

Campbell Law Review

Volume 37 | Issue 3

Article 5

2015

Reforming the Foreign Intelligence Surveillance Court to Curb Executive Branch Abuse of Surveillance Techniques

Allison E. Persinger

Follow this and additional works at: <http://scholarship.law.campbell.edu/clr>

Recommended Citation

Allison E. Persinger, *Reforming the Foreign Intelligence Surveillance Court to Curb Executive Branch Abuse of Surveillance Techniques*, 37 CAMPBELL L. REV. 519 ().

This Note is brought to you for free and open access by Scholarly Repository @ Campbell University School of Law. It has been accepted for inclusion in Campbell Law Review by an authorized administrator of Scholarly Repository @ Campbell University School of Law.

Reforming the Foreign Intelligence Surveillance Court to Curb Executive Branch Abuse of Surveillance Techniques

ABSTRACT

As intelligence agencies like the NSA increase their surveillance activities on law-abiding citizens, the need for protection of privacy rights becomes apparent. The Foreign Intelligence Surveillance Court (FISC) was designed to protect this fundamental right, but due to changes in the law and to the structure of the court, the court's role as a watchdog has been weakened. This Comment provides an overview of amendments to the Foreign Intelligence Surveillance Act that have tempered the court's role, including the USA FREEDOM Act of 2015 (Freedom Act), and discusses the need for reform of the FISC due to the unwieldy nature of surveillance agencies. Ultimately, this Comment identifies structural changes that could restore the court to the protector of privacy rights that it was initially intended to be.

INTRODUCTION

Imagine placing a call to a relative or an acquaintance in a foreign country and automatically having every detail of your call recorded—the duration, the contents of the conversation, and your phone number. You are not suspected of any criminal activity; however, an individual that your acquaintance contacted is suspected of a terrorist-type plot or some other activity that a United States intelligence agency deems threatening to national security interests. Would you feel comfortable having every phone conversation recorded for the sake of protecting the country? In July 2014, Americans discovered that this was not a hypothetical scenario—the United States government was collecting vast amounts of telephone data on American citizens.¹

1. See generally Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, *GUARDIAN* (June 6, 2013, 6:05 AM), <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (discussing a court order that “shows for the first time that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing”).

In the 1970s, the Executive Branch collected large amounts of data for the purpose of protecting national security interests, including communications of U.S. citizens.² In response, Congress passed the Foreign Intelligence Surveillance Act (FISA) to ensure that the privacy rights of American citizens would not be violated.³ FISA set up the FISC, primarily to review requests for surveillance to collect foreign intelligence.⁴ This system was designed to ensure that the government was not actively intercepting wholly domestic communications in an attempt to avoid having to obtain a search warrant.⁵ Subsequent amendments to FISA following the terrorist attacks on September 11, 2001, have severely handicapped the role of the FISC by lowering the standards that the government must meet to obtain permission for surveillance.⁶ As a result, the government has collected a massive amount of information on foreigners and Americans alike.⁷ At the center of the controversy lies the National Security Agency (NSA), the United States intelligence agency that decides what information can be collected under broad orders issued by the FISC.⁸

The FISC is in critical need of reform that effectively curtails the surveillance state and protects citizens from governmental intrusion into individuals' communications. Many of the current reform proposals are inadequate to address this goal. To effectuate the original purpose of the FISC, the court must be restructured and made more transparent.

This Comment proposes several reforms that will aid in reining in the surveillance state. First, the FISC needs more sitting judges, and those judges' terms should be extended. Second, court personnel and judges should be empowered with greater investigatory powers, enabling them to perform their own research rather than relying solely on information

2. Jeremy D. Mayer, *9-11 and the Secret FISA Court: From Watchdog to Lapdog?*, 34 CASE W. RES. J. INT'L L. 249, 249–50 (2002).

3. *Id.* at 249.

4. J. Christopher Champion, Note, *The Revamped FISA: Striking a Better Balance Between the Government's Need to Protect Itself and the 4th Amendment*, 58 VAND. L. REV. 1671, 1681 (2005).

5. *Id.* at 1672–73.

6. See *infra* notes 46–75 and accompanying text.

7. U.S. *Domestic Surveillance*, COUNCIL ON FOREIGN REL. (Dec. 18, 2013), <http://www.cfr.org/intelligence/us-domestic-surveillance/p9763#p1>.

8. See Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html (noting that the FISC relies heavily on the accuracy of information provided to it by the NSA because of the court's practical investigatory limitations and, similarly, it does not have the resources to investigate all instances of noncompliance with its orders).

supplied by the government. Third, to increase transparency, the FISC should be required to release a reasonably detailed account of its procedures for reviewing governmental-surveillance applications.

Part I of this Comment gives a brief history of FISA and the FISC, as well as the subsequent amendments to FISA that have severely weakened the role of the court. Part II exposes how unwieldy the NSA and other intelligence-gathering agencies have become, as well as problems with the FISC that have played a role in that expansion. Part III outlines some of the most popular reform proposals, such as allowing testimony or input from third parties, greater transparency, and greater oversight. In closing, Part IV evaluates the best solutions—those with the highest potential to have meaningful and lasting results in reining in surveillance activities—with a heavy focus on implementing structural changes to the FISC.

I. HISTORY OF FISA AND THE FISC

The initial aim of FISA was to curtail abusive intelligence-gathering practices taken against American citizens by the Executive Branch that were so obtrusive as to raise Fourth Amendment concerns.⁹ Through the amendments to FISA, Congress has expanded FISA's scope, decreased the oversight of government officials conducting surveillance operations, and made it easier for communications involving American citizens to be monitored.¹⁰ Additionally, FISA amendments have given the FISC a more limited role to play in intelligence-gathering.¹¹ This lack of oversight has allowed the NSA to gather private information on companies and citizens.¹²

A. *How the FISC Works*

The original FISA of 1978 set up two courts, the FISC and the Foreign Intelligence Surveillance Court of Review (FISCR).¹³ The FISC was initially composed of seven sitting federal district court judges who were charged with determining when to issue warrants for surveillance.¹⁴ Composed of three circuit court judges, the FISCR was established to hear appeals in the event that the FISC denied a government application for

9. Mayer, *supra* note 2, at 249.

10. See *infra* notes 76–108 and accompanying text.

11. See *infra* notes 109–23 and accompanying text.

12. See *infra* notes 76–123 and accompanying text.

13. See Note, *Shifting the FISA Paradigm: Protecting Civil Liberties by Eliminating Ex Ante Judicial Approval*, 121 HARV. L. REV. 2200, 2201 (2008).

14. *Id.*

surveillance.¹⁵ Later amendments increased the number of FISC judges to eleven, each selected by the Chief Justice of the United States Supreme Court.¹⁶ The judges serve for nonrenewable terms of no more than seven years and they travel to Washington, D.C. to preside over hearings on a rotating basis.¹⁷

FISA courts are established under Article III of the United States Constitution through Congress's power to create inferior courts.¹⁸ While this fact draws similarities among FISA courts and United States district courts and circuit courts of appeal, FISA courts operate unlike any other Article III court.¹⁹ The proceedings in FISA courts are closed-door, and the public typically does not have access to issued opinions.²⁰ Judge Pauley of the United States District Court for the Southern District of New York acknowledges that FISA courts are exceptions to the general openness and transparency of Article III courts, citing national security interests as justification for their secrecy.²¹

1. *FISC Consideration of Surveillance Applications*

Because of post-FISA amendments, surveillance applications must pass through several rounds of review before they are approved. In the first step toward FISC approval, general counsel at the NSA drafts a warrant application at the request of an intelligence-agency officer.²² The Attorney General must then certify that the target of surveillance is a "foreign power" or an "agent" of a foreign power and, in the case of a United States citizen, that the target may be involved in a crime.²³ After the court has

15. *Id.*

16. Owen Fiss, *Even in a Time of Terror*, 31 YALE L. & POL'Y REV. 1, 4–5 (2012) (citing 50 U.S.C. § 1803(a) (2012)).

17. *History of the Federal Judiciary: Foreign Intelligence Surveillance Court*, FED. JUD. CTR., http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html (last visited Sept. 5, 2015).

