SECURITY PROTOCOL: A PROCEDURAL ANALYSIS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS

KATE POORBAUGH*

This Note examines proposed changes to the Foreign Intelligence Surveillance Court following the NSA leaks by Edward Snowden. Specifically, it analyzes proposed procedural changes to the Foreign Intelligence Surveillance Act that attempt to provide a clear legal standard and effective oversight to ensure that intelligence activity does not undermine the democratic system or civil liberties. This Note argues that a public advocate should be added to FISC proceedings to represent the public's privacy and civil liberty interests and allow FISC final orders granting surveillance to be appealed to the Foreign Intelligence Surveillance Court of Review by a public advocate. In addition, this Note recommends that changes be made to the FISCR so that it may handle a larger caseload and become a more permanent entity with full-time judges.

TABLE OF CONTENTS

* J.D. Candidate, 2015, University of Illinois College of Law. B.S. Accountancy, 2012, University of Illinois Urbana-Champaign. I would like to thank the editors, members, and staff of the *University of Illinois Law Review* for their valuable edits and diligence.

I. INTRODUCTION

Tension between the conflicting demands of security and liberty is not a novel concept, and it has sparked many debates throughout our nation's history.[1] Today, however, the use of powerful new technologies has heightened this concern.[2] During the first six months of 2013, Google received 25,879 legal requests for users' data "from governments around the world," a number that has tripled since 2009.[3] Of these requests, 10,918 came from the U.S. government alone.[4] Other Internet companies, such as Facebook and Microsoft, have reported similar numbers.[5] These statistics reveal the "government's steadily growing appetite for more data from more users" and thus less privacy for individuals.[6]

This issue came to the forefront of U.S. policy makers' concerns in June 2013 when Edward Snowden leaked confidential information shedding light on the true depths of U.S. surveillance and eavesdropping programs.[7] The leaks caused panic among some U.S. citizens, who feared

1. Clayton Northouse, *Providing Security and Protecting Liberty*, *in* PROTECTING WHAT MATTERS: TECHNOLOGY, SECURITY, AND LIBERTY SINCE 9/11, at 8 (Clayton Northouse ed., 2006).

2. *Id.*

3. Michael Liedtke, *One Chart that Reveals Everything Google Can Say About FISA Requests*, HUFFINGTON POST (Jan. 23, 2014, 6:56 PM), http://www.huffingtonpost.com/2013/11/14/google-fisa requests_n_4275584.html.

4. *Id.*

5. Declan McCullagh, *Facebook, Microsoft Release NSA Stats to Reassure Users*, CNET (June 14, 2013, 7:20 PM), http://news.cnet.com/8301-13578_3-57589461-38/facebook-microsoft-release-nsa-stats-to-reassure-users/#!.

6. Liedtke, *supra* note 3 (quoting Leslie Harris, President of the Center for Democracy & Technology).

7. *See* Mark Hosenball, *NSA Chief: Snowden Leaked up to 200,000 Secret Documents*, HUFFINGTON POST (Jan. 23, 2014, 6:56 PM), http://www.huffingtonpost.com/2013/11/14/nsa-snowden-documents_n_4276708.html.

that their privacy had been compromised.[8] These concerns have spurred "the first serious re-examination of government spying" since the 1970s.[9]

Several proposed amendments to the current surveillance regime have been suggested, ranging from terminating the government's ability to store metadata to creating more oversight of the National Security Agency ("NSA").[10] Applying the Church Committee's insight that "the system of checks and balances—created in our Constitution to limit abuse of Governmental power—was seldom applied to the Intelligence Community,"[11] this Note focuses on the proposed procedural changes to the Foreign Intelligence Surveillance Act ("FISA"). Specifically, this Note examines proposed changes to the Foreign Intelligence Surveillance Court ("FISC"), because "clear legal standards and effective oversight are necessary to ensure" that "intelligence activity does not itself undermine the democratic system it is intended to protect."[12]

Procedural changes must be made to FISA in order to adequately protect civil liberties. Part II of this Note provides a history of the surveillance laws in the United States and examines the current application of FISA. Part III analyzes the benefits and concerns of several different proposed FISA amendments. Considering this analysis, Part IV recommends how FISA should be amended to adequately balance civil liberties with national security concerns. This Note proposes two changes be implemented to the FISC. First, this Note suggests that a public advocate be introduced to make FISC proceedings more adversarial, instead of the current *ex parte*, *in camera* review. Second, this Note suggests revising the definition of a "final judgment" under the FISA to create an improved appellate process.

II. BACKGROUND

When exploring proposed amendments to FISA, it is important to consider the history leading to its enactment and the act's original goals. "In the long run, if we are to cope with present and future crises, we must think deeply about how our historical experience bears on a changing world."[13] FISA represents just one of the government's several attempts to balance the long-term struggle between national security and individual liberty that has influenced surveillance law in the United States.[14]

8. McCullagh, *supra* note 5.

9. Bruce Ackerman, *Surveillance and the FISA Court*, L.A. TIMES, Sept. 24, 2013, http://articles.latimes.com/2013/sep/24/opinion/la-oe-ackerman-fisa-reform-20130924.

10. THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 25, 34 (2013) [hereinafter PRESIDENT'S REVIEW GROUP REPORT].

11. *Id.* at 59 (quoting *Church Committee Report* from April 26, 1976) (internal quotation marks omitted).

12. *Id.*

13. Daniel Farber, *Chapter 1: Introduction*, *in* SECURITY V. LIBERTY: CONFLICTS BETWEEN CIVIL LIBERTIES AND NATIONAL SECURITY IN AMERICAN HISTORY 1 (Daniel Farber ed., 2008).

14. Robert A. Dawson, *Foreign Intelligence Surveillance Act: Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1382 (1993).

A. The History of the Electronic Surveillance Law in the United States: Pre-FISA

Before FISA, the electronic surveillance law in the United States provided for vast government scrutiny and little protection of civil liberties. In 1791, the Bill of Rights was ratified to the U.S. Constitution, including the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[15]

In *Olmstead v. United States*, the Supreme Court held that electronic surveillance, in the form of a wiretap, did not infringe on the Fourth Amendment's warrant requirement because a Fourth Amendment "seizure" applied only to physical property and not to conversations.[16]

Despite the holding in *Olmstead*, the Federal Communications Act of 1934, as codified in 47 U.S.C. § 151 et seq., limited electronic surveillance, stating that "no person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person."[17] In 1937, the Supreme Court included the federal government within the act's jurisdiction and held that evidence obtained through wiretapping was inadmissible evidence in court.[18] Nevertheless, the government interpreted the 1934 act narrowly as "only prohibiting interception followed by divulging or publishing the contents outside the federal establishment," and thus did not affect intelligence surveillance for national security purposes.[19]

Additionally, the executive branch was granted broad national security powers. Article II, Section 1 of the Constitution grants the President the fundamental duty to "preserve, protect and defend the Constitution of the United States."[20] Within this duty is the inherent power to "protect our Government against those who would subvert or overthrow it by unlawful means."[21] Beginning with Franklin D. Roosevelt, presidents have exercised this inherent power in order to authorize warrantless electronic surveillance for national security purposes.[22] Thus, early on, electronic surveillance to protect national security had relatively few restrictions.

---

15. U.S. CONST. amend. IV.

16. 277 U.S. 438, 464 (1928).

17. 47 U.S.C. § 605(a) (2012).

18. Nardone v. United States, 302 U.S. 379, 380–85 (1937); *see also* Nardone v. United States, 308 U.S. 338, 341 (1939) (extending the exclusion of evidence to the "fruits" of the illegal surveillance).

19. William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099, 1104 (2007).

20. U.S. CONST. art. II, § 1, cl. 8.

21. United States v. U.S. District Court (*Keith*), 407 U.S. 297, 310 (1972).

22. S. REP. NO. 95-604, at 7 (1978) ("Every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority.").

The first attempts at limiting electronic surveillance began in the 1960s. In *Katz v. United States*, the Supreme Court overruled *Olmstead*, and held that electronic surveillance was a Fourth Amendment "search" and thus a warrant is required to authorize such surveillance.[23] The Court reasoned that "in light of the realities of modern technology, the Fourth Amendment must be understood to protect the individual's and society's 'reasonable expectations of privacy.'"[24] The Court mentioned, however, in a footnote that "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[25] Thus, the Supreme Court specifically left open this exception for warrantless electronic surveillances in a national security context.[26]

The next year, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[27] Title III requires that "[e]ach application for an order authorizing or approving the interception of a wire, oral, or electronic communication . . . be made in writing upon oath or affirmation to a judge of competent jurisdiction . . . ."[28] This generally requires that the government must obtain a warrant to conduct electronic surveillance.[29] Title III contained a proviso, however, making an exception for the President's power to use electronic surveillance for national security purposes:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.[30]

Thus, both *Katz* and Title III left open the possibility of the President conducting warrantless electronic surveillance in the interest of national security.[31]

---

23. 389 U.S. 347, 353–57 (1967) (extending this right against unreasonable searches and seizures through electronic surveillance extend to any location, including a telephone booth).

24. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 64 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

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

26. *See* Funk, *supra* note 19, at 1107 (discussing whether this possibility of a lack of a warrant for national security surveillance extended to criminal law enforcement purposes); Sharon H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1658 (2002) (discussing how Justice White's concurring opinion states that "the Supreme Court should not require the President to obtain a warrant for national security matters where the President had determined the reasonableness of the surveillance").

27. Pub. L. No. 90-351, 82 Stat. 197, 218 (codified as amended at 18 U.S.C. § 2518 (2012)).

28. *Id.* § 2518(1).

29. Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 330 (2005).

30. 18 U.S.C. § 2511(3) (Supp. V 1970), *repealed* by Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 178 (1978).

31. *See* Funk, s*upra* note 19, at 1108 (describing how this proviso and *Katz* create a Legislative and Judicial approval of this practice); Rackow, *supra* note 26, at 1660 ("[I]t is clear that the statute

In the 1970s, the Supreme Court revisited the President's claim to an inherent power to conduct national security surveillance. In *United States v. United States District Court* ("*Keith*"), the Court held that the Fourth Amendment does not permit warrantless wiretaps in cases involving domestic threats to national security.[32] The Court, however, stated "[w]e have not addressed, and express no opinion as to, the issues which may be involved with respect to the activities of foreign powers or their agents."[33] Thus, the scope of the *Keith* holding was limited to domestic surveillance and did not constrain the executive's power to conduct warrantless foreign intelligence surveillance.[34]

Following the *Keith* decision, the lower courts upheld the executive's power to conduct warrantless foreign intelligence surveillance in cases involving surveillance of foreign powers where U.S. citizens were overheard.[35] In a plurality decision, however, the D.C. Circuit in *Zweibon v. Mitchell* indicated that it would not recognize a "foreign security" exemption from the warrant requirement of the Fourth Amendment.[36] Thus, there was some resistance to the executive's inherent power to authorize warrantless foreign intelligence surveillance.

External events later forced Congress to resolve this issue. During this time, there was immense publicity covering the government's abuse of surveillance, including "NSA surveillance of Americans and drug traffickers, U.S. Army military intelligence surveillance of domestic groups, FBI covert operations against alleged subversive groups, CIA opening of domestic mail sent to or received from abroad, and electronic surveillance of political 'enemies.'"[37] The Watergate scandal further strengthened the cry for change when President Nixon abused his executive powers and "used the cloak of national security to justify unlawful surveillance of political dissidents."[38]

Many of these surveillance abuses were uncovered in the early 1970s by the Senate Select Committee to Study Governmental

was not meant to infringe upon the Executive's long-standing surveillance authority over matters concerning foreign intelligence."); *see also* Seamon & Gardner, *supra* note 29, at 330–31 (explaining how the proviso deals with the President's power to respond to both foreign and domestic threats).

32. 407 U.S. 297, 320–21(1972). The *Keith* case involved a domestic organization's plan to bomb a CIA office in Ann Arbor, Michigan. *Id.* at 299–300.

33. *Id.* at 321–22.

34. Rackow, *supra* note 26, at 1662; *see also* Seamon & Gardner, *supra* note 29, at 334 (describing how the *Keith* opinion sets up a framework of three different levels of stringent).

35. Funk, *supra* note 19, at 1110; s*ee* United States v. Troung Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980) ("[T]he executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons."); United States. v. Buck, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement."); United States v. Butenko, 494 F.2d 593, 608 (3d Cir. 1974) (finding a wiretap valid if primary purpose to gather foreign intelligence information); United States v. Brown, 484 F.2d 418, 421–22 (5th Cir. 1973) (upholding warrantless wiretap against foreign targets where conversations of a U.S. citizen were intercepted).

36. Zweibon v. Mitchell, 516 F.2d 594, 651 (D.C. Cir. 1975) (noting in dictum that the court would be unwilling to create a foreign intelligence exception in spite of the reasoning of other courts of appeals).

37. Funk, *supra* note 19, at 1110.

38. Dawson, *supra* note 14, at 1386.

Operations with Respect to Intelligence Activities, known as the Church Committee.[39] The Committee's mandate was to "investigate the full range of governmental intelligence activities and the extent, if any, to which such activities were 'illegal, improper or unethical.'"[40] Through their investigations, the Church Committee uncovered numerous government scandals, "including the overthrow of foreign governments . . . [and] a systemic effort to assassinate at least half a dozen national leaders around the world."[41] Additionally, the Church Committee reported numerous surveillance abuses and found that "domestic activities of the intelligence community at times violated specific statutory prohibitions and infringed the constitutional rights of American citizens."[42]

The Church Committee's findings led Congress to reexamine the President's ability to authorize warrantless electronic surveillance of foreign powers.[43] While protecting individual privacy was an important concern, Congress recognized the need for electronic surveillance to protect national security as well.[44] Thus, Congress was looking for a solution "to establish a 'secure framework by which the Executive Branch could conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.'"[45] In 1978, Congress created a framework to strike a balance between these two competing interests in the foreign intelligence surveillance context when it enacted FISA.[46]

B. Requirements of the Foreign Intelligence Surveillance Act

FISA established a legal regime for foreign intelligence surveillance that involves "strict rules and structured oversight by all three branches of government."[47] FISA provided the government with more leeway when conducting electronic searches of *foreign powers* than in other types of surveillance.[48] Under FISA, foreign powers include, among other groups, the following: foreign nations, groups engaged in international terrorism, and agents of a foreign power.[49] While FISA grants the government broad surveillance ability over foreign powers, it restricts the

39. Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 806–07 (1989) (noting the activities of the Church Committee in investigating intelligence agencies and finding that "warrantless electronic surveillance had been used against United States Citizens who were not readily identifiable as reasonable sources of foreign intelligence information").

40. S. REP. NO. 94-755, at 1 (1975).

41. U.S. NATIONAL SECURITY, INTELLIGENCE AND DEMOCRACY: FROM THE CHURCH COMMITTEE TO THE WAR ON TERROR 15 (Russell A. Miller, ed. 2008).

42. S. REP. NO. 94-755, at 137 (1976).

43. Rackow, *supra* note 26, at 1666.

44. S. REP. NO. 95-604, pt. 1, at 6 (1977).

45. Dawson, *supra* note 14, at 1387–88.

46. ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: OVERVIEW AND MODIFICATIONS 36 (2008).

47. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 65.

48. *Id.*

49. 50 U.S.C. § 1801(a) (2012).

government's ability to conduct "electronic surveillance *inside the United States* to obtain foreign intelligence from 'foreign powers.'"[50]

1. Foreign Intelligence Surveillance Court

FISA also created the FISC.[51] The FISC is composed of eleven federal district court judges publicly designated by the Chief Justice of the United States to serve for up to seven-year terms.[52] Of these eleven judges, at least three are required to reside within twenty miles of the District of Columbia.[53] FISC judges are ineligible for a second term.[54] The FISC has been held to be a proper Article III court because it consists of federal judges who are appointed for life and are simply serving temporary assignments.[55]

The FISC has the "exclusive jurisdiction to hear and grant applications for foreign intelligence surveillance orders."[56] In order for the government to conduct electronic surveillance inside the United States for foreign intelligence purposes, it must first obtain a warrant from the FISC.[57] The application for a warrant must be made by a federal officer, approved by the attorney general, and demonstrate that there is "probable cause" that the target of the electronic surveillance is a "foreign power."[58] Further, the application must include, among other things, the identity of the target of the surveillance if known, the facts that justify the applicant's belief it is a foreign power, a description of the information sought, the means by which the surveillance will be implemented, and the period of time for which the surveillance is required.[59] If a FISC judge denies an application, the judge is required to provide to a written statement containing the reasons for the denial.[60]

Information obtained through electronic surveillance approved under FISA may only be used in a criminal proceeding with the approval of the attorney general.[61] Further, if the government intends to use this evidence in a trial, it must notify the aggrieved person that it intends to disclose the information.[62] The aggrieved party may then move to suppress the evidence obtained from the electronic surveillance on the grounds that "(1) the information was unlawfully acquired; or (2) the surveillance

50. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 65.
51. 50 U.S.C. § 1803.
52. *Id.* § 1803(a)(1), (d).
53. *Id.* § 1803(a)(1).
54. *Id.* § 1803(d).
55. *See* United States v. Cavanagh, 807 F.2d 787, 792 (9th Cir. 1987); United States v. Megahey, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982).
56. David Hardin, Note, *The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 308 (2003) (citing 50 U.S.C. § 1803(a)).
57. 50 U.S.C. § 1805.
58. *Id.* § 1805(a)(1)–(2)(A).
59. *Id.* § 1804(a).
60. *Id.* § 1803(a)(1).
61. *Id.* § 1806(b).
62. *Id.* § 1806(c).

was not made in conformity with an order of authorization or approval."[63]

Applications submitted to the FISC are heard by a single judge and cannot be heard by another FISC judge unless the court is sitting *en banc*.[64] The *en banc* court consists of all eleven FISC judges.[65] After 2008, the FISA Amendments Act permits the FISC to hold *en banc* panels on its own initiative or at the request from the government in any proceeding.[66] An *en banc* panel is convened when a majority of the judges determine that "(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or (ii) the proceeding involves a question of exceptional importance."[67] The court will sit *en banc* for "[a]n initial hearing, as opposed to a rehearing, only if the matter 'is of such immediate and extraordinary importance that initial consideration' is necessary and feasible 'in light of applicable time constraints.'"[68]

Proceedings before the FISC are generally *ex parte*, *in camera*, and nonadversarial.[69] This type of review is required if the attorney general files an affidavit stating that "disclosure or an adversary hearing would harm the national security of the United States."[70] Thus, the FISC typically hears evidence presented solely by the federal government, and the defendants' interests are not represented.[71] In determining whether the surveillance was lawful, the FISC has the option to disclose portions of the application to the aggrieved party but is not required to do so.[72]

Since FISA's enactment, courts have unanimously held that the *ex parte*, *in camera* review of the FISC is constitutional.[73] In *United States v. Falvey,* the defendants argued that because FISA did not allow an adversarial hearing, it violated their constitutional right to counsel, to be present at the proceedings conducted against them, and to a public trial.[74]

63. *Id.* § 1806(e)(1)–(2).

