University of Arkansas at Little Rock Law Review

Volume 38 | Issue 1 Article 2

2015

The Foreign Intelligence Surveillance Act and The Separation of Powers

Scott A. Boykin

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND THE SEPARATION OF POWERS

Scott A. Boykin[*]

I. INTRODUCTION

In the 1950s and 1960s, J. Edgar Hoover's Federal Bureau of Investigation ("FBI") engaged in illegal and abusive surveillance and intimidation of political dissidents and civil rights activists,[1] and in the wake of that government misconduct, Congress adopted the Foreign Intelligence Surveillance Act ("FISA") to assert congressional and judicial oversight of executive branch agencies' intelligence-gathering activities.[2] There was a dramatic increase in requests for surveillance under FISA after the September 11, 2001 terror attacks,[3] and Congress amended FISA to enhance the government's authority to conduct such surveillance in response to those attacks.[4] When Congress discovered in the mid-2000s that the FBI and National Security Agency ("NSA") had overstepped their authority to conduct electronic intelligence with the Bush administration's blessing, Congress amended FISA again to permit the government to continue what had been illegal conduct.[5] Beginning in 2013, former NSA contractor Edward Snowden dis-

---

* Assistant Professor of Political Science, Georgia Gwinnett College, Lawrenceville, Georgia; Ph.D., Tulane University; J.D., University of Alabama School of Law; B.A., University of Alabama at Birmingham.

1. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at 2–18 (1976), http://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

2. PERMANENT SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. REP. NO. 95-1283, pt. 1, at 21 (1978), http://www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/HPSCI_FISA_Report_95-1283_Pt.1.pdf.

3. *See Foreign Intelligence Surveillance Act Court Orders 1979–2014*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited March 11, 2016) [hereinafter *FISA Ct. Orders* 1979–*2014*] (summarizing United States Department of Justice annual FISA reports to Congress).

4. SENATE COMM. ON INTELLIGENCE, TO PERMANENTLY AUTHORIZE CERTAIN PROVISIONS OF THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT) ACT OF 2001, TO REAUTHORIZE A PROVISION OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004, TO CLARIFY CERTAIN DEFINITIONS IN THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, TO PROVIDE ADDITIONAL INVESTIGATIVE TOOLS NECESSARY TO PROTECT THE NATIONAL SECURITY, S. REP. NO. 109-85, at 1–2 (2005), http://www.intelligence.senate.gov/sites/default/files/publications/10985.pdf.

5. *See* discussion *infra* Part II.D.

closed documents to the public that showed the surprising magnitude of governmental surveillance and collection of information regarding cell phone and internet communications of Americans, which prompted calls for reform.[6] The reform, the USA FREEDOM Act, became effective in November, 2015, and while it is an improvement in the law, it does not represent a great change in the access to information the government has had for more than a decade.[7]

What is more, the recent amendments make relatively minor changes to the FISA Court and the FISA Court of Review, established by the original FISA statute in 1978 to consider applications for electronic surveillance under the statute.[8] These courts are unlike any others in the history of the United States.[9] The judges of these courts are selected by the Chief Justice of the Supreme Court of the United States.[10] Although they are United States District judges or United States Court of Appeals judges, there is no congressional involvement in their appointment to these courts.[11] Their orders are mostly secret, and their proceedings are largely secret.[12] With rare exceptions, the only parties to appear before these courts are the federal agencies seeking orders to permit them to gather information about subjects for investigation.[13] Their proceedings are generally not adversarial in nature.[14] The federal government appears before them to obtain approval for searches without objection.[15] These courts are developing a body of secret law.[16] They have developed precedent that no lawyer can research, understand, and criticize because it is secret law.[17] While there is a FISA Court of Review, no higher court has ever examined a decision of the FISA Court on appeal. The FISA Court has approved thousands of requests for surveillance and modified only a small handful of such requests.[18] While the USA FREEDOM Act adopts some meaningful changes to these courts' procedures, the statute does not make these courts the check on executive power

6. H. JUDICIARY COMM., UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015, H.R. REP. NO. 114-100, at 2–3 (2015), https://www.congress.gov/congressional-report/114th-congress/house-report/109/1.

7. *See* discussion *infra* Part II.A.

8. *See* discussion *infra* Part II.

9. *See* discussion *infra* Part III.

10. *See* discussion *infra* Part III.

11. *See* discussion *infra* Part III.

12. *See* discussion *infra* Part III.

13. *See* discussion *infra* Part III.

14. *See* discussion *infra* Part III.

15. *See* discussion *infra* Part III.

16. *See* discussion *infra* Part III.

17. *See* discussion *infra* Part III.

18. *See FISA Ct. Orders 1979–2014*, *supra* note 3.

that FISA's authors envisioned.[19] Rather, the FISA Court's structure and limited review of applications for surveillance impose a very weak limitation on executive branch power.[20] Ironically, FISA has contributed to the concentration of power in the executive branch and to the deterioration of the separation of powers, which is a core principle of American government.[21]

In the second part of this article, I detail the provisions and historical development of FISA, which is a narrative of largely unsuccessful efforts to monitor and limit executive branch agencies' intelligence-gathering activities. In the third part, I discuss the FISA courts, including their authority, structure, and procedures. These courts, I argue, have very limited control over the executive branch's surveillance and intelligence-gathering programs and thus offer a limited check on executive branch power. In the final section, I discuss the separation of powers principle in the American political system and how FISA has contributed to a decades-long trend of increasing concentration of power in the executive branch.

II. HISTORICAL DEVELOPMENT OF FISA

Congress adopted FISA to impose judicial control over the executive branch's surveillance activities.[22] The statute was not often used until after the September 11, 2001 terror attacks,[23] which underscored the need for more effective surveillance and intelligence-gathering techniques to prevent additional attacks. Congress responded by amending FISA to broaden the freedom of executive branch agencies to conduct surveillance and gather electronic intelligence with relatively little judicial supervision.[24] In fact, as I show in the following sections, when Congress learned that the executive branch had violated FISA, Congress amended FISA to allow the executive branch to engage in previously-illegal activities.[25] When the American public became aware of the extent of the federal government's surveillance ac-

19. *See* discussion *infra* Part IV.

20. *See* discussion *infra* Part IV.

21. *See* discussion *infra* Part IV.

22. PERMANENT SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. REP. NO. 95-1283, pt. 1, at 21–22 (1978), http://www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/HPSCI_FISA_Report_95-1283_Pt.1.pdf.

23. *FISA Ct. Orders 1979–2014*, *supra* note 3.

24. ELIZABETH B. BAZAN, CONG. RESEARCH SERV., RL30465, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW DECISIONS 1–2 (2007), *available at* http://www.fas.org/sgp/crs/intel/RL30465.pdf.

25. *See* discussion *infra* Part II.D.

tivities in 2013, public demands for reform produced further amendments that do little to roll back the broad and largely unchecked intelligence-gathering and surveillance powers Congress authorized before.[26]

A. The Foreign Intelligence Surveillance Act

In December 1974, New York Times reporter Seymour Hersh disclosed to the public that the Central Intelligence Agency ("CIA") had been engaged in intelligence operations against American citizens and had taken part in acts designed to destabilize foreign governments.[27] The public alarm over these activities prompted the United States Senate to establish a special committee, chaired by Senator Frank Church, to investigate the government's activities.[28] Over a nine-month period, the committee interviewed hundreds of witnesses and conducted numerous hearings, ultimately producing analysis demonstrating that the FBI had engaged in illegal covert operations in the United States and that the CIA had engaged in illegal covert operations at home and abroad.[29] For example, the Committee's reports demonstrated that the FBI and CIA had harassed civil rights and political dissident groups, opened and read individuals' mail, and conducted warrantless break-ins to plant surveillance devices and steal information regarding the groups' members.[30] The "Church Committee," as it became known, is the forerunner to the present-day Senate Select Committee on Intelligence, charged with congressional oversight of executive branch intelligence activities, including intelligence agency reports, budgets, programs, and actions.[31]

As a result of the Church Committee's findings, Congress adopted the Foreign Intelligence Surveillance Act in 1978.[32] Under the statute as originally adopted, the President could authorize electronic surveillance of foreign powers to gather intelligence upon the Attorney General's certification that there was no "substantial likelihood" that the government would obtain the communications of a "United States person" (a citizen or other lawful resident of the United States) and that the minimization procedures for the

26. *See* discussion *infra* Part II.D.