18. U.S. CONST. art. III, § 1; *see* ACLU v. Clapper, 959 F. Supp. 2d 724, 731 (S.D.N.Y. 2013) (referring to the FISC judges as "Article III judges" and noting that the FISC operates the same as any other Article III court).

19. *Clapper*, 959 F. Supp. 2d at 731.

20. *Id.* The newly enacted Freedom Act allows the Director of National Intelligence, in consultation with the Attorney General, to conduct a "declassification review" of FISC and FISCR orders that will make opinions, or specific selections from court opinions, "publicly available to the greatest extent practicable." USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 602(a)–(b), 129 Stat. 268, 281 (2015) (codified at 50 U.S.C. §§ 1872(a)–(b) (2012)).

21. *Clapper*, 959 F. Supp. 2d at 731.

22. *History of the Federal Judiciary*, *supra* note 17.

23. *Id.*

this information, it begins 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.”²⁴

There is limited information concerning how the court decides which of the government’s requests to approve or deny. It is also unclear how the court interprets important terms in various FISA statutes.²⁵ As Senator Jeff Merkley of Oregon points out, “[w]e can’t really propose changes to the law unless we know what the words mean as interpreted by the court.”²⁶

Whatever processes the court employs, it has been heavily criticized for its extreme secrecy and for the lack of adversarial proceedings in deciding questions of individual privacy. The lack of transparency risks potential abuse, especially since court orders are unavailable to the public and the surveillance targets will never know that they were under observation.²⁷

To make matters worse, the FISC grants nearly all of the government’s surveillance requests. In 2012, the FISC reviewed approximately 1800 applications and rejected none.²⁸ In 2005, U.S. Attorney General Gonzales explained that of the 1758 applications in 2004, none were denied, but 94 were substantially modified by the FISC.²⁹ In the court’s thirty-three-year history, only 11 of 34,000 applications have been rejected.³⁰

Although there is some evidence that the FISC may modify requests before accepting them, the furtive nature of the court’s proceedings and the unwillingness to deny the government’s surveillance requests lead many to question what the court does behind closed doors. In fact, some

24. Spencer Ackerman, *FISA Chief Judge Defends Integrity of Court Over Verizon Records Collection*, GUARDIAN (June 6, 2013, 4:17 PM), <http://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance>.

25. *Id.* Some of these important terms define what “tangible items” means or, with regard to the PATRIOT Act, what “related to an investigation” means. *Id.*

26. *Id.*

27. Note, *supra* note 13, at 2206 (citing Kelly J. Smith, Note, *An Enemy of Freedom: United States v. James J. Smith and the Assault on the Fourth Amendment*, 39 LOY. L.A. L. REV. 1395, 1417 (2006)). *But see* USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 602(a)–(b), 129 Stat. 268, 281 (2015) (codified at 50 U.S.C. §§ 1872(a)–(b) (2012)); *supra* note 20.

28. Richard Blumenthal, *FISA Court Secrecy Must End*, POLITICO (July 14, 2013, 11:15 PM), <http://www.politico.com/story/2013/07/fisa-court-process-must-be-unveiled-94127.html>.

29. *USA PATRIOT Act: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 90–91 (2005) (statement of Alberto R. Gonzales, Att’y Gen. of the United States, and Robert S. Mueller, III, Director, Federal Bureau of Investigation).

30. Blumenthal, *supra* note 28.

characterize the FISC as “a secret kangaroo court that legitimates mass surveillance of Americans’ communications with employers, friends, and family in other countries by lending it the appearance, but not the substance, of judicial oversight.”³¹

Because almost all of the government’s surveillance applications are accepted, the appeals process through the FISC is rarely utilized. Twenty-four years after its inception, the FISC met for the first time in 2002.³² In the unlikely event that the FISC and the FISC were to deny one of the government’s petitions, officials are able to request review by the United States Supreme Court.³³

Because of the relaxed FISA requirements, the court now has almost meaningless oversight over the intelligence-gathering process. The FISC seems to exist purely for show, giving citizens hollow reassurance that their communications are not being unconstitutionally monitored. Because the court’s oversight is so insignificant, the laws governing the FISC must be amended to transform the court back to the powerful protector of constitutional rights that it was originally intended to be.

B. *The Foreign Intelligence Surveillance Act of 1978*

Congress enacted FISA in 1978 to permit the government to engage in electronic surveillance for the purpose of capturing foreign-intelligence information.³⁴ Prior to this legislation, the Executive Branch claimed an implicit right to perform warrantless electronic surveillance to protect national security interests under Article II of the United States Constitution, which allows the executive to “preserve, protect and defend the Constitution of the United States.”³⁵

In its report, one Senate Committee found that under this regime, the government “[had] swept in vast amounts of information about the personal

31. Jennifer Granick & Christopher Sprigman, *The Secret FISA Court Must Go*, DAILY BEAST (July 24, 2013, 4:45 AM), <http://www.thedailybeast.com/articles/2013/07/24/the-secret-fisa-court-must-go.html>.

32. *In re Sealed Case*, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

33. *Foreign Intelligence Surveillance Court*, ALLGOV.COM, <http://www.allgov.com/departments/departments-of-justice/foreign-intelligence-surveillance-court?agencyid=7206> (last visited Sept. 5, 2015).

34. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

35. CONST. art. II, § 1, cl. 7; see also James G. McAdams, III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, FED. L. ENFORCEMENT TRAINING CTRS. 2 (2007), <http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf>.

lives, views, and associations of American citizens.”³⁶ As a result of these findings, the Committee recommended that Congress create guidelines to ensure that the surveillance process operated legally and efficiently.³⁷

Congress responded by passing a law on October 5, 1978, that laid out procedures with which the Executive Branch would have to comply before the FISC would grant an order allowing it to obtain foreign intelligence via electronic surveillance.³⁸ The purpose of the new legislation was to protect the civil liberties of Americans by preventing the government from monitoring citizens’ communications without an individualized warrant, as required by the Fourth Amendment.³⁹ The President of the United States was authorized to acquire foreign intelligence for up to one year without a warrant,⁴⁰ so long as there was “no substantial likelihood” that any communications by a United States citizen would be received.⁴¹

The newly created FISC was tasked with issuing warrants pursuant to applications approved by the Attorney General.⁴² Whenever domestic or international telephone calls were transmitted through facilities located in the United States, the Attorney General had to seek permission from the FISC before intercepting the calls.⁴³ FISA allowed the FISC to issue surveillance orders only if there was probable cause that the target of the electronic surveillance was a “foreign power” or an “agent of a foreign power.”⁴⁴ In its report, the Senate Intelligence Committee made clear that the primary purpose of the surveillance must be for foreign-intelligence gathering.⁴⁵

The language of FISA and the initial Senate Committee Report point to the overarching purpose of FISA: the need to protect the constitutional rights of American citizens from encroachment by the government.

