, and determine if the warrants comply with the Fourth Amendment.

The Defendant can then file a motion to suppress tailored to any alleged constitutional violations.[138] The defendant can challenge the facial validity of the search warrant,[139] that the affidavit lacks probable cause,[140] that the affiant made a false statement or material omission in the affidavit,[141] that the search warrant was too broad or did not accurately identify the location to be searched,[142] and other things.[143] The court then holds a hearing, if necessary, where both parties can introduce evidence to support their version of the facts and argue the motion.[144] The judge, after hearing both arguments tailored to the facts of the documents, issues a fair and independent decision on whether the evidence is admissible. Judges can effectively terminate an intelligence collection program by determining it is unconstitutional.

This simplification of how defendants challenge evidence prior to trial is familiar to even first-year law students. A central tenet of this process is that the defendant is informed of the evidence to be used against him. Equally important, the defendant has access to the affidavits, warrants, and applications that the court approved to permit the search and seizure of evidence. This allows the defendant direct and meaningful opportunity to challenge the evidence being used against her. Further, it allows judges the opportunity to consider adversarial arguments that challenge the validity of the government's actions. The process in challenging FISA orders, however, is entirely different.

---

138. *See* FED. R. CRIM. P. 12, 41(h) ("A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.").

139. *See, e.g.,* Rawls v. Commonwealth, 434 S.W.3d 52 (Ky. 2014).

140. *See, e.g.,* Aguilar v. Texas, 378 U.S. 108, 115–16 (1964).

141. *See e.g.,* Franks v. Delaware, 438 U.S. 154, 155–56 (1978).

142. *See, e.g.,* Marron v. United States, 275 U.S. 192, 196 (1927).

143. *See* Morris D. Forkosh, *The Constitutional Right to Challenge the Content of Affidavits in Warrants Issued Under the Fourth Amendment*, 34 OHIO ST. L.J. 297 (1973); Steven M. Kipperman, *Inaccurate Search Warrant Affidavits as a Ground for Suppressing Evidence*, 84 HARV. L. REV. 825 (1971).

144. *See* FED. R. CRIM. P. 12(c).

B. Challenging FISA Warrants: Attacking Hidden Affidavits

Evidence derived from FISA is of a different character than evidence typically introduced in a criminal trial. The process to obtain FISA information[145] and the court orders that permit FISA searches are classified.[146] Initially, even the information collected is classified.[147] FISA information must first be declassified in order to be used as evidence in a criminal case.[148] Federal judges must rule on the evidence's admissibility and defendants must have an opportunity to challenge its constitutionality.[149]

The FISA affidavits and orders, however, are neither declassified nor disclosed to the defendant.[150] Instead of receiving the affidavits and warrants themselves, a defendant confronting FISA-derived evidence receives notice that the government intends to use information obtained from or derived from FISA activity.[151] In traditional FISA cases, federal prosecutors would send a notice to the defendant that the government intended to introduce evidence that had been obtained through the use of FISA.[152] But even then, the government

---

145. *See* United States v. Ott, 827 F.2d 473, 476 (9th Cir. 1987); United States v. Warsame, 547 F.Supp. 2d 982, 989 n.5 (D. Minn. 2008).

146. *See* 50 U.S.C. § 1806(f) (2015) (electronic surveillance); *id.* at § 1825(g) (physical search); *id.* at § 1845(f)(1) (pen/trap surveillance). *See* U.S. v. Amawi, 531 F. Supp. 2d 832, 837 (N.D. Ohio 2008). For a detailed discussion on this issue, see DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 30:7, (West 2016).

147. *See* KRIS & WILSON, *supra* note 146 (outlining the need for secrecy in FISA cases).

148. *See* 50 U.S.C. § 1806(f); *id.* at § 1825(g); *see* United States v. Daoud, 755 F.3d 479, 481–82 (7th Cir. 2014); Eric Lichblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (Jul. 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

149. *See* FED. R. CRIM. P. 41(h).

150. *Daoud*, 755 F.3d at 481 (noting "no court has ever allowed disclosure of FISA materials to the defense").

151. *See* 50 U.S.C. § 1806(c) (for electronic surveillance); *id.* at § 1825(b) (for physical searches); *id.* at §§ 1845(c)–(d) (for pen registers and trap and trace orders); *see also* KRIS & WILSON, *supra* note 146.