64. *Id.* § 1803(a)(1).

65. *Id.* § 1803(a)(2)(C).

66. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 109, 122 Stat. 2436, 2464–65 (codified at 50 U.S.C. § 1803(a)(2)(A).).

67. 50 U.S.C. § 1803(a)(2).

68. ANDREW NOLAN & RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43362, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: PROCEDURAL AND OPERATIONAL CHANGES 5 (2014) (quoting FISC RULES OF PROCEDURE 46).

69. FISC RULES OF PROCEDURE 17, 30.

70. 50 U.S.C. § 1806(f).

71. *See* Robert Barnes et al., *Government Surveillance Programs Renew Debate About Oversight*, WASH. POST (June 8, 2013), http://www.washingtonpost.com/politics/government-surveillance-programs-renew-debate-about-oversight/2013/06/08/7f5e6dc4-d06d-11e2-8f6b-67f40e176f03_story.html.

72. 50 U.S.C. §1806(f).

73. *See* United States v. Belfield, 692 F.2d 141, 149 (D.C. Cir. 1982) (holding that FISA incorporates nonjudicial safeguards to ensure the legality of the surveillance and no further judicial procedures are necessary to adequately safeguard the defendants' rights); Global Relief Found., Inc. v. O'Neill, 207 F. Supp. 2d 779, 779 (N.D. Ill. 2002); United States v. Ott, 637 F. Supp. 62, 65 (E.D. Cal. 1986) (reasoning that "in the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized"); United States v. Falvey, 540 F. Supp. 1306, 1306 (E.D.N.Y. 1982).

74. *Falvey*, 540 F. Supp. at 1315.

The court held the *ex parte*, *in camera* review process was constitutional and noted that such review was not unique to the foreign intelligence context and has been upheld at a pretrial hearing.[75] Years later, in *Global Relief Foundation, Inc. v. O'Neill*, the defendant argued that the *ex parte*, *in camera* review violated his right to confront witnesses and his due process rights.[76] Here again, the court held the *ex parte* review was constitutional and reasoned that the government demonstrated a compelling state interest in national security which outweighed the defendant's interest in responding to the evidence against him.[77] Additionally, attempts to review FISA records under the Freedom of Information Act have failed because of the necessity of keeping this information secret in the interest of national defense or foreign policy.[78] Thus, "[c]ounsel attempting to gain access to FISA materials face an uphill battle."[79]

2. Foreign Intelligence Surveillance Court of Review

FISA also created the Foreign Intelligence Surveillance Court of Review ("FISCR").[80] The FISCR is composed of three U.S. district court or U.S. court of appeals judges, publicly designated by the Chief Justice to serve seven year terms.[81] The FISCR has the jurisdiction to review any denial of a FISA application.[82] Under FISA only a decision that the surveillance was unlawful is a final order which may be appealed to the FISCR.[83]

Similar to the challenges against the FISC's *ex parte* review, courts have unanimously upheld FISA provisions that only denials of surveillance applications are final orders reviewable by the FISCR.[84] In *United States v. Hamide*, the defendant sought to vacate an order finding that the government's electronic surveillance was lawful.[85] The court, interpreting FISA, held that only rulings *against* the government—those determining that the surveillance was unlawful—were final orders for purposes of appellate review.[86] Because orders granting approval of the

75. *Id.* at 1315–16.

76. *Global Relief Found., Inc.*, 207 F. Supp. 2d at 808.

77. *Id.*

78. Marrera v. U.S. Dept. of Justice, 622 F. Supp. 51, 53 (D.D.C. 1985) (holding that FISA materials came within the first exemption to the Freedom of Information Act, which exempts from disclosure records that are specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to Executive Order).

79. John J. Dvorske, Annotation, *Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1987 (50 U.S.C.A. §§ 1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents*, 190 A.L.R. FED. 385 (2003).

80. 50 U.S.C. § 1803(b) (2012).

81. *Id.* § 1803(d).

82. *Id.* § 1803(e).

83. *Id.* § 1806(h).

84. *See, e.g.*, United States v. Hamide, 914 F.2d 1147 (9th Cir. 1990) (holding that only rulings against the government, determining that the surveillance was unlawful, were final orders for purposes of appellate review).

85. *Id.* at 1148.

86. *Id.* at 1151.

surveillance are interlocutory orders, and not final orders, the FISCR has no jurisdiction to review them and thus dismissed the appeal.[87] Essentially, only the government has the right to appeal FISC decisions denying surveillance applications, and defendants cannot appeal FISC decisions granting surveillance.[88]

In summary, FISA effectively limited the executive's ability to conduct foreign intelligence surveillance inside the United States by subjecting it to judicial oversight.[89] The executive's ability to conduct foreign intelligence surveillance outside the United States remained undisturbed, and no prior judicial approval was required for such activity.[90] Additionally, challenges against FISA have been largely unsuccessful. The courts have consistently held that FISA creates an adequate balance between individual privacy and national security.[91] Finally, the courts have held that FISA meets both the probable cause and particularity requirement of the Fourth Amendment.[92]

C. FISA Amendments

1. USA PATRIOT Act

The first major amendment to FISA came in 2001 when President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the "USA PATRIOT Act") into law.[93] The USA PATRIOT Act was a response to the September 11th attacks.[94] The pur-

87. *Id.* at 1153.

88. *See id.* at 1151; *see also* In re Grand Jury Proceedings of Special April 2002 Grand Jury, 347 F.3d 197, 205 (7th Cir. 2003) ("Congress intended that, when a person affected by a FISA surveillance challenges the FISA Court's order, a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge." (citation omitted)).

89. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 66.

90. *Id.*

91. *See, e.g.*, United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) ("[T]he procedures established in [FISA] are reasonable in relation to legitimate foreign counterintelligence requirements and the protected rights of individuals."); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 307 (D. Conn. 2008) (noting that FISA, as amended by the USA PATRIOT Act, "incorporate[d] numerous safeguards to achieve 'a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information'"); United States v. Falvey, 540 F. Supp. 1306, 1312 (E.D.N.Y. 1982) ("Congress has struck a reasonable balance between the government's need for foreign intelligence information and the rights of its citizens.").

92. *See, e.g.*, United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) (finding that FISA's allowance of a general description of the information sought from the electronic surveillance does not violate the Fourth Amendment's particularity requirement); *Duggan*, 743 F.2d at 74 ("FISA does not violate the probable cause requirement of the Fourth Amendment."); *Abu-Jihaad*, 531 F. Supp. 2d at 308 ("That the Government may now seek, and a FISC may approve, surveillance or physical searches when only 'a significant purpose'—rather than the 'primary purpose'—is collection of foreign intelligence information, does not alter the constitutional calculus."); *Falvey*, 540 F. Supp. at 1313 ("[T]he FISA probable cause standard fully satisfies the Fourth Amendment requirements").

93. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act Of 2001, Pub. L. No. 107–56, 115 Stat. 272 [hereinafter USA PATRIOT Act].

94. Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 963 (2002).

pose of the Act was "[t]o deter and punish terrorist acts in the United States and around the world, [and] to enhance law enforcement investigatory tools."[95]

The USA PATRIOT Act amended several provisions of FISA.[96] First, the USA PATRIOT Act amended FISA's restrictions to allow trap and trace devices to be used against U.S. citizens and lawful permanent aliens.[97] Second, the old FISA rule, allowing the FBI to only apply for an order requiring the disclosure of certain business records in an investigation, was amended to allow for the production of any "tangible things."[98] Third, the USA PATRIOT Act eliminated the need for a new FISA order each time the subject of the surveillance changed locations and allowed for roving surveillance.[99]

One amendment to FISA from the USA PATRIOT Act, in particular, created considerable controversy.[100] The USA PATRIOT Act amended the original FISA's purpose provision and required the government to certify only that "a significant purpose" of proposed surveillance was to obtain foreign intelligence information.[101] Following this amendment, there was heated debate as to what effect, if any, this had on the original FISA restrictions.[102] In *In Re Sealed Case*, the FISCR held that this amendment replaced the "primary purpose" test with a less demanding "significant purpose" test.[103] The FISCR reasoned that it was Congress' intent for the "significant purpose" amendment to "relax[] [the] requirement that the government show that its primary purpose was other than criminal prosecution."[104] There has been some disagreement among the courts as to whether this amendment violates the Fourth Amendment or not.[105] In sum, the USA PATRIOT Act expanded the government's ability to conduct foreign intelligence surveillance within the United States.