36. S. REP. NO. 94-755, at 5 (1976).

37. *Id.* at 296–98.

38. FISA of 1978 §§ 104–105 (codified as amended at 50 U.S.C. §§ 1804–1805 (2012)).

39. Glenn Greenwald, *FISA Court Oversight: A Look Inside a Secret and Empty Process*, GUARDIAN (June 18, 2013, 7:36 PM), <http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy>.

40. FISA of 1978 § 102.

41. *Id.*

42. *Id.* § 104.

43. Fiss, *supra* note 16, at 15.

44. FISA of 1978 § 105(a)(3)(A).

45. Joshua H. Pike, Note, *The Impact of a Knee-Jerk Reaction: The PATRIOT Act Amendments to the Foreign Intelligence Surveillance Act and the Ability of One Word to Erase Established Constitutional Requirements*, 36 HOFSTRA L. REV. 185, 201 (2007).

C. Expansions of FISA

The amendments to FISA since its promulgation have substantially diminished the initial protections of the Act. The new, more lenient standards for obtaining a FISC order ensure that a staggering amount of American citizens' data is swept up during foreign surveillance.

1. The PATRIOT Act of 2001

One month after the terrorist attacks of September 11, 2001, Congress amended FISA by enacting an act titled the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," also known as the USA PATRIOT Act (Patriot Act).⁴⁶ The Patriot Act's stated purpose is to "provide[] enhanced investigative tools and improve[] information sharing for the law enforcement and intelligence communities to combat terrorism and terrorist-related crimes."⁴⁷ By improving investigative tools and information sharing, Congress hoped to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities."⁴⁸ The Patriot Act was the starting point for subsequent amendments to FISA that ultimately allowed the government to collect information in a wider range of circumstances.⁴⁹

The Patriot Act contains three main provisions that authorized the expansion of FISA and increased the government's ability to conduct surveillance operations.⁵⁰ First, the Act requires foreign-intelligence gathering to be "a significant purpose" of the surveillance, which is a departure from the 1978 Act, which required the collection to be the sole or "primary purpose."⁵¹ Second, the Act allows "roving wiretap[s]," which authorizes surveillance of any communication to or by a target without specifying the particular communications meant to be monitored.⁵² Finally, the Patriot Act allows the government to obtain an order from the FISC for

46. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, H.R. REP. NO. 107-236, at 1-42 (2001).

47. H.R. REP. NO. 107-236, at 41.

48. *Id.*

49. EDWARD C. LIU, CONG. RESEARCH SERV., R40138, AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) EXTENDED UNTIL JUNE 1, 2015, at 1 (2011), <http://www.fas.org/sgp/crs/intel/R40138.pdf>.

50. *Foreign Intelligence Surveillance Act (FISA)*, EPIC.ORG, <http://epic.org/privacy/terrorism/fisa/> (last visited Sept. 5, 2015).

51. *Id.*

52. *Id.*

a pen register or trap-and-trace device without showing that the target was “an agent of a foreign power.”⁵³

2. *Protect America Act of 2007*

Several years after the Patriot Act was enacted, Congress passed the Protect America Act (PAA), which some viewed as an expansion on the government’s surveillance powers.⁵⁴ The Department of Justice described the purpose of the PAA as modernizing FISA to provide the intelligence community with key tools for acquiring information about potential terrorists.⁵⁵ The Department of Justice claimed that the PAA “restore[d] FISA to its original focus of protecting the rights of persons in the United States, while not acting as an obstacle to gathering foreign intelligence on targets located in foreign countries.”⁵⁶

The introduction to the PAA explains that “[n]othing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.”⁵⁷ The PAA also lowered the burden of proof needed to perform warrantless surveillance from probable cause to a reasonable belief that one of the parties to the communication is situated internationally, even if the communication comes from a person inside the United States.⁵⁸

The major change to FISA by the PAA allowed the Director of National Intelligence and the Attorney General to authorize foreign-intelligence gathering for up to one year on those targets “reasonably believed” to be outside of the United States without FISC approval if two conditions are met.⁵⁹ First, based on the information in front of them, the

53. *Id.* A pen register gathers phone numbers from outgoing calls placed on a specific line whereas the trap-and-trace device gathers the incoming phone numbers on the line. *Id.*

54. Cora Currier et al., *Mass Surveillance in America: A Timeline of Loosening Laws and Practices*, PROPUBLICA (June 7, 2013), <https://projects.propublica.org/graphics/surveillance-timeline>.

55. *What Is the Protect America Act?*, DEP’T JUST., <http://www.justice.gov/archive/ll/> (last visited Sept. 5, 2015).

56. *Id.*

57. Protect America Act of 2007, Pub. L. No. 110-55, § 105A, 121 Stat. 552 (repealed 2008).

58. Stephen Ross Johnson & Anne Passino, *The Protect America Act: Who Will Protect Us Against the Protectors?*, RITCHIE, DILLARD, & DAVIES, P.C. 1–2, <http://rddjlaw.com/articles/ProtectAmericaAct.pdf> (last visited Sept. 5, 2015).

59. Protect America Act of 2007 § 105B. The Act did, however, allow for some oversight by the FISC within 120 days after issuance of the warrant to determine whether the monitoring constituted electronic surveillance. *Id.* § 105C (“No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court . . . the procedures by which the Government determines that acquisitions conducted pursuant to

Director and Attorney General must determine that there are reasonable procedures in place for determining that the persons to be surveilled are located outside of the United States.⁶⁰ Second, a “significant purpose” of the surveillance must be to obtain foreign-intelligence information, and adequate minimization procedures that meet the statutory directive must be in place.⁶¹

3. *FISA Amendments Act of 2008*

On July 10, 2008, FISA was once again amended, this time by the FISA Amendments Act of 2008.⁶² One of the main provisions of the 2008 Act allows the FISC to approve surveillance of targets outside the United States without an individualized court order, thus allowing the government to respond quickly in time-sensitive situations.⁶³ These blanket warrants require the FISC to review, only on a yearly basis, certifications that identify categories of foreign-intelligence targets, as submitted by the Attorney General and Director of National Intelligence.⁶⁴

Proponents of the amendment argue that it provided a streamlined, more efficient approval process for establishing surveillance of targets located overseas.⁶⁵ These proponents emphasize that overseas surveillance does not implicate Fourth Amendment concerns,⁶⁶ arguing that the amended FISA has been “extremely valuable” in protecting the country from terrorists and other national security threats.⁶⁷

Critics of the FISA Amendment Acts maintain that the amendment has nearly eviscerated the original FISA system.⁶⁸ The FISC has a limited

section 105B do not constitute electronic surveillance.”). Some commenters suggested that this oversight was not effective because the expanded definition of “electronic surveillance” created a dragnet effect and the Attorney General was not required to explain to the court how the information of American citizens is treated upon interception. Johnson & Passino, *supra* note 58, at 2.

60. Protect America Act of 2007 § 105B.

61. *Id.*

62. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

63. See U.S. DEP’T OF JUSTICE & OFFICE OF DIR. OF NAT’L INTELLIGENCE, BACKGROUND PAPER ON TITLE VII OF FISA, S. REP. NO. 112-229, app. at 30 (2012).