152. *See* Savage, *supra* note 10. After receiving notice, a defendant in a federal terrorism trial may file a motion to suppress.

rarely notifies the defendant exactly what provision of FISA was used to obtain the information.[153]

Defendants who are faced with evidence that was gathered pursuant to FISA approvals, either through a traditional FISA warrant or another FISA order has an equal right to challenge the evidence on any and all grounds.[154] However, neither the defendant nor his attorney is permitted to read the application or affidavit for the FISA order.[155] Therefore, the defendant must file a motion blind and argue all conceivable theoretical reasons why the warrant is invalid.[156] It is up to the court to review the classified documents in camera and consider whether any of the list of possible challenges are valid attacks upon the FISA orders.[157]

The defendant, who is attempting to challenge the validity of orders and affidavits that he cannot review, is at a significant disadvantage as compared to the defendant challenging traditional warrants. Defendants cannot review the FISA orders to determine whether they are overbroad, whether there are significant typographical errors, or whether they permit searches beyond that for which there is a justification in the affidavits. Defendants cannot review the FISA affidavits to determine if there are false statements, material omissions, a lack of probable cause, or other information that may be useful to a defendant in challenging the admissibility of the evidence. This is a significant disadvantage to defendants against whom FISA-derived evidence is being introduced.

Judge Rovner, in her concurrence in a Seventh Circuit case that denied the defendant access to the FISA applications, affidavits, and orders, explained the dilemma that confronts such defendants. The *Daoud* case dealt specifically with a motion to suppress based on a claim that the officers made false material misrepresentations in the affidavit, citing *Franks v. Delaware.* As Judge Rovner notes, a defendant has great difficulty raising a claim that the agents lied on an affidavit when they cannot read the affidavit.

---

153. *Id.*

154. *See Daoud*, 755 F.3d at 485–96 (Judge Rovner, concurring) (recognizing that the defendant has the same right to challenge the admissibility of FISA derived evidence and noting the difficulties of doing so with classified materials).

155. Savage, *supra* note 10.

156. *Daoud*, 755 F.3d at 486 (Rovner, concurrence).

157. *Id.*

> *Franks* cannot operate in the FISA context as it does in the ordinary criminal case. To pretend otherwise does a disservice to the defendant and to the integrity of the judiciary. . . . [T]he defendant cannot make a viable *Franks* motion without access to the FISA application, and that the court, which does have access to the application, cannot, for the most part, independently evaluate the accuracy of that application on its own without the defendant's knowledge of the underlying facts. Yet, *Franks* serves as an indispensable check on potential abuses of the warrant process, and means must be found to keep *Franks* from becoming a dead letter in the FISA context.[158]

Judge Rovner calls upon Congress and the executive branch to provide a solution to correct this unfairness.[159]

There are justifiable reasons for these altered procedures—to protect the national security of the United States—but these reasons are less valid now that the USA FREEDOM Act includes an amicus curiae before the FISC. As will be demonstrated in the next section, a special advocate or amicus curiae at the trial level is the next essential step to protect individual defendants, provide security against an improper expansion of government surveillance programs, and ensure independent judicial decisions.

IV. FOREIGN INTELLIGENCE IN CRIMINAL CASES

The next step to ensuring the intelligence community pursues only appropriate collection programs is to create a panel of cleared defense counsel who can act as special advocates to litigate pretrial FISA motions. Having a handful of amicus curiae cleared to appear before the FISC in some limited proceedings has value, but the greater need is to have meaningful representation at the trial level for defendants that will have foreign intelligence evidence presented against them. Robust procedures have been developed over time to allow defendants a meaningful ability to challenge the evidence against them in criminal

158. *Id.*
159. *Id.*

cases. But, the procedures are significantly modified to the defendant's detriment in cases involving foreign intelligence.[160] These modifications contribute to a structure that will permit the intelligence community and the FISC to again pursue programs outside of their mandate. The resulting diminishment to a true adversarial process will hamper judicial independence.

Special advocates at the trial level can restore each defendant's right to challenge the introduction of evidence against her and to ensure that intelligence collection programs are legal and appropriate. This section will outline how these special advocates should be created and what authority they should have.