95. USA PATRIOT Act, 115 Stat. at 272.
96. Dvorske, *supra* note 79.
97. 50 U.S.C. § 1842(a)(1), (c)(2) (2012); USA PATRIOT Act § 214, 115 Stat. at 286–87.
98. 50 U.S.C. § 1861(a)(1); USA PATRIOT Act § 206, 115 Stat. at 287–88.
99. 50 U.S.C. § 1805(c)(2)(B); USA PATRIOT Act § 206, 115 Stat. at 282.
100. *See* Seamon & Gardner, *supra* note 29.
101. USA PATRIOT Act § 218, 115 Stat. at 291.
102. For a discussion on these debates, see Seamon & Gardner, *supra* note 29.
103. *In re* Sealed Case, 310 F.3d. 717, 746 (FISA Ct. Rev. 2002).
104. *Id.* at 732.
105. *See* United States v. Warsame, 547 F. Supp. 2d 982, 995 (D. Minn. 2008) (discussing how all but one court have upheld the "significant purpose" test as constitutional under the Fourth Amendment); *see also* Mayfield v. United States, 504 F. Supp. 2d 1023, 1038 (D. Or. 2007) (striking down PATRIOT Act amendment because "the primary purpose of the electronic surveillance and physical searching of [Plaintiff]'s home was to gather evidence to prosecute him for crimes").

2. Protect America Act

The second major amendment to FISA was in 2007, when the Protect America Act ("PAA") was passed into law allowing for a more flexible surveillance regime during the war on terror.[106] The PAA was a temporary measure designed to amend FISA "to provide additional procedures for authorizing certain acquisitions of foreign intelligence information."[107] The PAA enabled the government to engage in proactive surveillance without the prior approval requirement under FISA.[108] Specifically, the PAA allowed "the Director of National Intelligence and the Attorney General . . . for periods of up to one year [to] authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States."[109] Thus the role of the FISC was to review the surveillance after it had already been conducted instead of granting approval ahead of time.[110]

3. FISA Amendments Act of 2008

When the PAA expired in 2008,[111] Congress passed the FISA Amendments Act of 2008 ("FAA"), which made the provisions in the PAA more permanent.[112] Under the FAA, "the Attorney General and the Director of National Intelligence may authorize jointly for a period of up to [one] 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."[113] This surveillance may not intentionally target (1) "any person known at the time of acquisition to be located in the United States"; (2) "a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States"; or (3) "a U.S. person reasonably believed to be located outside the United States."[114]

The FAA also added mechanisms for oversight of surveillance by Congress and the FISC.[115] Prior to engaging in surveillance, the government must receive a written certification from the FISC (with the exception of when time does not permit the submission of a certification, such

106. Protect America Act of 2007, Pub. L. No. 110-55, § 105B(a), 121 Stat. 552, 552 (2007) (repealed 2008) (establishing procedures whereby "the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States"); *see also* Anthony M. Shults, *The "Surveil or Kill" Dilemma: Separation of Powers and the FISA Amendments Act's Warrant Requirement for Surveillance of U.S. Citizens Abroad*, 86 N.Y.U. L. REV. 1590, 1602 (2011).

107. Protect America Act of 2007 § 105B(a), 121 Stat. at 552.

108. Shults, *supra* note 106, at 1602.

109. Protect America Act of 2007 § 105B(a), 121 Stat. at 552.

110. Shults, *supra* note 106, at 1602.

111. Protect America Act of 2007 § 6(c), 121 Stat. at 552.

112. Shults, *supra* note 106, at 1603.

113. 50 U.S.C. § 1881a(a) (2012).

114. *Id.* § 1881a(b)(1)–(3).

115. Shults, *supra* note 106, at 1603 (citation omitted).

as in cases of emergency).[116] But, "[u]nlike with Traditional FISA, . . . the FAA authorizes wholesale surveillance, and the government 'does not need to specifically identify surveillance targets' in order to obtain a warrant."[117] The FAA also amends FISA to establish protections from unlawful surveillance of U.S. persons located overseas.[118] The FAA, for the first time, requires the government to obtain a court order based on probable cause for targeting U.S. citizens located outside the United States.[119]

In *Clapper v. Amnesty International USA*, the constitutionality of the FAA was challenged by attorneys and human rights, labor, legal, and media organizations, including Amnesty International and the American Civil Liberties Union ("ACLU").[120] The respondents argued that the FAA violated the First Amendment, the Fourth Amendment, Article III, and the principle of separation of powers.[121] The Court, however, never reached the constitutionality issue, dismissing the case for lack of standing in 2013.[122] Specifically, the Court held that the "respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[123]

4. Patriot Sunsets Extension Act

The next major amendment to FISA was the Patriot Sunsets Extension Act of 2011.[124] The purpose of this act was to extend expiring provisions of the USA PATRIOT Act to June 1, 2015.[125] After much debate, the 112th Congress decided to extend three expiring provisions of the USA PATRIOT Act: Section 206—roving wiretaps, Section 215—business records, and the "lone wolf" provision.[126] By extending these provisions, Congress has represented that these surveillance methods are still necessary—four years after their enactment—to protect national security.[127] Congress will have to determine whether these provisions should be extended when they sunset once again on June 1, 2015.[128]

116. 50 U.S.C. § 1881a(g)(1).
117. Shults, *supra* note 106, at 1603 (citation omitted); *see also* 50 U.S.C. § 1881a(d).
118. Shults, *supra* note 106, at 1603.
119. *Id.* at 1603–04 (citations omitted); *see also* 50 U.S.C. § 1881a(b)(3).
120. 133 S. Ct. 1138 (2013).
121. Michaela Chelsea Dudley & Allison Nolan, *Clapper v. Amnesty International USA (11-1025)*, CORNELL UNIVERSITY LAW SCHOOL (Oct. 29, 2012), http://www.law.cornell.edu/supct/cert/11-1025.
122. *Clapper*, 133 S. Ct. at 1155.
123. *Id.*
124. Patriot Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216.
125. *Id.*
126. For a discussion on each separate provision extended by the Patriot Sunsets Act of 2011, see Daniel E. Lungren, *A Congressional Perspective on the Patriot Act Extenders*, 26 NOTRE DAME J.L. ETHICS & PUB. POL'Y 427 (2012).
127. *Id.* at 456–57.
128. *Id.* at 457.

D. FISA Today

Over the past decade, the FISC has reviewed about 2000 FISA warrant requests for government surveillance per year.[129] The FISC approves approximately ninety-seven percent of these requests on their first submission, and about ninety-nine percent are approved on their second submission after some modifications have been made.[130] Between the court's creation in 1978 and 2012, the FISC has rejected only eleven of over 20,000 FISA applications.[131] This has created controversy over whether the FISC is just "rubber stamping"[132] these requests, or if the court truly is providing a credible oversight to governmental surveillance.[133]

In June 2013, the United States was forced to reexamine its government spying and surveillance laws when Edward Snowden, a former NSA contractor, leaked between 50,000 and 200,000 "top secret" U.S. documents.[134] Snowden's leaks revealed that the U.S. government had engaged in a massive amount of electronic surveillance, including collecting data from phone records and eavesdropping on the phone calls of foreign leaders.[135] Whether one believes Snowden is a traitor or a hero, Snowden's leaks have clearly fueled debates over government surveillance and the balance between national security and information privacy.[136]

Among the most shocking revelation stemming from these leaks is the U.S. government's participation in mass surveillance, which the government justified under Section 215 of the USA PATRIOT Act.[137] For example, a FISC order in April 2013 allowed the NSA to receive "all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within

129. Geoffrey R. Stone, *Reflections on the FISA Court*, HUFFINGTON POST (Sept. 4, 2013, 5:12 AM), http://www.huffingtonpost.com/geoffrey-r-stone/reflections-on-the-fisa-c_b_3552159.html.

130. *Id.*

131. Glenn Greenwald, *The Bad Joke Called 'The FISA Court' Shows How a 'Drone Court' Would Work*, GUARDIAN (May 3, 2013, 11:28 AM), http://www.theguardian.com/commentisfree/2013/may/03/fisa-court-rubber-stamp-drones. For a year by year breakdown of FISA applications, see *Foreign Intelligence Surveillance Act Court Orders 1979-2012*, ELECTRONIC PRIVACY INFO. CENTER (last updated May 1, 2014), http://epic.org/privacy/wiretap/stats/fisa_stats.html.

132. *See, e.g.*, Greenwald, *supra* note 131 (arguing that FISC is similar to a "drone court" just accepting every application); Gabriela Vatu, *NSA Declassified: FISA Court, Truly Just a Rubber Stamp*, SOFTPEDIA (Nov. 19, 2013, 8:43 AM), http://news.softpedia.com/news/NSA-Declassified-FISA-Court-Truly-Just-a-Rubber-Stamp-401460.shtml (arguing that the FISC was aware the NSA was collecting more data than allowed but still approved all requests).

133. *See, e.g.*, Stone, *supra* note 129 (discussing how the FISC is working exactly as intended and defending the approval rates).