64. *Id.* app. at 31.

65. *FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 24 (2012) (statement of Kenneth L. Wainstein, Partner, Cadwalader, Wickersham & Taft LLP) [hereinafter *FAA Hearing*].

66. *Id.* at 25.

67. *Id.*

68. Mitra Ebadolahi, *Warrantless Wiretapping Under the FISA Amendments Act*, HUM. RTS., Mar. 2013, at 11, 11.

oversight role, since it no longer makes individualized probable-cause determinations and no longer oversees whether the surveillance targets are inappropriately located inside the United States.⁶⁹

Four years after the FISA Amendments Act was passed, Congress extended the Act for five more years.⁷⁰ At the reauthorization hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, Representative Bobby Scott of Virginia described the Act as “result[ing] in massive amounts of information being collected with an untold amount of it affecting Americans in America.”⁷¹ Representative John Conyers, Jr. of Michigan explained that the FISA Amendments Act allows the FISC to issue orders for sweeping, mass-surveillance programs rather than approving individual targets.⁷² Instead of requiring the government to identify specific individuals, the court now merely certifies that procedures are in place to ensure the proposed surveillance targets only foreigners outside of the United States.⁷³

Rather than engaging in a meaningful review of the proposed surveillance, the FISC simply rubberstamps the government’s request if the court sees that general surveillance procedures are in place. Once the court approves the procedures, no further judicial review occurs on the targets that are selected for surveillance.⁷⁴ Some commentators have criticized the process, stating that “the FISC issues a blanket surveillance order whenever the government mouths the correct words—that it is collecting foreign-

69. *Id.*

70. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, § 2, 126 Stat. 1631.

71. *FAA Hearing*, *supra* note 65, at 15 (statement of Rep. Robert C. “Bobby” Scott, Member, H. Subcomm. on Crime, Terrorism, & Homeland Sec.).

72. *Id.* at 16 (statement of Rep. John Conyers, Jr., Member, H. Comm. on the Judiciary). Representative Conyers stated:

Although the foreign intelligence surveillance court has some measure of oversight over these programs, the sweeping and general nature of this authority has given many cause for concern.

For example, the government may describe its operations to the court in exceptionally general terms—as broad as “all phone calls, emails, and text messages originating in Pakistan”—and conduct wide-ranging, dragnet surveillance from there. Although the law requires the government to use “minimization procedures” that limit the impact of these programs on American citizens, there is no question that the government can and does intercept and listen in on the communications of U.S. persons.

Id.

73. Fiss, *supra* note 16, at 17–18 (citing 50 U.S.C. §§ 1881a(a)–(g) (2012)).

74. Greenwald, *supra* note 39.

intelligence information relevant to a non-U.S. target. The FISC provides very little independent oversight of the surveillance itself.”⁷⁵

II. IMMEDIATE NEED FOR REFORM

A. Recent Revelations

Until June 9, 2013, the majority of Americans were ignorant about the true breadth of the United States’s intelligence-gathering and domestic surveillance programs. On that day, *The Guardian* released classified documents obtained by an NSA subcontractor, Edward Snowden, who worked for the defense contractor Booz Allen Hamilton.⁷⁶ Snowden, a self-described whistleblower, implicated the NSA in a vast surveillance program that routinely gathered the communications of millions of American citizens.⁷⁷ By publishing a top secret PATRIOT Act order handed down from the FISC in April 2013,⁷⁸ Snowden’s leak set off an enormous backlash against the NSA and the FISC regarding the manner in which foreign intelligence is being gathered.

The court order from April 25, 2013, demanded that Verizon Wireless turn over all of its information on telephone calls on an “ongoing, daily basis,”⁷⁹ giving the government unlimited authority to obtain information on millions, perhaps billions, of telephone calls for a three-month period.⁸⁰ Authored by Judge Vinson, the order specifically requires Verizon to turn over all call detail records, also known as telephony metadata, of calls between the United States and other countries or those that take place wholly within the United States.⁸¹ Although telephony metadata does not include the collection of the contents of the conversation, all other call details are given to the NSA, such as the numbers of both parties, call duration, and location information.⁸² While the metadata seemingly gives off only innocuous information, the NSA can use the data to form a

75. Granick & Sprigman, *supra* note 31.

76. Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, *GUARDIAN* (June 9, 2013, 9:00 AM), <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

77. *Id.*

78. Andy Greenberg, *Intelligence Officials Admit That Edward Snowden’s NSA Leaks Call For Reforms*, *FORBES* (Sept. 13, 2013, 3:37 PM), <http://www.forbes.com/sites/andygreenberg/2013/09/13/intelligence-officials-admit-that-edward-snowdens-leaks-call-for-reforms/>.

79. Greenwald, *supra* note 1.

80. *Id.*

81. *Id.*

82. *Id.*

comprehensive picture of an individual's personal relationships and other intimate details about the individual's life.⁸³

Judge Vinson's order is an example of a blanket warrant, which allows the FISC to sign off on the collection of vast amounts of domestic communications. Two district court judges recently ruled on the constitutionality of the blanket warrants and came to opposite conclusions on whether to enjoin the bulk collection of metadata by the NSA.

In *Klayman v. Obama*,⁸⁴ Judge Richard Leon of the United States District Court for the District of Columbia enjoined the NSA after explaining his concern with the Agency engaging in systematic noncompliance with the FISC-ordered minimization procedures.⁸⁵ The method by which the NSA searches its massive database, a three-degrees-of-separation type search from the main search term, rakes in much information that Judge Leon describes as having a "spiderweb-like reach."⁸⁶

Less than two weeks after Judge Leon's ruling in *Klayman*, Judge William Pauley of the United States District Court for the Southern District of New York found that the bulk collection of metadata was not unconstitutional, arguing that "[t]his blunt tool only works because it collects everything."⁸⁷

The main point of disagreement between Judge Leon and Judge Pauley comes from a 1979 United States Supreme Court case, *Smith v. Maryland*.⁸⁸ In *Smith*, the police were monitoring a pen register, a device installed by the telephone company that recorded the numbers dialed from Smith's home.⁸⁹ The Supreme Court held that individuals have no legitimate expectation of privacy in dialed telephone numbers because they turn that information over to a third party, the phone company.⁹⁰

Judge Pauley relied on *Smith v. Maryland* to rule against unconstitutionality,⁹¹ whereas Judge Leon refused to extend the logic of *Smith* to the case before him.⁹² Judge Leon believed that the issue in *Smith* was not comparable because the bulk collection of telephone metadata at issue in *Klayman* was markedly different from a simple pen register, and

83. Granick & Sprigman, *supra* note 31.

84. *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013).

85. *Id.* at 39 n.62, 43.

86. *Id.* at 17 n.21.

87. *ACLU v. Clapper*, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013).

88. *Smith v. Maryland*, 442 U.S. 735 (1979).

89. *Id.* at 737.

90. *Id.* at 745–46.

91. *Clapper*, 959 F. Supp. 2d at 749–52.