A. Creation of the Federal Public Defender's Office of the FISA Special Advocate

The first step in providing defendants a meaningful ability to challenge the evidence being used against them is to create a staff of defense counsel that (1) have the appropriate clearance to review FISA applications and affidavits and (2) can legally represent defendants in criminal cases all over the country. This can be accomplished by creating a national office of the FISA Special Advocate that litigates FISA-related pretrial motions for defendants. This national level organization would function as the counterpart to the Litigation Section of the Office of Intelligence in the National Security Division of the Department of Justice.[161] The Litigation Section assists federal prosecutors across the country in responding to pretrial motions of defendants in FISA cases. These experts add value to each case and bring a wealth of experience to help ensure that the court benefits from an experienced advocate who is highly educated in this specialized area of the law. The Office of FISA Special Advocate can do the same.

The idea of a special advocate trained and qualified to handle particular litigation matters is not without precedent. Federal Public

160. *See generally,* Classified Information Procedure Act ("CIPA"), 18 U.S.C. app. § 3 (1980).

161. *See Office of Intelligence*, U.S. DEP'T OF JUSTICE (Jul. 23, 2014), https://www.justice.gov/nsd/office-intelligence.

Defenders already have specialized counsel for death penalty cases.[162] There are also "cleared" defense counsel who have authorization to review classified information in criminal cases.[163] Adding another category of cleared counsel would not be extraordinary. Considering the vast budget currently allocated to the government for FISA-related litigation, adding a panel of qualified defense counsel is not financially burdensome. Further, having a defense counterpart to the government's specialized FISA litigators, with access to the same documents, is exactly the level playing field the American adversarial system is designed for, upon which judges can make truly independent decisions.

B. The Special Advocate in Operation

Those challenging the creation of an Office of FISA Special Advocates may come from both government intelligence agencies and from the civil liberties groups challenging these collection programs. The national security community may object to further expansion of those who can have access to our nation's intelligence secrets. Civil liberty groups may argue that this proposal does not go far enough. However, this program will not endanger national security and it will provide further protection for both individual defendants and the national civil liberties.

Some may argue that creating special advocates for trial will unnecessarily expand those that can access our nation's secrets. Adding a small number of cleared defense counsel to litigate pretrial motions does not unduly expand access to sensitive programs. These advocates can go through an extensive background and security clearance procedure. Further, they would only be employed in situations where the government has already decided that some disclosure is appropriate because the government is in the process of taking FISA derived information and introducing it at trial. The extra cost to secrecy is minimal.

---

162. *See* 18 U.S.C. § 3005 (2013) (every defendant in a death penalty case is entitled to two counsel, one which must be "learned in the law applicable to capital cases").

163. *See e.g.*, Ellen Yaroshefsky, *Secret Evidence Is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1067–68 (2006).

There are already five individuals who the government believes can be entrusted with this responsibility. In fact, the amicus curiae appointed pursuant to the USA FREEDOM Act have potentially greater access to classified sources and methods of intelligence collection than a pretrial special advocate would have. Currently, the amicus curiae are provided access to "novel and significant" issues.[164] They can be called to review programs that are so sensitive that the intelligence community would not permit declassification or use in a criminal trial. But a specific amicus curiae cannot review the same FISA application when the FISA-derived information is being used to prosecute a defendant in a criminal case. Since the amicus can access the most sensitive intelligence collection programs, they should also have access to the information surrounding the use of FISA-derived information at trial. Because the government can find five individuals who may be cleared to review sensitive FISA information, it is reasonable to believe that the government can find additional attorneys to litigate these issues before district courts.

Civil liberties advocates may argue that a special advocate to assist criminal defendants pretrial is an insufficient step to protect Americans from the massive bulk collection programs that were revealed by Edward Snowden. Realistically, adding a special advocate is the next step to providing additional outside and adversarial oversight to government intelligence programs. The liberty interest is highest when the government is using intelligence searches to gather evidence used to prosecute individuals. At this critical point, adequate procedural safeguards are needed to ensure the defendant's constitutional rights are protected and to allow judges to make informed decisions about the government's intelligence programs.

Another concern will be the special advocate's interaction and relationship with the defendant and his primary counsel. The special advocate will have limits on what she can tell the defendant and his counsel, creating some tension and concerns. This is a legitimate problem, but this same problem is present in all cases in which a defense counsel has a security clearance and is provided access to information that her co-counsel or defendant is not permitted to know.[165] While

164. 50 U.S.C. § 1803(i)(2)(A) (2015).