134. Hosenball, *supra* note 7.

135. Colleen Curry, *NSA Spying Will Continue Despite Snowden's Leaks, Experts Say*, ABC NEWS (Oct. 30, 2013), http://abcnews.go.com/US/edward-snowdens-leaks-lead-change-intelligence-experts/story?id=20713875.

136. *Id.*

137. Spencer Ackerman, *FISA Judge: Snowden's NSA Disclosures Triggered Important Spying Debate*, GUARDIAN (Sept. 13, 2013, 1:14 PM), http://www.theguardian.com/world/2013/sep/13/edward-snowden-nsa-disclosures-judge.

the United States, including local telephone calls."[138] This "metadata" includes information such as "originating and terminating number," the duration of each call, telephone calling card numbers, trunk identifiers, International Mobile Subscriber Identity ("IMSI") numbers, and "comprehensive communication routing information."[139] Thus, "the communication records of millions of U.S. citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing."[140] This clearly is not aligned with the original intentions of FISA.

Shortly after the Verizon leak came the Prism program leak regarding a program which allows the NSA to gain information directly from the servers of internet companies such as Google, Facebook, and Apple.[141] "The Prism program allows the NSA . . . to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders."[142] It is possible that under the Prism program, communications made entirely within the United States could be collected without warrants.[143] This is because the FAA allows surveillance when there is "reasonable suspicion that one of the parties was outside the country at the time the records were collected by the NSA."[144] These recent developments demonstrate how FISA, which was established to allow limited foreign intelligence gathering, has slowly evolved over time to be used as a means to justify the mass surveillance of domestic communication.[145] This is the very problem that the Church Committee warned of over thirty years ago: "[t]he NSA's capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter."[146]

These controversial programs have caused several congressional leaders and civil liberties groups to question the surveillance regime established under FISA and demand more transparency from FISC decisions.[147] In a suit brought by the Electronic Frontier Foundation, the

138. Secondary Order at 2, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc, No. BR 13-80 (U.S. Foreign Intelligence Surveillance Ct. Apr. 25, 2013), *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order?guni=Article:in%20body%20link.

139. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 PM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

140. *Id.*

141. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to Used Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013, 3:23 PM), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

142. *Id.*

143. *Id.*

144. *Id.*

145. Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, *supra* note 139.

146. *Id.* (quoting Frank Church, the chair of the Church Committee).

147. *See, e.g.*, Barnes et al., *supra* note 71.

Department of Justice released hundreds of pages of government documents relating to the government's use of Section 215 of the USA PATRIOT Act in November 2013.[148] These documents revealed widespread violations by the NSA of FISA rules and a vast overcollection of communications unrelated to foreign intelligence surveillance.[149] On December 16, 2013, the U.S. District Court for the District of Columbia ruled that the NSA's mass collection of U.S. phone records likely violates the Fourth Amendment of the Constitution.[150] The order has been stayed pending the appeal by the Department of Justice.[151] On December 27, 2013, the U.S. District Court for the Southern District of New York held "the NSA's bulk telephony metadata collection program is lawful."[152] The ACLU appealed during the first week of 2014.[153]

Following these diverging district court opinions, the FISC reapproved the NSA's phone metadata collection program.[154] This is nothing new, however, as "15 judges on the U.S. Foreign Intelligence Surveillance Court have approved the NSA's metadata collection program on [thirty-six] separate occasions over the past seven years."[155] The FISC mentioned its position is "'open to modifications' that would improve privacy and civil liberty protections 'while still maintaining operational benefits.'"[156]

III. ANALYSIS

Having more information about the government's surveillance programs than ever before, U.S. policy makers are in a unique position to reexamine the current surveillance procedures. FISA, which was originally adopted to be an adequate compromise between national security and civil liberty interests, has been stretched over time to allow for some of the most obtrusive breaches of individual privacy. Thus, it has become

148. *See* Frederic J. Frommer, *Some Foreign Intelligence Surveillance Court Opinions Being Declassified*, HUFFINGTON POST (Sept. 5, 2013, 12:42 PM), http://www.huffingtonpost.com/2013/09/05/foreign-intelligence-surveillance-court_n_3874254.html; Mark Rumold, *Victory: Government to Release More NSA Documents and FISA Court Opinions in Response to EFF Lawsuit*, ELEC. FRONTIER FOUND. (Nov. 15, 2013), https://www.eff.org/deeplinks/2013/11/victory-government-release-more-nsa-documents-and-fisa-court-opinions-response-eff.

149. *See* Spencer Ackerman, *FISA Court Documents Reveal Extent of NSA Disregard for Privacy Restrictions*, GUARDIAN (Nov. 19, 2013, 1:42 PM), http://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy; Kevin Gosztola, *FISA Court: Vast Majority of Internet Communications Data NSA Collected Was Not Relevant to Counterterrorism*, DISSENTER (Nov. 19, 2013, 12:06 PM), http://dissenter.firedoglake.com/2013/11/19/fisa-court-vast-majority-of-internet-communications-data-nsa-collected-was-not-relevant-to-counterterrorism/.

150. Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013).

151. *Id.* at 10.

152. ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

153. Lisa Vaas, *Secretive US Spy Court Once Again OKs NSA Phone Record Collection*, NAKED SEC. (Jan. 7, 2014), http://nakedsecurity.sophos.com/2014/01/07/secretive-us-spy-court-once-again-oks-nsa-phone-record-collection/.

154. *FISC Reapproves the NSA Surveillance Program*, JDJOURNAL, http://www.jdjournal.com/2014/01/05/fisc-reapproves-the-nsa-surveillance-program/ (last visited Feb. 13, 2015).

155. *Id.*

156. Vaas, *supra* note 153.

clear that the current procedures are inadequate to protect civil liberty interests.

A. Balancing Civil Liberties with National Security Concerns

Before delving into all of the ways that FISA could be improved, it is important to consider the inherent struggle between civil liberties and national security concerns. "National security" involves protecting the nation from a perceived violent threat against the stability of the government, the safety of its citizens, or the government's success in armed conflicts.[157] The government is tasked with the fundamental responsibility of preventing these attacks. "The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future."[158] Rapid changes in technology, increased globalization of trade, and advancements in communications technology have resulted in more fluid attacks on national security, against which we expect our government to provide protection.[159]

On the other hand, the United States is also dedicated to protecting privacy and civil liberties, a concept that is an essential part of democracy.[160] "Civil liberties" includes freedom of expression, due process, and restrictions on government intrusion, among other issues.[161] "Protection of civil liberties and civil rights is perhaps the most fundamental political value in American society."[162] Thus, when addressing threats to national security, it is imperative that public officials also consider the risks their actions impose on privacy and civil liberty.[163]

While it is always challenging to strike the appropriate balance between national security and civil liberty, this task becomes even more complicated in times of crisis and public panic.[164] In over two hundred years since the Constitution's ratification, civil liberties have repeatedly been compromised during periods of national turmoil.[165] "Too often, we have overreacted in periods of national crisis and then later, with the benefit of hindsight, recognized our failures, reevaluated our judgments, and attempted to correct our policies going forward. We must learn the lessons of history."[166]

In sum, FISA was enacted to strike a balance between national security and civil liberty. Specifically, the FISC was created to provide a process of independent oversight to prevent improper invasions of indi-

157. Farber, *supra* note 13.
158. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 14.
159. *Id.* at 10.
160. *Id.* at 14.
161. Farber, *supra* note 13, at 1–2.
162. Independence Hall Ass'n, *Civil Liberties and Civil Rights*, AM. GOV'T, http://www.ushistory.org/gov/10.asp (last visited Feb. 13, 2015).
163. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 15.
164. *Id.* at 53.
165. Northouse, *supra* note 1, at 6.
166. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 53.

vidual privacy, while also meeting the unique needs of expediency and secrecy of foreign intelligence investigations.[167] The court's actions in recent years, however, along with Snowden's leaks, are evidence that the court may not be working as well as it had intended in striking the appropriate balance between these two concerns. Thus, some changes must be made to the FISC to recalibrate the balance between national security and civil liberty.

B. Potential Solutions to Amend FISA and Protect Civil Liberties

Increased disclosures of FISC documents revealing widespread abuses of individual privacy have prompted a wave of proposals to amend FISA. As of October 2013, "[t]wenty-two standalone bills have surfaced on Capitol Hill since Snowden's leaks in June [2013]," which range in proposals from procedural changes to complete policy overhauls for the NSA's mass surveillance programs.[168] Additionally, on August 27, 2013, the President created the Review Group on Intelligence and Communications Technologies.[169] On December 12, 2013, this presidential review group released a report including forty-six recommended changes to the current surveillance regime.[170] While many of these proposals furthered in this report and in the various bills have proposed amending the underlying substantive law regulating the surveillance, other proposals address the procedures for authorizing this surveillance.[171]

For purposes of this Note, the focus is on amending the procedures of the FISC, rather than the court's substantive reach. Whether someone's information was taken as part of a mass metadata collection or from an individual surveillance application, that person has suffered the same injury when denied due process of law. Whether or not bulk metadata collection persists, procedural safeguards must be put in place to protect infringements on civil liberty and to help the surveillance regime conform to a truly democratic government.