92. *Klayman v. Obama*, 957 F. Supp. 2d 1, 31–32 (D.D.C. 2013).

the same rules could not be used to evaluate the constitutionality of new, more powerful technology.⁹³ The conflict increases the odds that the Supreme Court will soon weigh in on the constitutionality of the blanket warrants.⁹⁴

Much like the FISA courts, until recently, the NSA was an executive agency that operated almost exclusively behind closed doors and hid many secrets from public view. Operating with little to no oversight over the data-collection process, in 2010, the NSA intercepted 1.7 billion e-mails and phone calls per day.⁹⁵ By March 2013, the Agency had amassed an estimated three billion pieces of intelligence from United States communications networks.⁹⁶ Using these dragnet tactics, it is inevitable that the Agency is collecting and storing a plethora of information on millions of innocent Americans.

Through an FISC-approved program called PRISM, the NSA has been able to send task instructions to the servers of Internet companies and social media networks, such as Apple, Yahoo!, Skype, and Google, to obtain chats, e-mails, photographs, and other documents.⁹⁷ The NSA assures United States citizens that it is capable of extracting all of the information obtained through PRISM, but because of current regulations, it does not attempt to.⁹⁸ The Agency is capable, however, of retaining all records from telecommunications companies for up to five years.⁹⁹ Analysts access the mass amount of data and enter search terms to make sure that, with 51% confidence, the content they are reading is produced by a foreign target.¹⁰⁰ However, a confidence level this low is unconvincing.

The NSA's overreaching does not stop with the United States. The Agency has been known to monitor foreign entities that pose no immediate threat to national security, including foreign officials and other well-known

93. *Id.* at 32.

94. Adam Liptak & Michael S. Schmidt, *Judge Upholds N.S.A.'s Bulk Collection of Data on Calls*, N.Y. TIMES (Dec. 27, 2013), http://www.nytimes.com/2013/12/28/us/nsa-phone-surveillance-is-lawful-federal-judge-rules.html?_r=0.

95. Greenwald, *supra* note 39.

96. *Id.*

97. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

98. *Id.*

99. *Klayman v. Obama*, 957 F. Supp. 2d 1, 30 (D.D.C. 2013).

100. Gellman & Poitras, *supra* note 97.

public figures.¹⁰¹ After German Chancellor Angela Merkel discovered that the NSA was monitoring her personal cell phone, she reportedly had some choice words for President Obama, telling him that the surveillance tactics were reminiscent of the Stasi, the powerful secret police of Communist East Germany.¹⁰² Merkel also voiced concern about the NSA's inability to keep classified information secret, considering how easy it was for Snowden to obtain secrets and release them to the world.¹⁰³

In another recent snafu, the NSA reportedly spied on Pope Francis during the Vatican conclave by intercepting data on telephone calls.¹⁰⁴ The information obtained was divided into four categories—leadership intentions, threats to financial system, foreign policy objectives, and human rights—all of which are a far cry from foreign-intelligence gathering in the interest of national security.¹⁰⁵

If the surveillance state is not quickly reined in, the United States will cease to be the beacon of freedom in the international community and will lose the trust of other foreign nations. Blowback from other countries may result in intelligence agencies becoming adversarial and more reticent to share information with the United States.¹⁰⁶ Foreign leaders have recently castigated the United States, with Germany threatening to delay United States–European Union trade discussions, and the President of Brazil cancelling a visit to the White House in protest.¹⁰⁷ In an address at the Opening Debate of the United Nations General Assembly, the President of Brazil condemned the NSA surveillance program and its intrusion into foreign countries, stating that “[a] sovereign nation can never establish

101. James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, *GUARDIAN* (Oct. 25, 2013, 2:50 AM), <http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>.

102. Ian Traynor & Paul Lewis, *Merkel Compared NSA to Stasi in Heated Encounter with Obama*, *GUARDIAN* (Dec. 17, 2013, 1:23 PM), <http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama>.

103. *Id.*

104. Nick Squires, *US 'Spied on Future Pope Francis During Vatican Conclave'*, *TELEGRAPH* (Oct. 30, 2013, 6:35 PM), <http://www.telegraph.co.uk/news/worldnews/europe/italy/10415228/US-spied-on-future-Pope-Francis-during-Vatican-conclave.html>.

105. *Id.*

106. Michael Young, *Backlash Inevitable as No One Likes Being Spied Upon*, *NATIONAL* (July 11, 2013), <http://www.thenational.ae/thenationalconversation/comment/backlash-inevitable-as-no-one-likes-being-spied-upon>.

107. See Karen Kornbluh, *Could the Revelations Regarding the NSA PRISM Program Hinder U.S. Relations Around the World?*, *COUNCIL FOREIGN REL.* (Oct. 7, 2013), <http://www.cfr.org/defense-and-security/could-revelations-regarding-nsa-prism-program-hinder-us-relations-around-world/p31566> (responding to a question submitted by Andre Ribeiro from LaGuardia Community College).

itself to the detriment of another sovereign nation. The right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country.”¹⁰⁸

B. Problems with the FISC

Originally intended to keep the Executive Branch in check and to ensure that American citizens were not spied on without some suspicion of wrongdoing, the FISC has now morphed into a rubber stamp for the government’s fishing expeditions. The post-9/11 amendments to FISA have played a large part in significantly weakening the oversight role of the FISC.

After the FISA Amendments Act, the court need not evaluate probable cause or require individualized suspicion of the proposed target.¹⁰⁹ The government is never required to identify its targets to the court, or to anyone else for that matter.¹¹⁰ Recently, the chief judge of the FISC, Reggie Walton, admitted that the court’s limited resources do not provide the ability to determine whether surveillance operations violate the court’s orders.¹¹¹ The court must rely on the information provided by the government in deciding to grant the surveillance request.¹¹² After the court grants the request, it cannot investigate noncompliance with the orders.¹¹³ Considering the numerous accounts of the NSA’s over-collection of information, the expansion of the original FISA should have come with more oversight by the FISC, not less.

Again, making matters worse is the fact that the FISC operates under extreme secrecy.¹¹⁴ Its opinions never see the light of day, with a few very rare exceptions, and all hearings are closed to the public.¹¹⁵ A real and urgent need exists to keep national security secrets classified that may be contained in these opinions. Alternatively, allowing the FISC to operate as a largely autonomous entity creates dangerous precedent for future

108. H. E. Dilma Rousseff, President of the Federative Republic of Brazil, Statement at the Opening of the General Debate of the 68th Session of the U.N. G.A. at 1 (Sept. 24, 2013), http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

109. Ebadolahi, *supra* note 68.

110. *Id.*

111. Leonnig, *supra* note 8.

112. *Id.*

113. *Id.*

114. 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?pagewanted=1&_r=0.

115. *Id.*

intelligence-gathering operations.¹¹⁶ Seemingly, the court effectuates the FISA by relying solely on the government's position in each individual case it hears.

Even more disconcerting is the fact that the FISC does not operate in an adversarial manner like a normal Article III court where both parties brief a case and the court hears oral arguments from both sides.¹¹⁷ The process is *ex parte*, meaning the government files the application for surveillance, the court receives only the government's briefing, and the government is the only party to appear before the court for an oral argument.¹¹⁸ Critics aptly point out "in a fight where only one side is allowed to show up, the government's view almost always prevails."¹¹⁹

This environment is not likely to produce reliable legal decisions, as the judges do not have the benefit of hearing countervailing arguments or a full factual record upon which to base an informed determination.¹²⁰ "Judges can't be expected to be both neutral arbiters of the law and advocates for the defense," just as the government cannot be expected to present facts that do not support its interpretations.¹²¹

Ex parte procedures are common in criminal law where law-enforcement officers are granted warrants without a formal adversarial hearing; however, the criminally accused have the option of filing motions to suppress evidence uncovered pursuant to the issued warrant.¹²² On the other hand, in the national security context, the goal of surveillance is to covertly monitor targets. Naturally, allowing the validity of the application for surveillance to be litigated would defeat the purpose.¹²³

A process cloaked in such secrecy and capable of having a high degree of error should, at the very least, have adequate safeguards to ensure the court's decision is based on a complete factual record.