27. *Church Committee Created*, U.S. SENATE, http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm (last visited Nov. 15, 2015).

28. *See id.*

29. *See id.*

30. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 10–13 (1976), https://archive.org/stream/finalreportofsel03unit/finalreportofsel03unit_djvu.txt.

31. *See id.*

32. Christopher P. Banks, *Protecting (or Destroying) Freedom Through Law: The USA PATRIOT Act's Constitutional Implications*, *in* AMERICAN NATIONAL SECURITY AND CIVIL LIBERTIES IN AN ERA OF TERRORISM 34 (David B. Cohen & John W. Wells eds., 2004).

surveillance protected the private information of United States persons.[33] The FISA Court, created by the statute, could issue orders for electronic surveillance of foreign powers or their agents upon application by federal officers authorized by the Attorney General on behalf of the President.[34] A United States person could not be regarded as a foreign power for purposes of obtaining an order from the FISA Court for activities protected by the First Amendment.[35] Nevertheless, a United States person could be an agent of a foreign power when the person engages in clandestine intelligence activities on a foreign power's behalf, when such activities may involve a violation of the criminal laws of the United States, when a person engages or prepares to engage in sabotage or international terrorism on behalf of a foreign power, when a person enters the United States under a false identity on behalf of a foreign power, or when a person aids or abets or conspires to do any of the foregoing.[36]

Under FISA, the location of the surveillance must be a place that is to be used by a foreign power or its agent.[37] The minimization procedures had to meet the same requirement as for electronic surveillance without a court order.[38] Further, the order had to specify the target and location for the surveillance, the method of conducting the surveillance, the duration of the surveillance, and the number of devices employed to conduct the surveillance and order that the minimization procedures be followed.[39] The USA PATRIOT Act made profound changes to FISA and gave broad new powers to the executive branch to conduct surveillance activities with relatively little oversight from the judiciary.

B. The USA PATRIOT Act

After the September 11, 2001 terror attacks on the United States, Congress adopted the USA PATRIOT Act, and Title II of the new law amended

---

33. Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 787, §§ 102(a)(1), 101(h) (codified as amended at 50 U.S.C. §§ 1801(f)(1)–(4), 1802(a)(1)(A)(i)) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

34. *See* 50 U.S.C. § 1802 (West, current through P.L. 114-115 (excluding 114-94 and 114-95) approved 12-28-2015).

35. *See* Foreign Intelligence Surveillance Act of 1978 § 105(a)(3)(A) (Westlaw).

36. 50 U.S.C. § 1801(b)(2) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

37. *See* Foreign Intelligence Surveillance Act of 1978 § 105(a)(3)(B) (Westlaw).

38. *See id.* § 105(a)(4).

39. *See id.* § 105(b). If the target was a foreign power, FISA did not require the order to specify the type of information or the method and number of devices to be used for the surveillance. *See id.* § 105(c).

the FISA statute.[40] An application for an order allowing electronic surveillance under FISA requires a statement of a federal officer under oath attesting to the identity or description of a proposed target for surveillance, a statement of the "facts and circumstances" showing that the target is "being used or is about to be used" by "a foreign power or an agent of a foreign power," a description of the communications sought and the types of communications being sought, and "that a significant purpose of the surveillance is to obtain foreign intelligence information" that cannot be obtained by ordinary intelligence-gathering techniques.[41] "Foreign intelligence information" is information limited to that needed to protect the United States against hostile acts, terrorism, or intelligence operations directed against the United States by a foreign power or its agent.[42] A judge must find that there is probable cause showing that the target of the surveillance is a foreign power or its agent and that the facilities targeted are being used or are about to be used by a foreign power or its agent.[43] In determining whether the required probable cause exists, a judge may consider "past activities of the target, as well as facts and circumstances relating to current or future activities of the target."[44]

Under the USA PATRIOT Act, "[m]inimization procedures" are those adopted by the Attorney General intended to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons" in the acquisition and use of foreign intelligence information, "unless such person's identity is necessary to understand foreign intelligence information or assess its importance."[45] Nonetheless, such information may be retained and used for general law enforcement purposes or if the Attorney General concludes that the "information indicates a threat of death or serious bodily harm to any person."[46]

Section 215 of the USA PATRIOT Act amended FISA to allow for the acquisition of business records of United States businesses in a way that permitted wholesale collection of databases containing records of electronic

---

40. "USA PATRIOT" is an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." *See* USA PATRIOT Act, Pub. L. No. 56-107, § 1(a), 115 Stat. 272, 272 (2011).

41. 50 U.S.C. § 1804(a) (2010). Before the USA PATRIOT Act amendments to FISA were adopted in 2001, the "primary purpose" of surveillance had to be to gather foreign intelligence. *See* USA PATRIOT Act, sec. 218. *But cf.* Foreign Intelligence Surveillance Act 50 U.S.C. § 1804 (a)(b)(7).

42. 50 U.S.C. § 1801(e) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

43. *Id.* § 1805(a)(2)(A).

44. *Id.* § 1805(b).

45. *Id.* § 1801(h)(1)–(2).

46. *Id.* § 1801(h)(3)–(4).

communications that occurred wholly within the United States.[47] FISA now authorizes the FBI to apply for an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[48] The application for records has to show "that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . ."[49] There is a presumption that the things, or items, sought are relevant if related to a foreign power or its agent, or persons in contact with or known to such agents.[50] In addition, the application must set forth the minimization procedures regarding the dissemination and retention of information regarding United States persons.[51] The only substantive limitation on the records sought is that the investigation to which they are relevant is not being conducted on "a United States person solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States."[52] Under the USA PATRIOT Act, FISA thus permits the government to obtain information records of electronic communications that occur wholly within the United States provided these are included in the records obtained to target persons located overseas.

Not only did the USA PATRIOT Act amendments to FISA permit wholesale acquisition of databases of electronic communications in principle, the government used FISA to obtain massive amounts of such records in fact, and it was the disclosure of these practices by former NSA contractor Edward Snowden that brought these practices to the public's attention.[53] On April 25, 2013, the FISA Court ordered Verizon Business Network Services to provide to the FBI "all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad, or (ii) wholly within the United States, including local telephone calls."[54] The

47. *See* 50 U.S.C. § 1861 (West, Westlaw through P.L. 114-115 (excluding 114-95) approved 2015).

48. *Id.* § 1861(a)(1).

49. *Id.* § 1861(b)(2)(B).

50. *Id.* § 1861(b)(2)(B)(iii).

51. *Id.* § 1861(b)(2)(D).

52. *Id.* § 1861(a)(2)(B).

53. Garance Franke-Ruta, *Meet Edward Snowden, the NSA Whistleblower: He's in His 20s, He Votes Third Party, and He's Holed up in Hong Kong*, THE ATLANTIC (June 9, 2013), http://www.theatlantic.com/politics/archive/2013/06/meet-edward-snowden-the-nsa-whistleblower/276688/.

54. In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc., on Behalf of

order required Verizon to produce the records for a period of three months.[55] FISA thus authorizes the government to obtain records of communications between persons located in the United States, provided they are contained within records deemed relevant to an "investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[56] The government could now obtain information regarding the communications of United States persons without any showing that the persons whose records are obtained are engaged in any sort of criminal activity or any activity hostile in any way to the United States.