1. Public Advocate

As mentioned in Part II, proceedings before the FISC are *ex parte*. When there is a hearing before the FISC, only the government's attorneys are allowed to argue in favor of the surveillance, and the current

167. Gregory T. Nojeim, *FISA Court Advocate Helpful, but No Replacement for Ending Mass Surveillance*, YAHOO! NEWS (Nov. 1, 2013, 9:30 AM), http://news.yahoo.com/fisa-court-advocate-helpful-no-replacement-ending-mass-093205942.html.

168. Ali Watkins, *Congress Now is Expected to Revise NSA, FISA Court Operations*, MCCLATCHY DC (Oct. 7, 2013), http://www.mcclatchydc.com/2013/10/07/204557_congress-now-is-expected-to-revise.html?rh=1.

169. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 10.

170. *Id.* at 1.

171. Raffaela Wakeman, *An Overview of FISA Reform Options on Capitol Hill*, LAWFARE (Nov. 3, 2013, 10:08 AM), http://www.lawfareblog.com/2013/11/an-overview-of-fisa-reform-options-on-capitol-hill/.

proceedings do not include a mechanism for the FISC to hear from any representative arguing against the surveillance.[172] This procedure has been the center of much debate since the government's reexamination of surveillance laws. Many proposals have suggested creating an office led by an attorney or a "public advocate" who would argue against the government's foreign surveillance applications and represent the civil liberties and privacy interests of the general public.[173] For example, the President's Review Group on Intelligence and Communications Technologies recommends that "Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court . . . ."[174]

This public advocate role would be a novel component of our legal system.[175] Attorneys, however, have often been employed in similar functions to the role envisioned for the public advocate.[176] For example, the U.S. International Trade Commission employs a staff attorney as a "'Commission Investigative Attorney' . . . whose primary function is to protect the public interest by ensuring that all issues are fully explored" during a trademark investigation.[177] Further, many regulatory and civil state proceedings have "Consumer Advocates" who represent the public interest in utility cases.[178] While some may argue these examples are "far removed from the typical FISA proceedings,"[179] there is precedent in the United Kingdom for specially-appointed attorneys to argue against the government in the national security context.[180] Thus, this idea is not as new as it may seem.

a. Adversarial Process

Supporters of creating a public advocate position argue that the adversarial process is an essential component of our legal system.[181] The adversarial process, and specifically the "'sharp clash of proofs presented' by opposing advocates,"[182] creates "an engine of truth."[183] Judges are in a

172. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 201.

173. ANDREW NOLAN ET AL., CONG. RESEARCH SERV., 7-5700, INTRODUCING A PUBLIC ADVOCATE INTO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT'S COURTS: SELECT LEGAL ISSUES 1 (2013).

174. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 200.

175. Max Helveston, *Promoting Justice Through Public Interest Advocacy in Class Actions*, 60 BUFF. L. REV. 749, 753, 799 (2012) (suggesting a public advocate to represent the public interest in class action litigation).

176. *Id.* at 799.

177. *Id.* (explaining how this attorney develops a complete "factual and legal record" and is allowed to participate in discovery and present witnesses at hearings).

178. *Id.* at 799–800.

179. NOLAN ET AL., *supra* note 173.

180. Alan Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance*, 48 NEW ENG. L. REV. 55, 90 (2013) (discussing how this system has been in place for over a decade).

181. *See* NOLAN ET AL., *supra* note 173; PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 203.

182. NOLAN ET AL., *supra* note 173 (quoting STEPHEN LANDSMAN, THE ADVERSARY SYSTEM: A DESCRIPTION AND DEFENSE 2–3 (1984)).

better position to accurately and confidently decide a case when they have heard competing views on the issue.[184] This idea is represented in our legal system's case or controversy requirement, which requires some type of "concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination of difficult . . . questions . . . ."[185]

There are rare exceptions, however, to the adversarial process in our legal system which one side is allowed to address the court unopposed in *ex parte* proceedings.[186] Opponents of a public advocate solution point to the fact that FISC proceedings are consistent with the federal proceedings for issuing a warrant, which creates the foundation that FISA was originally built upon.[187] Traditional warrant proceedings, however, differ from FISC proceedings in fundamental ways. For example, the officer conducting a traditional warrant search must give a copy of the warrant and a receipt of property taken to the target of the search.[188] Additionally, the target of a warrant has the opportunity to contest the results through a judicial process and may request a return of his property.[189] Conversely, targets of FISA orders are often unaware they are being targeted, have no available avenue of arguing the FISC's determination, and the "property" taken from them—their private communications—remains in the government's hands.[190] Further, much has changed since FISA was enacted. The FISC was initially intended to resolve "routine and individualized questions of fact."[191] As technology and the law evolved, so too did the issues brought before the FISC.[192] Today FISC judges are called upon "to make novel and significant legal determinations regarding important constitutional rights,"[193] such as the legality of the bulk metadata program.[194] When analyzing these complex

183. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 203.

184. NOLAN ET AL., *supra* note 173; PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 203.

185. Baker v. Carr, 369 U.S. 186, 204 (1962).

186. NOLAN ET AL., *supra* note 173, at 2 ("Such *ex parte* proceedings typically exist in the context of pretrial criminal procedure.").

187. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 202–03. *See generally Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess. 29 (1978) (statement of Hon. Edward P. Poland, Chairman, H. Permanent Select Comm. on Intelligence) (exemplifying arguments from the Department of Justice that FISA orders are analogous to warrants and thus constitutional).

188. NOLAN ET AL., *supra* note 173, at 18 (citing FED. R. CRIM. P. 41(f)(C)).

189. *Id.* (citing FED. R. CRIM. P. 41(g); TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 86 (1969).

190. *See* Bruce Schneier, *Let the NSA Keep Hold of the Data*, SLATE (Feb. 14, 2014, 3:03 PM), http://www.slate.com/articles/technology/future_tense/2014/02/nsa_surveillance_metadata_the_government_not_private_companies_should_store.html. *But see* Jason Pye, *Obama to Take Metadata Collection out of NSA Hands*, UNITED LIBERTY (Jan. 17, 2014, 9:01 AM), http://www.unitedliberty.org/articles/16240-obama-to-take-metadata-collection-out-of-nsa-hands.

191. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 203.

192. *Id.*

193. Butler, *supra* note 180.

194. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 203.

and sensitive issues, the FISC would be able to make a better decision if it had heard the arguments of both sides.[195]

Supporters also point to the FISC's overwhelming approval rate of over ninety-nine percent of surveillance requests as an additional reason why a public advocate is needed.[196] They argue that the FISC is unable to properly scrutinize the government's argument for surveillance under the current regime,[197] and that they are just simply "rubber stamping" approvals.[198] These statistics, however, can be misleading because, as FISC Presiding Judge Reggie Walton explained, those numbers do "not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them."[199] Moreover, the FISC has a staff of five full-time legal assistants with foreign intelligence expertise who work with the government's attorneys when an application is brought before the FISC.[200] This process only implies that the government's attorneys are well prepared to make their arguments for surveillance and the court still does not consider arguments against surveillance. Thus, adding a public advocate to FISC proceedings would "ensure that legal developments at FISC do not suffer from unbalanced advocacy."[201]

b. Logistics of a Public Advocate Solution

"The concept of a public advocate is a novel one for the American legal system, and, consequently the proposal raises several difficult questions . . . ."[202] Who shall serve as the public advocate? Where should the advocate be housed? Should it be just one person? How should they be selected? What powers do they have? These questions, along with many more, must first be solved before we can introduce a public advocate into FISC proceedings. During 2013 and 2014, several bills have been introduced that attempt to answer many of these questions.[203]

One of the major contentious issues is where the office of the public advocate should be housed. The President's Review Group on Intelligence and Communications Technologies has proposed two options: (1) house the public advocate on the Civil Liberties and Privacy

195. Butler, *supra* note 180.

196. *See supra* notes 129–33 and accompanying text.

197. NOLAN ET AL., *supra* note 173, at 2.

198. *See supra* note 132.

199. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 202 (citing Letter from Chief Judge Reggie Walton to Honorable Patrick Leahy (July 29, 2013)).

200. *Id.* at 201.

201. Butler, *supra* note 180.

202. NOLAN ET AL., *supra* note 173, at Summary.

203. *See, e.g.*, FISA Court Reform Act of 2013, S. 1467, 113th Cong. (1st Sess. 2013); Privacy Advocate General Act of 2013, H.R. 2849, 113th Cong. (1st Sess. 2013); USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013).