116. *Id.*

117. Granick & Sprigman, *supra* note 31.

118. *Id.*

119. *Id.*

120. Orin Kerr, *A Proposal to Reform FISA Court Decisionmaking*, VOLOKH CONSPIRACY (July 8, 2013, 1:12 AM), <http://www.volokh.com/2013/07/08/a-proposal-to-reform-fisa-court-decisionmaking/>.

121. *Ideas for Reforming the FISA Court*, WASH. POST (July 23, 2013), http://www.washingtonpost.com/opinions/ideas-for-reforming-the-fisa-court/2013/07/23/9a3f35e4-f31b-11e2-bdae-0d1f78989e8a_story.html.

122. *Id.*

123. *Id.*

III. REFORM PROPOSALS

Recent reform proposals generally fall into four categories. The first involves allowing outside third parties to act as opposing parties or advocates in FISC proceedings, such as conducting adversarial hearings and allowing amici curiae and special advocates before the court. The second proposal involves increasing transparency in court documents and proceedings by declassifying opinions. The third proposal calls for Congress to maintain more oversight over intelligence agencies. The fourth and final major proposal involves ending the FISC and replacing it with a more effective solution.

A. *Allowing Testimony or Guidance from Third Parties*1. *Adversarial Hearings*

The first of the primary proposals for improving the FISC and restoring confidence in its decisions is to appoint attorneys to oppose the government's surveillance requests.¹²⁴ This idea originated two decades ago when a lawyer in the Carter Administration who helped set up the FISC argued before Congress that the court should have an option to ask for a briefing by outside counsel when the judge wanted to hear an opposing viewpoint in a particular case.¹²⁵ The proposed system would ideally involve appointing independent attorneys to individual cases, and giving those attorneys security clearance on a limited basis.¹²⁶ When the government is the only party present and it has the benefit of national security expertise, the FISC must have a skeptical opposing party to challenge the government's legal arguments.¹²⁷

Critics of this proposal claim that the appointed attorneys will essentially have no clients to guide the litigation.¹²⁸ Without a client, many of these attorneys run the risk of being ideologues who are more concerned with changing policy and voicing their own views than with advocating for

124. Stewart Baker, *Critiquing FISA Reforms*, VOLOKH CONSPIRACY (Aug. 1, 2013, 5:54 AM), <http://www.volokh.com/2013/08/01/critiquing-fisa-reforms/> (referring to the author's own testimony on FISA reform before the Senate Judiciary in 2013).

125. *Ideas for Reforming the FISA Court*, *supra* note 121.

126. Baker, *supra* note 124 (noting that appointing lawyers to counter government-surveillance requests is impractical because it would take too long to clear entire law offices that work on these individual cases, and that lawyers would struggle in deciding which policy arguments to make without clients to guide the decision-making process).

127. Note, *supra* note 13, at 2207.

128. Baker, *supra* note 124.

an unknown client.¹²⁹ Considering the time-sensitive nature of the information that could be obtained from surveillance of a target, this proposal may be too time-consuming, as the opposing party would have to have sufficient time to review, investigate the government's claim, and develop a defense.¹³⁰ In the interim, a terrorist plot or other national security disaster could be unfolding.

Another viable criticism is that there are already numerous individuals in the FISC hearing process to serve as checks on the government's position, such as law clerks, inspectors general, and intelligence community staffers.¹³¹ The government's attorneys come from the Justice Department, which also serves as a check on the intelligence community and is theoretically compelled to provide all the facts and arguments the court needs to make a decision.¹³²

While this line of thought ideally is sound, it is not likely the reality. The Department of Justice is also an executive agency and, rather than serving as a beacon of truth and justice, likely endures enormous pressure to maintain the status quo in the name of preserving national security.

2. *Amici Curiae*

A second proposal for third-party involvement suggests adoption of amicus curiae to assist the court in determining the privacy and liberty interests implicated by the surveillance application.¹³³ While section 401 of the Freedom Act provides for amicus curiae,¹³⁴ it fails to allow these legal experts to participate in the court's decision-making process in a meaningful way.

Section 401 of the Freedom Act states that the FISC and FISCR "shall appoint an individual . . . to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate."¹³⁵ Despite the use of the word "shall" in section 401, the law allows the court to evade this requirement if it finds that an appointment is

129. *Id.*

130. Note, *supra* note 13, at 2214.

131. Baker, *supra* note 124.

132. *Id.*

133. ANDREW NOLAN & RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43362, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: PROCEDURAL AND OPERATIONAL CHANGES 11 (2014), <http://www.fas.org/sgp/crs/intel/R43362.pdf>.

134. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268, 279 (2015).

135. *Id.* § 401(i)(2)(A), 129 Stat. at 279.

not “appropriate.”¹³⁶ Moreover, the new law leaves to “the opinion of the court” whether “any application for an order or review . . . presents a novel or significant interpretation of the law.”¹³⁷ In other words, if the court decides that a case does not present a novel or significant issue, the amicus curiae have no role in that proceeding.

While the provision for amicus curiae in section 401 of the Freedom Act is a step in the right direction, it is unlikely that the new law will allow amicus curiae to participate in a meaningful way.

3. *Special Advocate*

Finally, absent from the Freedom Act is language in earlier legislation that provided for a “public interest advocate” with “access to all relevant evidence” in matters before the FISC.¹³⁸ A public interest advocate, defined by the earlier legislation, would have had the ability to “petition the court to order the Federal Government to produce documents, materials, or other evidence necessary to perform the duties of the public interest advocate.”¹³⁹ Perhaps most importantly, one report indicates that “[o]nce a Special Advocate ha[d] been invited to participate with respect to an application or other matter, the Special Advocate . . . should have access to all government filings.”¹⁴⁰

Unfortunately, the Freedom Act provides much less-expansive access to necessary information than earlier legislation would have granted to special advocates. Under the Freedom Act, there is a possibility that amicus curiae might not be able to obtain basic court documents, such as preliminary briefing and docket materials. The provision for special advocates in the 2013 legislation would have been a better reform measure for the FISC.

B. *Increased Transparency*

The second major proposal involves increasing transparency in FISC activities. The gist of this proposal is that the FISC may become more wary of surveillance requests and exercise more caution and scrutiny

136. *Id.* The court is required only to issue a “finding” explaining that it has found an appointment unnecessary. *Id.*

137. *Id.*

138. H.R. 3159, 113th Cong. § 2(b)(i)(3)(C) (2013).

139. *Id.*

140. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 186 (2014), <http://fas.org/irp/offdocs/pclob-215.pdf>.

before approval once the spotlight is trained on the court and their practices come to light. One method of bringing some of the court's practices to light is by declassifying more opinions.¹⁴¹ Currently, the court rarely declassifies opinions and when it does, the opinions are heavily edited so the sources of information and the methods the court uses to make determinations are not compromised.¹⁴² All of the facts are highly classified, and therefore it is almost impossible to evaluate how the court applied legal principles to reach its decision.¹⁴³

There is also very little information available about the proceedings in the FISC. The bulk of information available to the public consists of a letter to Patrick Leahy, Chairman of the Commission on the Judiciary in the Senate, from Reggie Walton, a presiding FISC judge.¹⁴⁴ This letter contains a brief, and not very descriptive, account of the process the court employs when considering applications for electronic surveillance under the FISA.¹⁴⁵ A second source of information is the Rules of Procedure for the FISC.¹⁴⁶ Neither of these sources provides an abundance of information regarding what goes on inside the court.