Judicial review of such requests was highly circumscribed. The judge was required to approve the application upon finding that it satisfied the relevance, minimization, and First Amendment requirements of § 1861.[57] The recipient of an order to produce under § 1861 could challenge the order, but the FISA Court would grant the petition "only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful."[58] Recipients of orders under § 1861 may not disclose the order.[59] The recipient may challenge the nondisclosure provisions of an order, and the court may grant a petition to set aside or modify the nondisclosure provision on a showing that "there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person."[60] Thus, for example, data providers Microsoft, Inc.[61] and Google, Inc.[62] petitioned the FISA Court to authorize disclosing aggregate data concerning government requests to the companies, which remain pending before the FISA Court. Provider Yahoo!, Inc. petitioned the court to publish its opinion and the briefs submitted in its challenge to an order to Yahoo! to produce

---

MCI Communications Services, Inc., d/b/a Verizon Business Services, No. BR 13-80, at 2 (FISA Ct. 2013), https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.

55. *See id.* at 4.

56. 50 U.S.C. § 1861(a)(1).

57. *See id.* § 1861(c)(1).

58. *Id.* § 1861(f)(2)(B).

59. *Id.* § 1861(d).

60. *Id.* § 1861(f)(2)(C).

61. In re Motion to Disclose Aggregate Data Regarding FISA Orders, No. MISC. 13-04 (FISA Ct. 2013).

62. In re Motion for Declaratory Judgment Regarding Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders, No. MISC. 13-03 (FISA Ct. 2013).

issued by the FISA Court,[63] which the court rejected. The FISA Court of Review affirmed the decision.[64]

Other important amendments to FISA effected by the USA PATRIOT Act significantly increased the government's ability to conduct electronic surveillance. These include a provision authorizing roving wiretaps "in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons . . . ."[65] In addition, the USA PATRIOT Act amended FISA to authorize the government to seek court orders authorizing the "installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[66] Finally, the USA PATRIOT Act authorized information obtained through FISA to be used for ordinary criminal investigations and prosecutions provided that a "significant purpose" of the surveillance was to obtain foreign surveillance information, where formerly FISA had required that "the purpose" of the surveillance was to obtain such information.[67]

The government's ability to use information obtained via FISA for criminal prosecutions has proved controversial. The NSA shares information it obtains through FISA requests approved by the FISA Court with other agencies engaged in ordinary law enforcement activities, such as the Drug Enforcement Administration (DEA).[68] What is more, the DEA instructs agents to conceal the source of information it obtains from the NSA by "parallel constructions" of its investigations so that no one, including criminal defendants, will learn the source of information used in the investigations.[69] A parallel construction of an investigation is a false account of the source of the information used in an investigation, created so that no one may discover the true source of the information used to conduct the investigation.[70]

---

63. *In re* Directives to Yahoo! Inc., Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01, 2008 WL 10632524 (FISA Ct. 2008).

64. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

65. 50 U.S.C. § 1805(c)(2)(B) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

66. *Id.* § 1842(a)(2).

67. *See id.* §§ 1804(a), 1823(a).

68. Brian Fung, *The NSA Is Giving Your Phone Records to the DEA. And the DEA Is Covering It up*, WASH. POST (Aug. 5, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/.

69. *See id.*

70. *See id.*

In *In re Sealed Case*, the FISA Court of Review considered whether FISA's requirement that only a "significant purpose" of a FISA request be related to obtaining foreign intelligence information complies with the reasonableness requirement of the Fourth Amendment.[71] In that decision, one of only a small number released to the public, the court held that the USA PATRIOT Act's amendments to FISA were intended to enable the government to obtain foreign intelligence information for ordinary law enforcement purposes, provided that a "significant purpose" of the surveillance is to obtain foreign intelligence.[72] The court was troubled by the PATRIOT Act's amendments to FISA, which made clear that there is, in fact, a distinction to be made between foreign intelligence and law enforcement investigation.[73] This distinction arises from the provision that a "significant purpose" of a surveillance order under FISA must be to gather foreign intelligence, which implies that there may be other statutorily permissible purposes other than foreign intelligence gathering for FISA requests.[74] The court concluded that national security is such a weighty governmental interest that the FISA orders do not violate the Fourth Amendment's reasonableness requirement for searches.[75] Thus, the government may use information obtained via FISA orders for ordinary law enforcement purposes unrelated to national security.

The FISA procedures are strikingly more lenient than those required for a federal wiretap under the Omnibus Safe Streets and Crime Control Act of 1968 ("Omnibus Act").[76] The Omnibus Act procedures require the government to provide a statement under oath of the facts and circumstances showing that a crime is being or is about to be committed, a description of the facilities from which electronic communications will be intercepted, a statement why other investigative techniques have failed or will fail to enable the government to obtain the information sought, and a statement of the length of time for which the information obtained will be kept by the government.[77] To obtain an order permitting a wiretap, the judge must find that there is probable cause that the purported offense is being committed or will be committed and that the wiretap will disclose information regarding the offense.[78]

Under FISA, there is no requirement of probable cause that the surveillance will disclose evidence of a crime, or even of any sort of violent or hos-

71. 310 F.3d 717 (FISA Ct. 2002).
72. *Id.* at 723.
73. *See id.* at 724–25.
74. *See id.* at 729.
75. *See id.* at 744.
76. 18 U.S.C. § 2518 (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).
77. *See id.* § 2518(1).
78. *See id.* § 2518(3).

tile activity. In addition to such acts, definitions of "foreign intelligence information" include attack, sabotage, international terrorism, or the proliferation of weapons of mass destruction.[79] Other covered acts, however, need not be hostile to the United States nor, indeed, hostile toward anyone.[80] "Foreign intelligence information" includes "clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power" and "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to the national defense or the security of the United States; or the conduct of the foreign affairs of the United States."[81]Although the USA PATRIOT Act greatly strengthened the government's ability to conduct electronic surveillance, there were still more changes to come.

C. The USA FREEDOM Act

Americans became aware of the extent of the data collection and surveillance being conducted under FISA through the media disclosures of former NSA contractor Edward Snowden, and as public criticism of the government's conduct mounted, Congress members considered ways to amend the statute to address these criticisms. Congress adopted the USA FREEDOM Act[82] on June 2, 2015, within days of the expiration of the USA PATRIOT Act's provisions regarding electronic surveillance, almost all of which were thereby renewed through 2019. This is a bill that had originally been introduced in Congress following the revelations about the federal government's surveillance activities by whistleblower Eric Snowden.[83] Its ostensible purpose is to reign in the collection and surveillance of Americans' communications.[84] Its chief effect is to end the government's ability to collect and maintain in its possession information about persons' communications in its own databases, but it does very little to limit the government's ability to search the databases of private companies that possess such information. Of particular interest here is the limited changes the law imposes on the courts' ability to monitor the executive branch's activities.

---

79. 50 U.S.C. § 1801(e) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

80. *See id.* § 1801(e)(1).

81. *Id.* § 1801(e)(1)(c), (e)(2)(A)–(B).

82. "USA FREEDOM Act" is an acronym for "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act." USA FREEDOM Act, Pub. L. No. 114-23, § 1(a), 129 Stat. 268, 272 (2015).

83. Ellen Nakashima, *With Deadline Near, Lawmakers Introduce Bill to End NSA Program*, WASH. POST (Apr. 28, 2015), https://www.washingtonpost.com/world/national-security/with-deadline-near-lawmakers-introduce-bill-to-end-nsaprogram/2015/04/28/8fd1cf6e-edb4-11e4-a55f-38924fca94f9_story.html?tid=hybrid_linearcol_1_na.