165. *See, e.g.*, Government's Assent to Motion for a Protective Order, United States v. Tsarnaev, No. 13-10200-GAO (D. Mass. Aug. 16, 2013) (setting limits on

this is a matter for concern, the defendant is better situated with counsel that can view everything, but not share it with the defendant, than counsel who cannot see all of the evidence but can share all she has access to. The attorney-client privilege would still attach, so the special advocate can learn everything about the defense's case in order to better prepare for the pretrial motions. Therefore, not only would this proposal benefit the defendant, but counsel would also be able to navigate the ethical and legal challenges in a manner that is not uncommon in other criminal cases.

A special advocate in criminal trials will have some limits on her effectiveness because she will only be used to challenge intelligence programs that collect information to be used in criminal prosecutions. But these special advocates are in a better position to protect civil liberties than the amicus curiae in the USA FREEDOM Act. Special advocates are arguing based on past concrete actions, searches, and seizures that are well defined. These advocates can apply traditional notions of constitutional rights before a diversity of federal judges who can review the government programs to determine whether they comply with current law and constitutional protections. The fact that the intelligence searches have already happened gives these advocates an advantage over the amicus, who must attempt to predict the effects of searches that have not yet been conducted.

These special advocates are needed to ensure fair trials and that government intelligence programs are constitutional. The government has taken significant steps to incorporate law enforcement into its national security apparatus to be used as a tool to prevent, disrupt, and punish terrorism.[166] Law enforcement is often the best available tool to stop an imminent terrorist attack inside the United States.[167] Thus, there will likely be occasions in the future where the government must permit the disclosure and use of information derived from intelligence

what information defense counsel can disseminate); *see also* Classified Information Protection Act ("CIPA"), 18 U.S.C. app. III § 3 (2016).

166. *See generally* KRIS & WILSON, *supra* note 146, at ch. 24 (discussing "Law Enforcement as a . . . Counterterrorism Tool").

167. *See generally* David S. Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SEC. L. & POL'Y 1, 2 (2011).

collection programs in a criminal trial.[168] If the special advocate program is created, these attorneys can review and challenge the lawfulness of any of any collection programs.

The creation and use of the special advocate program would increase the likelihood that a variety of cleared attorneys who can be trusted with national secrets can raise challenges to the use of intelligence collections programs before a wide variety of federal judges. This program is the next step in ensuring that the government does not seek, and the courts do not condone, intelligence collection programs that are improper.

V. CONCLUSION

The truth behind the bulk collection and other secret intelligence collection programs revealed by Edward Snowden is that they were sought and approved through the very procedures set up to protect individual civil liberties and ensure judicial restraint on government surveillance. Although these leaks created a necessary public debate about what level of security is appropriate when balanced with liberty and privacy, very little has been done to change the process by which the government seeks, and the courts approve, additional intelligence collection programs.

The USA FREEDOM Act brought some needed changes to correct the expansive programs that were inconsistent with American values and Congress's intent. Unfortunately, the changes brought by the USA FREEDOM Act are insufficient to prevent another broad misuse of the intelligence authorities.

While the amicus curiae is a step towards greater oversight and civil liberties protections in intelligence collection programs, there is an even greater need to preserve individual liberties and to provide adversarial input into the intelligence gathering programs. Criminal defendants must have the right to review both the evidence collected on them and the process used to gain approval for these searches. A panel of special advocates must be created to assist defendants in pretrial criminal litigation.

These special advocates can ensure that criminal defendants can meaningfully challenge FISA collection and also ensure that the FISC

168. *Id.*

and the intelligence community do not again exceed their Congressional mandate. Congress must establish a panel of cleared defense counsel—special advocates—who can review FISA applications and file motions to suppress evidence on behalf of criminal defendants in any district court in the United States where FISA evidence will be used in a criminal case. Every defendant has the constitutional right to challenge the evidence being used against him. Defendants being confronted with FISA-derived evidence need the same right to challenge the manner in which the evidence was obtained. Doing so will ensure that the defendants receive the fair trial that the Constitution guarantees them. By protecting individual defendants in criminal cases, special advocates can also challenge overreaching intelligence programs and ensure that all Americans have another tool to protect them from improperly intrusive intelligence collection programs. Judges, with the benefit of an adversarial process, can provide the essential check on the executive branch and fulfill their constitutional role to ensure the other branches of government are acting within their constitutional authority.