Some argue that national security interests would not be harmed if the FISC were to merely release summaries of its legal conclusions and the underlying reasoning.¹⁴⁷ A more open system would not require disclosure of individual targets, but tactics and an explanation of how the surveillance programs work, at least at a general level, should be disclosed.¹⁴⁸ Rather than releasing declassified documents in a haphazard way, Congress could step in to set up a system that releases information on an ongoing basis.¹⁴⁹

The unspoken hope behind the transparency proposal is that once the public knows what is happening behind closed doors, it will be in a better position to monitor the constitutionality of FISC activities. Once citizens know what the FISC court actually does and how it interprets legal texts,

141. *See Baker, supra* note 124.

142. *Id.*

143. *Id.*

144. Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary 1–2 (July 29, 2013), <https://www.fas.org/irp/news/2013/07/fisc-leahy.pdf>.

145. *See id.* at 1–5.

146. *See* RULES OF PROCEDURE FOR THE FISA CT., <http://www.uscourts.gov/uscourts/rules/FISC2010.pdf>.

147. Kerr, *supra* note 120.

148. Granick & Sprigman, *supra* note 31.

149. *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 10 (2013) (statement of Carrie F. Cordero, Director of National Security Studies & Adjunct Professor of Law, Georgetown University Law Center).

the public may accept its role as a watchdog over the government's surveillance activities. If citizens do not approve of the FISC's operations and tactics, they would be in a better position to pressure their representatives into changing the current structure of FISA and the FISC.

C. *Increased Oversight*

The third reform proposal involves a reform of the intelligence-gathering process. Critics take varied approaches to this proposal, but one common link unites all—the current system does not effectively oversee the activities of the FISC to ensure that it does not overstep constitutional bounds. One line of suggestions focuses on changing the operating structure of the intelligence agencies so that overly broad data collection is less likely to occur.¹⁵⁰

Under the current system, there are offices in the Executive Branch that oversee the NSA and other intelligence agencies to ensure that the agencies are compliant in their intelligence-gathering efforts.¹⁵¹ If the agencies were adequately funded to put in the manpower required to oversee the tremendous job of intelligence-gathering, it is less likely that information incidental to individual targets would be collected.¹⁵² Congress should also use its oversight activities to reduce the complexity of operating procedures within the agencies so that employees at the ground level have a clear grasp on the appropriate rules to follow.¹⁵³ None of these ideas deal with the larger problem of the agencies obtaining the initial authority to conduct large-scale surveillance activities. If the NSA cannot be relied on to follow the FISC court orders initially, it cannot be relied on to internally monitor its collection process in a way that ensures that mass amounts of incidental information are not being collected.

Others propose that Congress amend FISA to enhance the power of the Oversight Section of the Department of Justice's National Security Division.¹⁵⁴ The Oversight Section could fulfill the role of independent outside counsel in FISC proceedings by filing motions to oppose applications and supporting briefs.¹⁵⁵ One major concern with this proposal is that the swift-moving process of FISC approval will become slower due to litigation.¹⁵⁶ More importantly, the Oversight Section cannot be trusted

150. *Id.* at 9.

151. *Id.*

152. *Id.*

153. *Id.*

154. Kerr, *supra* note 120.

155. *Id.*

156. *Id.*

to adequately protect civil liberties because it is not truly independent of the intelligence-gathering process.¹⁵⁷

The most noteworthy idea is to allow Congress to oversee more of the intelligence-gathering process and to minimize the role of the FISC. Making Congress primarily responsible for intelligence-gathering procedures would force public debate and lead to serious thought on how best to balance security with privacy.¹⁵⁸ Citizens would be in a position to demand accountability from their representatives rather than from a secret court that the majority of Americans do not know exists.¹⁵⁹ Congress should frequently hear testimony from intelligence agencies that fully disclose the time, place, target, and the reasons for surveillance.¹⁶⁰ Rather than prematurely approving surveillance requests, the court would engage in an after-the-fact review to determine whether the surveillance was reasonable and compliant with Fourth Amendment requirements.¹⁶¹

D. *Ending the FISC*

The fourth—and likely the most extreme—proposal is to bury the FISC and replace it with a more effective oversight mechanism. As critics have pointed out, it may be high time for the FISC to go, because it was not designed for the purpose of determining the legitimacy of mass surveillance programs.¹⁶² At FISA's inception, when specific persons and facilities were being targeted, the court served a valid oversight role and protected against government encroachment, but today the government collects everyone's communications.¹⁶³ Given the current path and track record of the FISC in approving surveillance requests, there is no chance that the court will serve as a wall between citizens and government overreaching.¹⁶⁴ This extreme step is unwarranted. The FISC has a valid and helpful role to play in curbing government excess in the national security realm, but it cannot realize that potential under the current system.

157. *Id.*

158. Note, *supra* note 13, at 2218.

159. *Id.*

160. *Id.*

161. *Id.* at 2219.

162. Granick & Sprigman, *supra* note 31.

163. *Id.*

164. *Id.*

IV. MOST-ACCEPTABLE REFORM PROPOSALS

Reforming the FISC is not an easy task. There are no obvious answers to the difficult national security matters that are implicated. However, there are three main concerns that every serious FISC reform proposal must address. The primary obstacle in reforming the FISC, and what all critics struggle with in their proposals, is how to effectively balance the need for discretion and secrecy in foreign-intelligence decisions with the competing interest in openness to ensure that Americans' privacy rights are not continuously violated. Additionally, every proposal should provide for a process that moves quickly to address the time constraints inherent in national security concerns. Finally, constitutional constraints on Congress's ability to impose rules and increased oversight over the FISC must also be considered.

Because the current reform proposals and the recently enacted Freedom Act leave gaps, it is necessary to supplement them with other changes. Additional reforms should focus on changing the structure of the court—namely, altering the current structure that the court follows to hear applications, and giving judges and staffers more investigatory powers. To allow for a more open process without compromising national security, the FISC should also publish an established procedure for hearing applications.

A. *Changes in Court Personnel*

Currently, the FISC is composed of eleven district court judges who hear applications and grant electronic surveillance orders.¹⁶⁵ Only one judge sits on the court each week and reviews each application along with a staff attorney's analysis of the application.¹⁶⁶ Applications involving novel or complex issues are occasionally given a lengthier review.¹⁶⁷ Legal staffers on the court frequently communicate with the government, and a hearing is held only when the judge determines that additional information is needed.¹⁶⁸

The rotating judge schedule has been criticized in several ways. First, there may be a lack of continuity in decision making on surveillance applications.¹⁶⁹ Surveillance applications may be decided in a variety of

165. 50 U.S.C. § 1803(a)(1) (2012).

166. Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary, *supra* note 144, at 1–2.

167. *Id.* at 4.