Protection Board ("CLPP Board")[204] or (2) outsource the public advocate responsibilities to a group of attorneys in a private law firm or a public interest group.[205] Housing the public advocate on the CLPP Board would allow the advocate to gain experience in the intelligence field and give the advocate other responsibilities to fill his or her time, but could also create serious conflicts of interest from requiring one person to perform these multiple roles.[206] Outsourcing the public advocate duties to a law firm or public interest group solves the conflict of interest problem, but also creates issues of continuity of knowledge, security clearances, and selection of representation.[207]

Another suggestion is to house the public advocate within the executive branch. One option is to house the advocate in an existing agency, such as the Department of Justice.[208] This proposal, however, does nothing to address the conflict of interest concerns observed from the proposal to house the advocate the CLPP Board, and even exacerbates the problem, because the advocate would be arguing against an employee in the same department.[209] Another option is to house the public advocate in a newly created and independent agency of the executive branch.[210] While this proposal addresses the conflict of interest that comes along with performing dual roles, it creates constitutional concerns regarding "intrabranch" litigation because the public advocate office would be arguing against another executive entity, the Department of Justice.[211] This contradicts the principle that an "Article III court does not adjudicate a dispute between a solitary legal entity."[212]

Because of these intrabranch conflicts, other proposals have been made to house the public advocate within the judicial branch as its own independent office.[213] Article III allows the court to adjudicate *inter*-branch disputes.[214] Housing the public advocate in the judicial branch, however, creates separation of powers concerns. Allowing a member of

204. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 21 (suggesting replacing the Privacy and Civil Liberties Oversight Board with a stronger and more independent Civil Liberties and Privacy Protection Board).

205. *Id.* at 204–05.

206. *Id.* at 204.

207. *Id.* at 204–05.

208. NOLAN ET AL., *supra* note 173, at 3 (citing 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/).

209. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 205 n.166.

210. FISA Court Reform Act of 2013, S. 1467, 113th Cong. § 3(a) (1st Sess. 2013) (creating an Office of the Special Advocate in the executive branch as an independent establishment); Privacy Advocate General Act of 2013, H.R. 2849, 113th Cong. § 901(a) (1st Sess. 2013) (creating an Office of the Privacy Advocate General as an independent office in the executive branch).

211. *See* NOLAN ET AL., *supra* note 173, at 24–26 (providing an in-depth analysis of the constitutionality of "intra-branch disputes").

212. *Id.* at 26.

213. USA FREEDOM Act, H.R. 3361, 113th Cong. § 902(a) (1st Sess. 2013) (creating an Office of the Special Advocate within the judicial branch); FISA Court Reform Act of 2013, H.R. 3228, 113th Cong. §3(a) (1st Sess. 2013) (creating an Office of the Constitutional Advocate within the judicial branch).

214. NOLAN ET AL., *supra* note 173, at 26.

the judiciary to litigate on the public's behalf would expand the current role of the judiciary of impartially resolving disputes.[215] It is uncertain how a court would approach this separation of powers issue because there is a lack of precedent.[216]

Lastly, some proposals suggest there is no adequate place to house a public advocate, because the advocate could never be a truly independent adversary representing the public's interests, and thus one should not be created.[217] Instead of a public advocate, some proposals argue that the FISC should have the ability to appoint amicus curiae to brief the court on the civil liberties issues and make the proceedings more adversarial.[218] This suggestion does little to change FISC proceedings, because the FISC already has the aid of its legal assistants and has even accepted briefs from amicus curiae in the past.[219] Further, this proposal does not create the same "strong and consistent adversarial voice" as a public advocate.[220]

Another contentious issue regarding the creation of a public advocate position is how the advocate is chosen. Some proposals suggest the Privacy and Civil Liberties Oversight Board should appoint the advocate,[221] while other proposals suggest the board select a list of five candidates, from which the Chief Justice of the United States[222] or the presiding judge of the FISCR[223] appoints the public advocate. A more creative proposal suggests that the public advocate be appointed "jointly by the Chief Justice of the United States and the most senior associate justice of the Supreme Court appointed by a President that at the time of appointment was a member of a political party other than the political party of the President that appointed the Chief Justice."[224] There is the possibility of the public advocate being an elected, rather than an appointed position as well.

2. En Banc Review

Under FISA, applications submitted to the FISC are heard by a single judge, and cannot be heard by another FISC judge unless the court is sitting *en banc*.[225] The weight of these decisions and the impact they have

215. *Id.* at 26–28 (discussing how introducing a public advocate in the judiciary would violate both tests set out in *Mistretta*).

216. *Id.* at 28.

217. Steven G. Bradbury, *FISA Court 'Works Well as It Is': Opposing View*, USA TODAY (July 18, 2013, 9:33 PM), http://www.usatoday.com/story/opinion/2013/07/18/foreign-intelligence-surveillance-cort--steven-bradbury-editorials-debates/2567025/.

218. FISA Improvements Act of 2013, S. 1631, 113th Cong. §4 (1st Sess. 2013).

219. Butler, *supra* note 180, at 100.

220. *Id.*

221. Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. § 2(a) (1st Sess. 2013).

222. USA FREEDOM Act, H.R. 3361, 113th Cong. § 902(b)(2) (1st Sess. 2013); FISA Court Reform Act of 2013, H.R. 3228, 113th Cong. § 3(b)(2) (1st Sess. 2013).

223. FISA Court Reform Act of 2013, S. 1467, 113th Cong. § 3(a)(2) (1st Sess. 2013).

224. Privacy Advocate General Act of 2013, H.R. 2849, 113th Cong. § 901(b)(1) (1st Sess. 2013).

225. 50 U.S.C. § 1803(a)(1) (2012).

had on the everyday lives of U.S. citizens has prompted the proposal of requiring certain proceedings before the FISC be given mandatory *en banc* review, instead of optional *en banc* review.[226] Specifically, one proposal would have FISC judges sit in three-member panels for each hearing, and if one of the judges dissents, that judge would be given the right to ask all eleven judges to review the case *en banc*.[227]

This proposal raises some constitutional concerns. *En banc* review requires decisions to be made by a majority of FISC judges rather than just one, but has no impact on the court's power to "independently adjudicate a matter to finality."[228] Thus, Congress can constitutionally require the FISC to sit *en banc* because it does not impose on the court's Article III powers.[229] Further Congress has required the use of three judge panels in other circumstances, such as to adjudicate antitrust suits and in suits seeking to enjoin state officers from enforcing allegedly unconstitutional laws.[230]

In addition to aligning with precedent, the use of three judge panels has other benefits as well. Large advancements in communications technology and surveillance abilities have been made since FISA's enactment in 1978. Single judge decisions may have been more applicable in the past when the court was dealing with more limited "low-tech" surveillance and was not deciding issues involving the mass data collection programs of the NSA today.[231] Further, requiring multiple judges to review an application can ensure that more than just one person's view is represented in deciding these sometimes highly sensitive and constitutional issues.[232]

On the other hand, there are some practical limitations of this proposal. Requiring *en banc* or three judge panels places a large burden on the judicial system. Requiring more judges to review an application will burden and slow the process as the judges waste time convincing the others to agree. Panel or *en banc* review is less efficient than having just one judge decide. Further, a full *en banc* review of all eleven judges could be even more unnecessarily burdensome and lead to a very lengthy decision making process, placing even more of a backlog and burden on the courts. The Supreme Court itself only has nine judges to decide the most controversial issues of our nation; it seems unreasonable this specialty court would require more.

226. Ackerman, *supra* note 9.
227. *Id.*
228. NOLAN & THOMPSON II, *supra* note 68, at 21 (citing United States v. Klein, 80 U.S. 128, 146 (1872)).
229. *Id.*
230. *Id.*
231. Ackerman, *supra* note 9.
232. *Id.*

3. FISC Judge Selection

Currently, the judges on the FISC and the FISCR are appointed by the Chief Justice of the United States.[233] Typically, the judges serving on Article III courts are chosen by the President with confirmation by the Senate.[234] This difference is an important one because the judges chosen for the FISC are never questioned by the Senate about their stance on national security and civil liberty.[235] This variance from typical Article III courts has spurred a debate over whether the judge selection process under FISA should be amended.

Further, this debate has been fueled by the current makeup of the FISC. As of 2013, ten of the eleven judges on the FISC were initially appointed to the federal branch by a Republican president.[236] Moreover, every Chief Justice since FISA's enactment was also appointed by a Republican president.[237] While one would generally expect rulings to differ between Republican and Democratic judges, there is a distinct variance when it comes to civil liberties cases. "[A]mong Supreme Court justices appointed in the last 30 years, those appointed by Republican presidents support civil liberties claims roughly 34 percent of the time, whereas those appointed by Democratic presidents support such claims approximately 74 percent of the time."[238] Thus, one can expect the current FISC is "dramatically" more likely to approve surveillance requests than a court with more Democratic influence.[239] In perhaps an effort to reconcile this difference and to spur some of the criticism, in early 2014 Chief Justice Roberts appointed two judges who were initially appointed to the federal branch by Democratic presidents to serve on the FISC.[240]

In response to these concerns, several proposals for amending FISA judicial appointments have surfaced. One popular proposal is to adopt the procedure applied by other Article III courts, using presidential appointment and Senate conferral.[241] This proposal would provide more consistency across our judicial system and ensure that it is more than just one man's whim deciding who sits on one of the most secretive courts in the United States. Further, this would give the people more of a voice in who is deciding these issues that have a direct impact on their everyday lives.[242] It is unclear, however, how much of a difference, if any, this

233. 50 U.S.C. § 1803(a)(1) (2012).

234. U.S. CONST. art. II, § 2, cl. 2.

235. Editorial, *Privacy and the FISA Court*, L.A. TIMES, July 10, 2013, http://articles.latimes.com/2013/jul/10/opinion/la-ed-fisa-court-20130710.