84. *See id.*

Under the new law, to obtain information from communications providers, the government must offer a "specific selection term" to be used in searching call detail records, which are communications metadata.[85] The requirement of a "specific selection term" is important because its intention is to end the bulk collection of data under Section 215 of the USA PATRIOT Act.[86] In fact, Sections 103 and 501 of the USA FREEDOM Act prohibit bulk collection of data for business records and national security letter collection, respectively. The NSA has announced that it will cease accessing data collected under Section 215 of the USA PATRIOT Act on November 29, 2015, 180 days after the passage of the USA FREEDOM Act, but will maintain the data as long as it has litigation obligations related to the data.[87]

In order to obtain such information from a communications provider under the USA FREEDOM Act amendments to FISA, the government must show:

> (1) reasonable grounds to believe that the call detail records are relevant to such investigation; and (2) a reasonable, articulable suspicion that the specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation for such terrorism.[88]

It is important to note that the government need only show that its specific selection term used to obtain call detail records is relevant to an investigation of international terrorism. There is no requirement that there be any connection between an individual's communication and any potential terrorist activity. It is only the specific selection term itself that has the higher requirement of a reasonable, articulable suspicion of a connection with terrorism. There is a world of difference between these two because there is no requirement of a reasonable suspicion, much less probable cause, to relate a search of a person's communications with terrorist activity.

As before, the role of the courts is limited. The court must determine that the search is limited in duration, that the search term is acceptable under

---

85. USA FREEDOM Act of 2015, 50 U.S.C. § 1861, Pub. L. No. 114-23, § 101(a)(3), 129 Stat. 270 (2015).

86. In *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 792, 826 (2d Cir. 2015), the court concluded that § 215 of the USA PATRIOT Act did not authorize bulk collection because it authorized the collection of things relevant to an investigation authorized under the statute, and bulk collection entailed the collection of irrelevant materials.

87. Office of the Dir. of Nat'l Intelligence, *Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA PATRIOT Act*, IC ON THE RECORD (July 27, 2015), http://icontherecord.tumblr.com/post/125179645313/statement-by-the-odni-on-retention-of-data.

88. USA FREEDOM Act of 2015 § 101(a)(3)(C) (Westlaw).

the statute, and that acceptable minimization procedures are observed.[89] The judge must limit the production period for call records under a request to 180 days and limit the request to two "hops," i.e., an initial request and a second request based on information disclosed by the first request for call detail records, and the court must "adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information."[90] This is not a significant change, in terms of judicial review, over the previous statute. Section 103 of the statute requires courts to include a "specific selection term to be used as the basis for the tangible things sought," and section 104 requires a FISA court to find that the minimization procedures submitted with the application meet applicable FISA standards.[91]

The USA FREEDOM Act attempts, in a weak way, to address the absence of adversarial proceedings in the FISA courts. Section 401 of the statute directs the presiding judges of the FISA Court and the FISA Court of Review to jointly designate at least five individuals to serve as amicus curiae to assist in the consideration of any application for an order or review that presents a novel or significant interpretation of the law, and it "permits FISA courts to appoint an individual or organization to serve as amicus curiae in other instances, including to provide technical expertise."[92]

Section 402 of the USA FREEDOM Act requires the Director of National Intelligence and the Attorney General to act as follows:

> [C]onduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.[93]

That section also authorizes the Director of National Intelligence and the Attorney General to issue such decisions in redacted form or to waive the requirement to declassify such decisions if doing so is "necessary to protect the national security of the United States or properly classified intelligence sources or methods."[94] The requirement to consider declassifying the FISA

89. USA FREEDOM Act of 2015, 50 U.S.C. § 1861, Pub. L. No. 114-23, § 104, 129 Stat. 272 (June 2, 2015).

90. *Id.* §§ 101(b)(3), 401, 402.

91. *Id.* §§ 103(a), 104.

92. *Id.* § 401(i).

93. *Id.* § 402(a).

94. *Id.* § 602(c)(1).

Courts' decisions is an effort to reduce the problem of secret law under FISA. Note, however, that the USA FREEDOM Act places this decision firmly in the hands of the executive branch.

The USA FREEDOM Act is an improvement over the unamended FISA statute, but it is not a great improvement. While it does not authorize the federal government to engage in bulk collection of data and to continue to maintain databases of information of persons' communications, it continues the practice of permitting the government to search the information of any person's communications based upon the search selection term employed. Judicial review of these searches remains limited. The court must consider only the search selection term, whether the search contents are metadata, and the minimization procedures used to limit the exposure of the information obtained. None of these requirements approach the individualized inquiry characteristic of a judicially-authorized search. Instead, they resemble more closely the administrative review of executive action under a highly deferent standard. Furthermore, the efforts to reform the FISA Court and FISA Court of Review grant the Director of National Intelligence and the Attorney General broad discretion to maintain the secrecy of the courts' opinions provided that, in their judgment, maintaining their secrecy is necessary to national security. This does not address the problem of concentrated power in the executive branch. The appointment of amici curiae by the FISA courts to advocate for civil liberties is better than the one-sided proceedings that have predominated in these courts, but it does not establish a norm of adversarial proceedings in which a private party facing governmental coercion has a powerful incentive to litigate vigorously on behalf of their own interests.[95]

D. Unlawful Surveillance Activities and FISA Amendments

Congress and the Bush administration intended the USA PATRIOT Act to strengthen the nation's ability to combat terrorism after the 9/11 attacks on the United States.[96] The Bush administration was convinced that it

95. *See* Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 523, 546–47 (2014) (arguing that adversarial proceedings are needed under FISA).

96. SELECT COMM. ON INTELLIGENCE, TO PERMANENTLY AUTHORIZE CERTAIN PROVISIONS OF THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT) ACT OF 2001, TO REAUTHORIZE A PROVISION OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004, TO CLARIFY CERTAIN DEFINITIONS IN THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, TO PROVIDE ADDITIONAL INVESTIGATIVE TOOLS NECESSARY TO PROTECT THE NATIONAL SECURITY, S. REP. NO. 109-85, at 1–2 (2005), http://www.intelligence.senate.gov/publications/report-accopmany-s-1266-permanently-authorize-certain-usa-patriot-act-provisions-june.

needed to avoid FISA's requirements that it obtain judicial approval for surveillance activities, so it devised and implemented the Terrorist Surveillance Program (TSP) in the mid-2000s.[97] The TSP consisted of warrantless surveillance on persons the Bush administration suspected might be involved in terrorist activities.[98] Under the TSP beginning in 2001 the government intercepted international phone calls,[99] and the NSA's STELLARWIND program mined information from email databases and gathered telephone metadata from the databases of cell phone service providers.[100] The NSA also gathered and analyzed the content of telephone conversations and email communications from these databases,[101] and, from the beginning of the TSP through January 2007, eight percent of the communications analyzed were those of United States persons.[102]

The Bush administration did not inform the FISA Court or Congress about the TSP. Instead, the public learned about the TSP when the administration's warrantless searches were leaked to the New York Times in 2005.[103] The administration's surveillance activities violated FISA because the government had failed to follow the procedures outlined in the statute for obtaining judicial approval for its surveillance and failed to submit the reports to Congress required by FISA and the National Security Act of 1947.[104] Nonetheless, the Bush administration argued that Congress had approved its conduct in the Authorization to Use Military Force (AUMF) in Afghanistan that Congress adopted following the 9/11 terror attacks.[105] The

---

97. OFFICE OF THE INSPECTOR GEN. REP. 11–14 (Nat'l Sec. Agency, Central Sec. Office, Working Draft No. ST-09-0002, 2009), http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

98. SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2007, S. REP. NO. 110-209, at 5–6 (2007).

99. OFFICES OF INSPECTORS GEN. OF THE DEP'T OF DEF., DEPT. OF JUSTICE, CENT. INTELLIGENCE AGENCY, NAT'L SEC. AGENCY, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, REP. NO. 2009-0013-AS, at 5–6 (July 10, 2009), http://fas.org/irp/eprint/psp.pdf.