168. *Id.* at 6.

169. Andrew Weissmann, *The Foreign Intelligence Surveillance Court: Is Reform Needed?*, JUST SECURITY (June 12, 2014, 9:45 AM), <http://justsecurity.org/11540/guest->

ways, and FISC precedent may suffer as a result. Second, each FISC judge has less experience in dealing with national security issues and in dealing with problematic surveillance applications.¹⁷⁰ More time spent in total on the court increases each judge's knowledge about the delicate balance between national security and protecting individual rights, thus increasing consistency among opinions.¹⁷¹

A relatively simple series of solutions would put an end to these issues and would provide much-needed reform to the FISC. First, rather than one judge sitting on the court deciding applications each week, multiple judges should grant or deny applications at the same time. At least three judges sitting on the FISC at the same time would help to alleviate the fractured decision-making process that leads to expansive surveillance operations. Multiple judges would also preserve continuity on the court, as each judge would gain more experience.

Normally, the one judge sitting on the court each week operates on a strict time frame for each application due to the fast-paced nature of national security concerns. At any given time, that judge is dealing with multiple applications with quick turnaround times. It is not implausible to believe that the workload placed on one judge may cause some key details in applications to fall through the cracks, resulting in decisions that are made without complete information.

Increasing the number of judges that sit on the court at any given time would reduce the number of applications before any one judge and would ensure a more thorough review of each application. The less time pressure that a judge is under, the more complete and informed the surveillance decision will be.

Secondly, judges should sit on the court for several weeks at a time, rather than for one-week periods. This would provide each judge with more experience in dealing with applications and in determining when an application should be granted. More importantly, this would foster continuity in decision making. If each judge were to serve for a month at a time, this would provide the opportunity to develop precedent that can be built upon and followed by the next judges.

post-foreign-intelligence-surveillance-court-reform-needed/ (explaining that there may be less continuity in FISC decisions than in decisions from other federal courts).

170. *Id.*

171. *See id.* (explaining the view of some that permanent clerks solve the FISC's continuity problems by holding long-term positions with the court).

B. Additional Investigatory Powers

If the court were granted supplementary investigatory powers beyond the face of the warrant, the odds are lower that an application that exceeds the permissible scope of surveillance would pass review. Currently, a member of the FISC staff reviews the application to determine if it meets the statutory framework.¹⁷² Often, a staff attorney will converse with the government to receive additional information about the surveillance application.¹⁷³ Based on the staff attorney's feedback, the FISC judge then decides whether to approve the application with or without a hearing or whether to impose conditions on approval.¹⁷⁴ This entire process is carried out mostly internally. The only party to give the court any information external to the application is the government.

Considering the delicate balance between individual privacy and the need for intelligence collection, the court should have procedures in place that allow it to retrieve information from an outside source other than the party seeking application approval. Allowing court personnel to perform outside information gathering would provide staffers and judges with more information to render a more factually complete judgment. A more-complete picture may make judges wary of granting overreaching applications.

Specifically, court personnel should have the ability to research the government's application. Information that the government gives on targeted individuals and any incidental surveillance that may be swept in on innocent individuals may be tainted by the desire to have the request granted. The eagerness to surveil a suspected terrorist may cause the government representative to fail to accurately disclose key facts to the court. The court should be empowered to do behind-the-scenes research on exactly who the surveillance will target and the amount of surveillance on secondary individuals that will be swept in.

To perform this research, the court should have several staffers with national security experience, possibly former intelligence agency employees, and the appropriate security clearance to view classified documents. The government should then turn over most of the information that they have to the staffers and aid them in going over the material and answering any questions. Ideally, these staffers would have contacts at the

172. Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary, *supra* note 144, at 2.

173. *Id.*

174. *Id.* at 2–3.

CIA or with other intelligence agencies to determine the degree of surveillance that may be appropriate on a particular target.

Rather than taking the government's word at face value, this extracurricular information-gathering would allow the FISC judges to determine if the risk of violating countless innocent individuals' privacy rights is really worth granting the application. If not, the court would then be armed with enough knowledge to determine the level of minimization procedures that are needed.

C. *Releasing a Procedure*

One main criticism of the FISC is its extreme secrecy and the body of secret case law that the court generates.¹⁷⁵ The court should release an established procedure for hearing cases to combat this secrecy. If the public had an inside account of what actually happened in the court once an application is received, they may be more accepting of the secret proceedings that occur. Even if a record of proceedings and key interpretations of certain terms in the opinions cannot be released, releasing the procedure the court adheres to will create more transparency. Current proposals for greater transparency involve releasing more declassified court opinions or summaries of these opinions. Because of the inherent national security risk and the public's likely failure to understand many of these court documents, the court should release an easy to understand account of exactly how all parties involved behave while in a FISC courtroom.

The letter from Judge Walton is the best available account of the procedures that the court follows, but the letter lacks in substance.¹⁷⁶ While Judge Walton does explain that court staffers are usually in communication with the government regarding applications,¹⁷⁷ the letter does not explain the frequency of communications or the typical information that the court has to solicit from the government to make the application more complete. Further, this account fails to go into any detail involving the court procedures when the surveillance application is not immediately granted and the government has to go before a FISC judge. An account of what actually happens inside the FISC courtroom, such as the most common reason the government has to defend the application in a proceeding and common questions that a judge asks in a hearing, would lead to greater transparency in the application process and increased acceptance by the

175. Lichtblau, *supra* note 114.

176. See Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary, *supra* note 144.

177. *Id.* at 2.

public. The FISC Rules of Procedure suffer from the same deficiencies: they fail to provide any detail about the inner workings of the court.

Releasing a detailed account of the procedure that the court utilizes when it receives an application is an effective solution to combat the questions that surround the way the court operates and the alleged *carte blanche* approval of governmental applications. The more information that is released to the public, the greater the appearance of openness. This information release would of course have to be executed with national security concerns in mind. Any procedural information that would jeopardize the surveillance of targets should not be released.

CONCLUSION

Ayn Rand once stated that “[c]ivilization is the progress toward a society of privacy. The savage’s whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.”¹⁷⁸ If this is true, society is moving in the wrong direction when it gives governmental-surveillance programs greater priority than preserving privacy rights. The explosion of new technology and increased speed with which terrorist activities can be carried out do not justify the government’s disregard for the constitutional rights of American citizens.

The court, initially intended to be the bastion of freedom and to guard against government encroachment, has stepped far outside of its watchdog role. Since the passage of FISA, and especially since 9/11, the court has morphed into nothing more than a kangaroo court,¹⁷⁹ existing only to give the illusion of oversight to quiet valid concerns about the government’s overexpansion into the private lives of U.S. citizens. The blame cannot be placed solely on the court and its internal operations. Most of the blame lies with Congress and the vast authority that it has granted the court to make far-reaching, nonreviewable decisions. The current statutory provisions unacceptably allow the court to exercise wide discretion in granting surveillance requests and sweeping blanket warrants. By awarding a large amount of unchecked power to the government, the court virtually invites constitutional violations.

*Allison E. Persinger**

178. AYN RAND, *THE FOUNTAINHEAD* 684–85 (Signet ed., The Bobbs-Merrill Company 1993) (1971).

179. Granick & Sprigman, *supra* note 31.

* J.D. 2015, Campbell University School of Law. The author thanks Professor Sarah Ludington for her feedback and guidance in writing this Comment.