100. OFFICE OF THE INSPECTOR GEN., *supra* note 97, at 11–14.

101. *Id.* at 5.

102. *See id.* at 15.

103. 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/16program.html?pagewanted=all.

104. *See* Heidi Kitrosser, *Congressional Oversight of National Security Activities: Improving Information Funnels*, 29 CARDOZO L. REV. 1049, 1059–63 (2008) (discussing how reports of intelligence activities to members of Congress have limited oversight value because the reports are disclosed only to leaders on the intelligence committees in the House and Senate, who are obligated to maintain the confidentiality of what they learn in such reports).

105. Memorandum from Alberto R. Gonzalez, Att'y Gen. of the U.S., to William H. Frist, Former Senate Majority Leader 1–3 (Jan. 19, 2006), https:www.justice.gov/sites/default/files/olc/opinions/2006/01/31/nsa-white-paper.pdf.

administration reasoned that since the AUMF authorized the President to use all necessary force to defeat the nation's enemies responsible for the 9/11 attacks, the government had thereby been authorized to conduct surveillance activities it found useful for combating terrorism and was not bound by FISA's requirements in doing so.[106] Thus, for example, on March 11, 2004, White House Counsel Alberto Gonzalez certified the President's authorization to continue the TSP (PSP) because Attorney General John Ashcroft had refused to certify it, and the authorization "explicitly asserted that the President's exercise of his Article II Commander-in-Chief authority displaced any contrary provisions of law, including FISA."[107]

No sanctions of any kind were meted out to Bush administration officials by Congress or the courts for their disregard of FISA. Instead, in 2007, Congress adopted the Protect America Act (PAA), which essentially adopted the Bush administration's TSP.[108] The PAA had a short lifespan, but Congress amended FISA in 2008 in ways that adopted the PAA program, and thus also the TSP program that the Bush administration had used to avoid FISA for several years.[109] It was under this version of FISA that the government was empowered to engage in fishing expeditions through massive databases of information, and through discovery orders it was authorized via FISA to submit to telecommunications companies and internet service providers. The FISA statute, originally intended to impose checks on the ability of the executive branch to engage in surveillance operations against the American people, had come full circle and had enhanced the surveillance capabilities of the federal government to an unprecedented degree.

The 2008 amendments to FISA broadened the government's authority to request blanket surveillance of large quantities of information. Before the 2008 FISA amendments, the government had to obtain a warrant to collect electronic intelligence on communications between persons located in the United States and persons abroad.[110] The application for the warrant had to identify the persons whose communications would be intercepted and show probable cause that they were agents of a foreign power as defined under FISA.[111] Under the 2008 FISA amendments, however, the government is not required to identify the persons whose communications will be intercepted or to show that they are agents of a foreign power. Under

106. *See id*.

107. OFFICES OF INSPECTORS GEN. OF THE DEP'T OF DEF. ET AL., *supra* note 99, at 26.

108. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (codified as amended at 50 U.S.C. §§ 1801–1811 (2006)).

109. 154 CONG. REC. S6386-02 (2008).

110. The current version of these provisions is at 50 U.S.C. § 1805(a) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

111. *See id.*

section 702(a) of the 2008 FISA amendments, the Attorney General and Director of National Intelligence "may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[112] The amendments also impose limitations on collecting information. Section 702(b) of the 2008 FISA amendments prohibits the "targeting" of persons located in the United States, of persons located abroad where the intent is to target persons located in the United States, of United States persons located abroad, and of communications that occur within the United States.[113] Authorizations for the targeting of persons under section 702(a) must be consistent with the Fourth Amendment.[114]

Judicial review of authorizations to acquire electronic communications under section 702(a) is limited. The application to the FISA Court need only state that the procedures to be implemented for the authorization satisfy the targeting and minimization procedures set forth in section 702 and the Fourth Amendment.[115] The targeting procedures should be approved if they "ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States" and "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[116] The minimization procedures should be approved if they satisfy the requirements of FISA.[117] As a result, under the FISA 2008 amendments, the government could conduct large-scale surveillance activities collecting information about communications between persons in the United States and persons located overseas, provided it is the persons overseas who are being targeted and that minimization procedures to protect persons located in the United States are in place. By 2008, Congress had adopted great changes to FISA, which conferred upon the executive branch the ability to conduct large-scale activities with relatively little judicial supervision. The structure of the FISA Court itself further limits the scope of judicial scrutiny of executive branch surveillance activities.

112. 50 U.S.C. § 1881a(a) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).
113. *Id.* § 1881a(b).
114. *Id.* § 1881a(b)(5).
115. *Id.* § 1881a(c)(1).
116. *Id.* § 1881a(d).
117. *Id.* § 1881a(e).

III. THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

The manner in which judges for the FISA Court are chosen circumvents the political process that makes judicial selection accountable to the public. The judges on the FISA Court are chosen by the Chief Justice of the United States Supreme Court.[118] This selection procedure enables the Chief Justice to shape the court in accordance with his own preferences, not only as to personnel but also as to policy. The overwhelming majority of Chief Justice John Roberts's appointees to the court were appointed to the federal bench by Republican presidents, and half of them are former executive branch employees.[119] Roberts's predecessors Burger and Rehnquist appointed fewer Republican-appointed judges and fewer former executive branch employees.[120] Clearly, the method employed for selecting judges for the FISA Court does not provide any sort of public accountability. The method enables one person, not himself an elected official, to appoint judges to the court that reflect the Chief Justice's policy preferences. There are no public hearings or debates about the merits of any appointees to the court. The rationale and basis for such appointments rests with the Chief Justice alone, who does not answer to any authority in the matter.

The spare provisions for adversary proceedings before the FISA Court have had a perceptible impact on the quality of its product quite apart from the overwhelming approval of federal requests for surveillance, which have given the court the appearance, at least, of acting as a virtual rubber stamp for the executive branch. In an October 3, 2011 opinion of the court, released via a Freedom of Information Act request on August 21, 2013, the court stated that the NSA had "circumvented" the FISA statute to obtain domestic telephone and internet communications not appropriate for surveillance activities under FISA.[121] The court stated that it was "troubled that the government's revelations regarding NSA's acquisition of Internet Transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[122] The misrepresentations included claims about the scope of collection of internet communications which, contrary to previous government representations, included information about the names of

118. 50 U.S.C. § 1803(a) (West, Westlaw through P.L. 114-114 (excluding 114-92, 114-94, 114-95 and 114-113) approved 2015).

119. Charlie Savage, *Roberts's Picks Reshaping Secret Surveillance Court*, N.Y. TIMES (July 25, 2013), http://www.nytimes.com/2013/07/26/us/politics/robertss-picks-reshaping-secret-surveillance-court.html.

120. *See id.*

121. Case Name Redacted, 2011 WL 10945618, at *16 (FISA Ct. 2011), https://www.eff.org/node/75426.

122. *Id.* at 16 n.14.

persons in internet transactions, and others included misrepresentations about the manner in which the NSA searched telephone call records it had obtained.[123] As a result of these misrepresentations, the NSA had been permitted by the court to collect and analyze data outside that permitted by FISA and the Fourth Amendment.[124] In spite of these findings, the court approved the targeting and minimization procedures employed by the CIA, NSA, and FBI upon its analysis of changes in those procedures that are redacted from the court's opinion.[125] As to the government's collection of "internet transactions," the court concluded that the NSA's practices regarding the collection of multiple internet communications violated FISA section 702 and the Fourth Amendment.[126]

The court is comprised of eleven United States District judges, but the work of the court is handled by a single judge, as the judges rotate on a weekly basis.[127] The court is assisted by staff attorneys who render an analysis provided to the duty judge, who makes a preliminary decision communicated to the government, which may request a hearing to challenge any modifications to its request.[128] The duty judge may also set a hearing with the government to obtain additional information needed to make a decision on an application.[129] Orders of the court may be appealed by the government or a provider to the FISA Court of Review.[130]

The FISA Court and the FISA Court of Review have developed a body of secret law interpreting the FISA statute and the Fourth Amendment.[131] Secret law is alien to the Anglo-American system of jurisprudence and is inconsistent with the rule of law. The law "must have the capacity to guide people in their actions. Encompassed within this is the notion that law must be transparent (publicly available, knowable) and nonarbitrary. Secret rules, applied in secret, fail this criterion."[132] FISA and the United States Constitution are public documents, but their interpretation by these courts is con-

123. *See id.*
124. *See id.* at 16–18.
125. *See id.* at 18–27.
126. *See id.* at 78–79.
127. Letter from Reggie G. Walton, FISA Ct. Judge, to Patrick J. Leahy, Chairman, S. Judiciary Comm. 1 (July 29, 2013), http://www.leahy.senate.gov/imo/media/doc/Honorable%20Patrick%20J%20Leahy.pdf.
128. *See id.* at 2–3.
129. *See id.* at 6.
130. FISA CT. R. 31.
131. Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.
132. Diane P. Wood, *The Rule of Law in Times of Stress*, 70 U. CHI. L. REV. 455, 467 (2003).

cealed from the public, purportedly on grounds of national security.[133] Only select orders and filings before the FISA courts are disclosed to the public, and these are redacted to protect national security information from disclosure. A judge who authors an opinion or order for the court may publish it *sua sponte* or by a party's motion for release of the order or opinion.[134] The judge may also permit the government to review and redact the opinion or order before it is published.[135] The presiding judge of the court or the government may release orders and opinions of the court to Congress.[136] In releasing decisions and records to the public or to Congress, the court is bound by Executive Order 13526,[137] which sets forth procedures for classifying national security information.[138]

A basic function of the law is to put persons on notice of what is required of them and of how the government will treat them. Thus, as Lon Fuller argued, promulgation to the public is a key feature of a just legal system:

> The laws should also be given adequate publication so that they may be subject to public criticism, including the criticism that they are the kind of laws that ought not to be enacted unless their content can be effectively conveyed to those subject to them. It is also plain that if the laws are not made readily available, there is no check against a disregard of them by those charged with their application and enforcement.[139]

Publicity is such a key feature of any legal system that its absence calls into question the legal validity of the system itself, and the deterioration of this condition signifies the deterioration of the legal system featuring secret laws.[140] Publicity or promulgation is a feature of the rule of law, as is the law's being clear and understandable and that those to whom the law will be applied having notice and an opportunity for a hearing before the law is ap-

133. *See, e.g.*, Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, WALL ST. J. (July 8, 2013), http://www.wsj.com/articles/SB10001424127887323873904578571893758853344.

134. FISA CT. R. 62(a).

135. *Id.*

136. FISA CT. R. 62(c)(2).

137. FISA CT. R. 3.

138. *See, e.g.*, Classified National Security Information, Exec. Order No. 13526, 75 Fed. Reg. 707 (Dec. 29, 2009), http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.

139. LON L. FULLER, THE MORALITY OF LAW 51 (Yale Univ. Press rev. ed. 1969).

140. *See id.* at 39–40.

plied to them.[141] To the extent that laws within a legal system do not have these features, the rule of law and the legitimacy of the system deteriorate.[142]

Prior to the amendments in 2001 and 2008, the FISA Court had been limited to considering requests for specific warrants for electronic surveillance.[143] United States District Judge James Robertson, formerly a member of the FISA Court, has publicly criticized the use to which the FISA amendments have permitted the government to put the court. The court, he stated, "has turned into something like an administrative agency," and "the court is now approving programmatic surveillance. I don't think that is a judicial function."[144] Judge Robertson resigned from the court in 2005 after news reports showed the Bush administration was conducting extensive wiretaps without warrants or approval from the FISA Court.[145] The limited nature of judicial review of applications to acquire information under 50 U.S.C. § 1881a and 50 U.S.C. § 1861 suggests that Judge Robertson's observations about the function of the FISA Court are well-taken.

The FISA Court does not conduct an individualized review of the government's acquisition of the electronic communications of any particular person.[146] Instead, the court reviews the relevance of such communications sought to be obtained pursuant to the very broad scope of records reasonably believed to be related to the conduct of foreign affairs and national security interests of the United States, where these relate to the activities of foreign powers or their agents. The court's inquiry under the broad reach of FISA amounts to a review of administrative procedures to be implemented by the government to acquire information. The FISA Court of Review has expressly held that there is a foreign intelligence exception to the Fourth Amendment's warrant requirement where "surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located

---

141. Robert S. Summers, *The Principles of the Rule of Law*, 74 NOTRE DAME L. REV. 1691, 1693–95 (1999).

142. *See id.* at 1704.

143. PERMANENT SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. REP. NO. 95-1283, pt. 1, at 23 (1978), http:// www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/HPSCI_FISA_Report_95-1283_Pt.1.pdf.

144. Stephen Braun, *Former Judge Admits Flaws in Secret Court*, ASSOCIATED PRESS (July 9, 2013), http://news.yahoo.com/former-judge-admits-flaws-secret-145513130.html.

145. *See id.*; *see also* Risen & Lichtblau, *supra* note 103 (discussing the use of wiretaps, without warrants or approval from the FISA Court, under the Bush administration).

146. *See* Tyler C. Anderson, Note, *Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act*, 8 HARV. J.L. & PUB. POL'Y 413, 426–30 (2014) (arguing that more individualized assessment is needed to effectively monitor surveillance activities).

outside the United States."[147] Where the government's targeting and minimization procedures satisfy FISA and "a significant purpose of a surveillance is to obtain foreign intelligence information," and the relevant executive branch authorities authorized by FISA to apply for surveillance orders have made the required certifications to the court, an application for acquiring electronic communications satisfies the Fourth Amendment's reasonableness requirement.[148] In essence, the court reviews administrative procedures to be implemented by the government. The court reviews the minimization procedures the government will implement to limit dissemination and retention of communications and records obtained under FISA, which indeed is simply a review of a government administrative procedure.[149] The USA FREEDOM Act amendments do not change this in a significant way. They do require the government to show that it seeks to employ a specific selection term that is relevant to an investigation of international terrorism.[150] Such a term is one that the government would presumably use to search the massive databases of information that the government had obtained through Section 215 of the USA PATRIOT Act.[151] The real difference after the adoption of the USA FREEDOM Act is the location of the information the government will search, not the information the government will search.

The lack of an adversary procedure has rendered the court less capable of addressing as well as possible the complex constitutional and statutory questions surrounding the government's large-scale acquisition of electronic communications and information regarding such communications. It is important that the FISA courts are developing legal doctrines such as the foreign intelligence exception to the warrant requirement in non-adversarial proceedings in which the only party is the government. In the Anglo-American system of justice, the adversary system has proven a means by which courts are afforded the benefit of hearing the best arguments that two opposing sides in a dispute can offer on their own behalf and against each other's. In the absence of adversary proceedings, the FISA courts hear from the government only and not from parties who contend the government's powers to conduct surveillance operations on the American people should

147. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

148. *Id.* at 1014.

149. 50 U.S.C. § 1881a(d)(2) (West, Westlaw current through P.L. 114-115 (excluding 114-94 and 114-95) approved 2015).

150. USA FREEDOM Act of 2015, 50 U.S.C. § 1861, Pub. L. No. 114-23, § 101(a)(3), 129 Stat. 270 (2015).

151. *But see* Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 50 (2014) (arguing that the "specific selection term" requirement represents a genuine congressional effort to limit the scope of searches to terror-related matters).

be more limited than we have learned they are only recently. Under these conditions, it is hardly surprising that the FISA Court's decisions overwhelmingly approve government requests for surveillance, and it is likewise unsurprising that the FISA courts have generally approved what became a massive intelligence-gathering operation by the government, in which the government scooped up millions of communications and records of communications of Americans.

Some of the weaknesses of the regime established in 1978 by FISA lay in the idea that there needed to be a separate set of courts to address questions under the statute. In *United States v. United States District Court (Keith)*, the Supreme Court held that the government was obliged under the Fourth Amendment to obtain a warrant to conduct electronic surveillance on persons who plotted to bomb a CIA office in Michigan, where all the conspirators were Americans.[152] The *Keith* Court rejected the government's argument that the needs of domestic surveillance supported an exception to the Fourth Amendment's warrant requirement:

> We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. Certainly courts can recognize that domestic security surveillance involves different considerations from the surveillance of "ordinary crime." If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.
>
> Nor do we believe prior judicial approval will fracture the secrecy essential to official intelligence gathering. The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III of the Omnibus Crime Control and Safe Streets Act already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason, §§ 2516 (1)(a) and (c), each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an ex parte request before a magistrate or judge. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to

152. 407 U.S. 297, 299, 320 (1972).

> the point of allowing the Government itself to provide the necessary clerical assistance.[153]

The reasoning in *Keith* applies to the conduct of electronic intelligence under FISA. Federal courts are capable of handling sensitive information and deciding cases where information has been sealed to protect its confidentiality. Consideration of FISA applications by United States District judges, not of one court only, but of multiple courts reflecting the diversity of the federal judiciary, developing the law in a transparent manner so that there is no secret law as a matter of course and not by discretionary decisions of the executive branch (as under the USA FREEDOM Act) would make the judiciary a more effective check on executive power than exists under FISA.

The purpose of FISA and the establishment of the FISA courts was to impose legal and judicial checks on the ability of the executive branch to conduct surveillance activities and to store information obtained from them.[154] The USA PATRIOT Act and amendments to the FISA statute in 2007 and 2008 have been intended to enhance the power of the executive branch to conduct such activities, and they did so.[155] The political situation that evolved from the terror attacks of September 11, 2001 made it easier for Congress to place more power in the hands of the executive branch to fight terrorism, and the weak form of judicial review exercised by the FISA courts, combined with the lack of transparency surrounding their decisions and operations, rendered them a very weak institutional check against the concentration of unmonitored power in the executive branch agencies that used FISA to conduct electronic intelligence gathering. This is destructive of the separation of powers and contributes to the general growth in the power of the executive branch.

IV. SEPARATION OF POWERS

Throughout American history, national security threats have often prompted the exercise of unchecked power by the executive branch, often with congressional approval, and this includes the federal government's response to the 9/11 attacks.[156] The accumulation of power in the executive

153. *Id.* at 320–21.

154. PERMANENT SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. REP. NO. 95-1283, pt. 1, at 21–22 (1978), http://www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/HPSCI_FISA_Report_95-1283_Pt.1.pdf.

155. SELECT COMM. ON INTELLIGENCE, REP. TO THE SENATE, S. REP. NO. 111-6, at 1–6 (2009).

156. *See* LOUIS FISHER, THE CONSTITUTION AND 9/11: RECURRING THREATS TO AMERICA'S FREEDOMS 361, 364 (Univ. Press of Kan. 2008); *see also* David G. Delaney, *Cybersecurity*

branch brought on by the national security crisis made clear by the 9/11 attacks is a real challenge to the separation of powers and the rule of law in the United States. Such power has been concentrated in the executive branch and its national security apparatus within the last decade that neither Congress nor the courts can effectively check the continued growth of executive supremacy over domestic security. This concentration of power has continued, as the recent revelations in the press have made clear, as the executive branch develops further its ability to monitor the communications and activities of Americans in the United States. The separation of powers principle, supported by the system of checks and balances in the United States Constitution, is the cornerstone of our system of government and was believed by the Constitution's framers to be the bulwark of limited government and individual liberty. It is this principle and idea that is degraded as the executive branch claims such independence from control and exercises such independence from control in fact, that legislative and judicial checks on executive power prove ineffectual and pose a genuine threat to the rule of law in the United States.

The Framers regarded separation of powers as essential to limiting the overall power possessed by the national government and essential to the ability of the people to hold the government politically accountable for its decisions and actions.[157] "The accumulation of all powers, legislative, executive, and judiciary, in the same hands, whether of one, a few, or many, and whether hereditary, self-appointed, or elective, may justly be pronounced the very definition of tyranny."[158] Madison recognized that the doctrine of the separation of powers, taken over by the Framers of the United States Constitution and various state constitutions from Montesquieu,[159] Locke,[160] and Blackstone,[161] did not require a strict and total separation of authority among the legislative, executive, and judicial branches, but rather a separation of function among them, so that none might usurp the authority entrusted to another. On the contrary, each of the different branches must be authorized to check the powers of the others by mechanisms involving each in the operations of the other two in order to preserve the separation of powers: "unless these departments be so far connected and blended as to give to

---

and the Administrative National Security State: Framing the Issues for Federal Legislation, 40 J. LEGIS. 251, 265, 268–69 (2013–2014) (arguing that excessive focus on security emergencies has prevented Congress from addressing other important technological, political, and economic matters).

157. THE FEDERALIST NO. 51 (James Madison) (Jacob E. Cooke ed., 1961).

158. THE FEDERALIST NO. 47, at 324 (James Madison) (Jacob E. Cooke ed., 1961).

159. *See, e.g.*, MONTESQUIEU, THE SPIRIT OF THE LAWS, Bk. 11, Ch. 6 (1750).

160. *See, e.g.*, JOHN LOCKE, TWO TREATISES OF GOVERNMENT, II, §§ 143–59 (1689).

161. *See, e.g.*, WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, BOOK ONE, 149–50 (Clarendon Press, Oxford 2009) (1765).

each a constitutional control over the others, the degree of separation which the maxim requires, as essential to a free government, can never in practice be duly maintained."[162] The separation of powers thus rests ultimately on the checks and balances: "but in which the powers of government should be so divided and balanced among several bodies of magistracy, as that no one could transcend their legal limits, without being effectually checked and restrained by the others."[163] The Framers of the United States Constitution "laid its foundation on this basis, that the legislative, executive, and judiciary departments should be separate and distinct, so that no person should exercise the powers of more than one of them at the same time. But no barrier was provided between these several powers."[164] A plain constitutional statement that the powers of each branch should be inviolate is insufficient to preserve the separation of powers in fact. That is, "a mere demarcation on parchment of the constitutional limits of the several departments, is not a sufficient guard against those encroachments which lead to a tyrannical concentration of all the powers of government in the same hands."[165] Checks and balances among the different branches are needed to preserve the separation of powers and prevent the accumulation of power in one institution of government:

> This policy of supplying, by opposite and rival interests, the defect of better motives, might be traced through the whole system of human affairs, private as well as public. We see it particularly displayed in all the subordinate distributions of power, where the constant aim is to divide and arrange the several offices in such a manner as that each may be a check on the other—that the private interest of every individual may be a sentinel over the public rights. These inventions of prudence cannot be less requisite in the distribution of the supreme powers of the State.[166]

The key to preserving the separation of powers is that each branch of government is able to limit the power of the other two branches.

The development of the surveillance apparatus in the executive branch has undermined the separation of powers. It has undermined congressional oversight of the implementation of laws the Congress has enacted to impose limits on the conduct of surveillance activities by the executive branch. While Congress adopted FISA to check the ability of the executive branch to conduct surveillance operations,[167] surveillance operations have expanded

---

162. THE FEDERALIST NO. 48, at 332 (James Madison) (Jacob E. Cooke ed., 1961).
163. *Id*. at 335.
164. *Id*.
165. *Id*. at 338.
166. THE FEDERALIST NO. 51, *supra* note 157, at 349.
167. PERMANENT SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. REP. NO. 95-1283, pt. 1, at 21 (1978), http://

dramatically since 9/11.[168] Congress adopted FISA in part because the executive branch failed to provide Congress with the information Congress needed to make decisions about the propriety of surveillance activities.[169] But Congress has subsequently adopted laws, such as the USA PATRIOT Act and the 2008 amendments to FISA, that have given the executive branch carte blanche to gather information about United States persons, provided the "target" is some foreign power or agent thereof. In its haste to do something to protect Americans from further terrorist attacks after 9/11, Congress has given away the store to the executive branch.

The development of surveillance activities in the executive branch has undermined judicial control over the executive branch. This has happened in part because the surveillance courts have become a rubber stamp for the executive branch. From 1979 through 2012, the government requested 35,537 orders for surveillance under FISA, and the FISA Court approved 35,530 such requests.[170] In that same period, the court rejected only twelve government requests for surveillance.[171] The court never rejected any government request for surveillance until 2003.[172] Judge Reggie Walton, former presiding judge of the FISA Court, has stated that the number of FISA requests approved by the court does not indicate that the court acts as a rubber stamp for the executive branch:

> The perception that the court is a rubber stamp is absolutely false. . . . There is a rigorous review process of applications submitted by the executive branch, spearheaded initially by five judicial branch lawyers who are national security experts and then by the judges, to ensure that the court's authorizations comport with what the applicable statutes authorize.[173]

Of the 1588 applications for FISA surveillance the government presented to the FISA Court in 2013, for example, the FISA Court modified only thirty-four of them.[174]

---

www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/HPSCI_FISA_Report_95-1283_Pt.1.pdf.

168. *See FISA Ct. Orders 1979–2014*, *supra* note 3.

169. *See* THE FEDERALIST NO. 51, *supra* note 157.

170. *FISA Ct. Orders 1979–2014*, *supra* note 3.

171. *See id*.

172. *See id*.

173. Spencer Ackerman, *FISA Judge Defends Integrity of Court over Verizon Records Collection*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance.

174. Letter from Peter J. Kadzick, Principal Deputy Assistant Att'y Gen., to Harry Reid, Senate Majority Leader (Apr. 30, 2013), https://www.justice.gov/sites/default/files/nsd/legacy/2014/07/23/2013fisaltr.pdf; s*ee also* Laura K. Donohue, *Bulk Metadata Collection:*

The approval rate for FISA surveillance requests is not conclusive evidence that the FISA Court has given carte blanche to the executive branch to conduct surveillance operations that sweep up millions of communications by Americans into government databases. The approval rates for federal wiretaps in ordinary criminal investigations also have very high approval rates.[175] What created the rubber stamp was Congress, which adopted amendments to FISA that fundamentally altered the manner in which the FISA Court would examine requests for surveillance under FISA.

As a result, the very limited review that the FISA Court exercises over government requests for surveillance imposes only a minimal check on the exercise of executive power under FISA. This very limited review has enabled executive branch officials to claim that their surveillance activities are approved by the courts.[176] The stamp of judicial approval has served to enhance executive power with little judicial supervision of executive acts. Hamilton warned of the threat presented where the judiciary, as the "weakest" branch, would become subservient to executive branch interests:

> [L]iberty can have nothing to fear from the judiciary alone, but would have everything to fear from its union with either of the other departments; that as all the effects of such a union must ensue from a dependence of the former on the latter, notwithstanding a nominal and apparent separation; that as, from the natural feebleness of the judiciary, it is in continual jeopardy of being overpowered, awed, or influenced by its coordinate branches; and that as nothing can contribute so much to its firmness and independence as permanency in office, this quality may therefore be justly regarded as an indispensable ingredient in its constitution, and, in a great measure, as the citadel of the public justice and the public security.[177]

It is arguable that the judiciary has been "captured" by the executive branch through FISA and the FISA courts. When the FISA Court stated that the government had misrepresented important facts about its surveillance activities to the court on numerous occasions, there is no hint that the court imposed any sanction on the government for its misconduct.[178] Any practicing lawyer would be amazed at the FISA Court's tolerance of such misconduct.

Statutory and Constitutional Considerations, 37 HARV. J.L. & PUB. POL'Y 757, 834–35 (2014) (arguing that high approval rate evidences weak oversight).

175. ADMIN. OFFICE OF U.S. COURTS, WIRETAP REPORT 2012, TABLE 7: AUTHORIZED INTERCEPTS GRANTED PURSUANT TO 18 U.S.C. § 2519 AS REPORTED IN WIRETAP REPORTS FOR CALENDAR YEARS 2002–2012, http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2012/Table7.pdf.

176. Memorandum from Alberto R. Gonzalez, *supra* note 105, at 17.

177. THE FEDERALIST NO. 78, at 524 (Alexander Hamilton) (Jacob E. Cooke ed., 1961).

178. *See* Case Name Redacted, 2011 WL 10945618 (FISA Ct. 2011).

The rule of law is built into our constitutional system through the separation of powers and checks and balances. It is these central features of our system of government that are designed to promote, though not guarantee, that power is exercised in accordance with law. When its historical advocates refer to the tyranny that results from the accumulation of power in the hands of one institution of government, they mean government by the will of one institution unchecked by law.[179] The rule of law is not an end in itself, but is instead a means to see that power is exercised by government in a manner that promotes the shared interests of the political community rather than promoting the interests of one section of that community to the detriment of others. It appears in Western thought first in Aristotle's *Politics* expressly for this function.[180] When Aristotle argued that the best form of political community is one in which power is shared by different social classes and governed by law, he established the line of thought that grew into modern constitutionalism.[181] When Montesquieu, Blackstone, Madison, and others write in support of the separation of powers principle, they continue the thought that to be limited by law, power should be shared and checked by competing interests. The alternative, they argue, is power concentrated in one institution, which, as Madison suggested, "is the very definition of tyranny."[182]

The separation of powers demands that there be effective judicial and legislative checks on the exercise of executive power, but the structure of the regime for electronic surveillance and intelligence gathering under FISA fails to establish such checks. The statute gives courts very limited control over the conduct of the executive branch agencies responsible for these programs, and Congress, due to understandable concerns over national security threats, has not insisted on extensive monitoring or control over these agencies. In fact, as I have shown here, Congress has acquiesced in executive branch demands for very limited monitoring over its intelligence-gathering programs. FISA and the amendments to the statute over the last fifteen years have contributed to the concentration of power in the executive branch and, therefore, to the degradation of the separation of powers in our system of government.

V. CONCLUSION

Changing technology and new threats, perceived or real, gave rise to governmental intelligence-gathering activities that prompted Congress to

179. THE FEDERALIST NO. 47, *supra* note 158, at 324.

180. *See* ARISTOTLE, THE POLITICS, Bk. IV, ch. 11 (R.F. Stalley ed., New York, Oxford Univ. Press 1958).

181. Ernest Barker, *Introduction* to ARISTOTLE, THE POLITICS lx.

182. THE FEDERALIST NO. 47, *supra* note 158, at 324.

adopt FISA in 1978 in an effort to impose legal and institutional checks on the power of the executive branch agencies responsible for such programs. Further changes in technology and new security threats prompted Congress to amend FISA to give these agencies more authority and latitude to strengthen national security through electronic surveillance and intelligence gathering, which resulted in a largely unregulated exercise of such power by the mid-2000s. Congress responded by giving these agencies still more authority, until public disclosures of abuses led to calls for reform by 2013. This narrative parallels the historic trend of growth and concentration of power in the federal government generally and in the executive branch thereof in particular. Congress understandably does not want to be accused of failing to protect the public against another 9/11 style terror attack, but Congress has not served our system of government well because it has failed to establish an effective judicial check on executive power under FISA. The separation of powers is a core principle of American government, and FISA has contributed to its deterioration.