236. Stone, *supra* note 129.

237. *Id.*

238. *Id.*

239. *Id.*

240. David Ingram, *John Roberts Adds Two Judges With Democratic Ties to FISA Court*, HUFFINGTON POST (Feb. 7, 2014), http://www.huffingtonpost.com/2014/02/07/john-roberts-fisa-court_n_4745888.html.

241. *Privacy and the FISA Court*, *supra* note 235.

242. Editorial, *More Independence for the FISA Court*, N.Y. TIMES, July 28, 2013, http://www.nytimes.com/2013/07/29/opinion/more-independence-for-the-fisa-court.html?_r=4&.

would make. FISC judges are federal district judges who receive life tenure and a salary that cannot be diminished, which acts to insulate them from political pressures.[243]

Another solution, proposed by Senator Richard Blumenthal, among others, is to have the chief judge from each of the twelve federal courts of appeal elect one member of the FISA court.[244] A third solution, suggested by the President's Review Group on Intelligence and Communications Technologies, is to give each member of the Supreme Court the authority to select one or two members of the FISC from within the circuit(s) that particular judge has jurisdiction.[245] These solutions have many of the same benefits of the first proposal, such as preventing one man from having too much power, making the court more accountable to the public, and minimizing the risk of politicizing the process.[246] Another proposal suggests review of appointees by a board composed of members of Congress with national security and civil liberties expertise.[247]

While these proposals may sound good in theory, it is unclear what effect this would have on the rulings of the FISC and it would greatly complicate the judicial selection and approval process. Who would be included on the board? How many members should it be? Which members of the Supreme Court get to appoint two instead of just one FISC judge? These proposals inevitably raise more issues than they address.

4. Appellate Process

If the FISC denies a surveillance application, the government has the opportunity to appeal that denial to the FISCR.[248] The FISCR may remand the matter back to the FISC to "hear further evidence, to modify its findings or opinions, or to make additional findings consistent with applicable law and the order of this court."[249] If the FISCR determines that the FISC correctly denied the application, then "the court shall immediately provide for the record a written statement of each reason for its decision . . . ."[250] If the application is denied by the FISC, the government has the opportunity to file a writ of certiorari to have the Supreme Court review such decision.[251] Under these current procedures, there is no venue to appeal an approval of a surveillance application.

One way to make this appellate process more democratic is to allow not only the denial, but also the approval of an application to be consid-

243. United States v. Cavanagh, 807 F.2d 787, 791 (1987).
244. *More Independence for the FISA Court*, *supra* note 242.
245. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 208.
246. *More Independence for the FISA Court*, *supra* note 242.
247. *Id.*
248. 50 U.S.C. § 1803(b) (2012).
249. Rules for the United States Foreign Intelligence Surveillance Court of Review (Jan. 22, 1980), *available at* http://www.fas.org/irp/agency/doj/fisa/fiscr-rules.pdf.
250. 50 U.S.C. § 1803(b).
251. *Id.*

ered a "final" appealable order. This proposal would fit more squarely with our concept of justice and be more consistent with the practice of other U.S. courts. In most other federal cases in the United States, either side of the litigation has the ability to appeal the decision.[252] The only other prime example in our judicial system where one party to the litigation is continuously denied the right to appeal is in criminal cases, where the government may not appeal a not guilty verdict.[253] This is clearly a stark contrast from FISC procedures, which grant only the government, and not the defendant (surveillance target), the opportunity to appeal. While both criminal and foreign intelligence proceedings have the same overarching goal of protecting U.S. citizens, the former puts the defendant's rights above that of the state's while the latter grants the state overwhelming power at the expense of the defendant.

This proposal of course goes hand in hand with the proposal to make FISC proceedings more adversarial, because some party needs to represent the surveillance target's interest in order to appeal on his or her behalf. Thus one flaw of this suggestion is that it is contingent upon other amendments being made to FISA as well. Another potential flaw of this proposal is that granting a public advocate the ability to appeal could slow down the ability for a surveillance request to be approved if they constantly have to get approval from both the FISC and then the FISCR as well. Hearing more cases than the few they currently have will also put additional strains on the FISCR's ability to quickly decide cases. Burdening these courts could have negative impacts on national security if the government is denied the ability to collect timely surveillance. This process will create a more careful review of the surveillance application, and thus better protect the civil liberties of U.S. citizens.

A potential solution to address the issue of burdening the courts is to establish a pool of judges to sit on the FISCR, similar to the FISC, or to make the FISCR appointment more permanent. Having more judges at the court's disposal will allow the court to more efficiently hear a larger number of cases. To date, the FISCR has only publicly decided two cases.[254] Other cases that have come before the FISCR have been dismissed as interlocutory orders not subject to the court's review.[255] Thus under the current standards, only a part-time, three-member panel is necessary to handle this extremely small caseload. But if the appeals process is changed and more cases must be heard in front of the FISCR, then changing the current structure of the FISCR could help address this additional burden.

252. *The Appeals Process*, UNITED STATES COURTS, http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/HowCourtsWork/TheAppealsProcess.aspx (last visited Mar. 24, 2015).

253. *Id.*

254. *In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (U.S. Foreign Int. Surv. Ct. Rev. 2008); *In re* Sealed Case No. 02-001, 310 F.3d 717 (U.S. Foreign Int. Surv. Ct. Rev. 2002).

255. *See* United States v. Hamide, 914 F.2d 1147, 1151 (9th Cir. 1990) (indicating only rulings against the government are final orders for the purposes of appellate review).

Further, judges currently appointed to the FISC and the FISCR often maintain their current positions as judges in their home districts, and only devote part of their time to their FISC/FISCR responsibilities.[256] For example, Justice William Curtis Bryson is serving on the U.S. Court of Appeals for the Federal Circuit as well as serving as the presiding judge of the FISCR.[257] This practice of dual positions is not going away, as both of the newly appointed FISC judges are keeping their prior placements while serving on the FISC.[258] This is shocking considering the thousands of surveillance requests received by the FISC.[259] It is difficult to imagine how a judge can adequately split his or her time between these two very important positions. This inevitably makes it more difficult for these judges to adequately protect our civil liberties and national security.[260]

IV. RECOMMENDATION

A. Public Advocate

I recommend that a public advocate be added to FISC proceedings to represent the public's privacy and civil liberty interests, a proposal that is supported by President Obama as well.[261] The adversarial process is a core tenant of our U.S. legal system.[262] Typically both parties to a dispute have the right to represent their interests in court. When many people suffer the same injury they create a class action lawsuit and have a member of the class represent their interests.[263] When millions suffer the same injury of having their privacy compromised through government surveillance programs, they too should be able to have their interests represented in court. This is much more difficult, however, than simply picking a member of the "class," because the "class" is the entire public, and many of those injured are unaware of their injuries. Thus, a special role must be created to represent the public's civil liberty interests in front of the FISC.

Further, I recommend the public advocate should be housed in a newly created independent agency of the executive branch. While there are concerns of intrabranch litigation, the "'mere assertion' that a legal action 'is an intra-branch dispute, without more,' does not operate to de-

256. David Gewirtz, *For Spy Court Judges, Overseeing America's Surveillance Efforts is a Part-Time Job*, ZDNET (Feb. 10, 2014, 10:47 PM), http://www.zdnet.com/for-spy-court-judges-overseeing-americas-surveillance-efforts-is-a-part-time-job-7000026173/.

257. *William Bryson*, JUDGEPEDIA (last updated Feb. 10, 2014), http://judgepedia.org/William_Bryson.

258. Gewirtz, *supra* note 256.

259. *Id.*

260. *Id.*

261. *See* Fred Kaplan, *Pretty Good Privacy: The Three Ambitious NSA Reforms Endorsed by Obama, and the One He Rejected*, SLATE (Jan. 17, 2014, 4:01 PM), http://www.slate.com/articles/news_and_politics/war_stories/2014/01/obama_s_nsa_reforms_the_president_s_proposals_for_metadata_and_the_fisa.html.

262. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 203; NOLAN ET AL., *supra* note 173, at 1.

263. *See* Helveston, *supra* note 175.

feat federal jurisdiction."[264] The case should be justiciable because there are "real parties in interest" here—the public whose privacy and civil liberties are harmed from the surveillance and the government who seeks to conduct more surveillance to protect national security.[265] This option is preferential to the other proposals. It would be unwise to outsource this position to a private law firm or advocacy group due to the sensitive nature of FISC proceedings and longevity concerns. Further, the public advocate should not be housed in the judicial branch because this violates the principle of separation of powers by "casting the judicial branch into the role of advocate, as opposed to neutral arbiter."[266]

Lastly, I recommend that the public advocate be an elected position. While this recommendation runs contrary to the current leading bills on this issue,[267] I believe there is real merit in this proposal. First, the public should be the one to choose who represents them as the *public* advocate in the FISC. If the public advocate was elected, he or she would be more accountable to the public, and less likely to be influenced by the other branches of government, or an officer with appointment powers. Some may argue that the public will not be able to distinguish between the candidates, and that a more competent public advocate would be selected if it was an appointed position. The public, however, is the one who is having their privacy and civil liberties jeopardized, so they should be the ones to decide who will represent their interests, much like an injured party in a typical lawsuit has the ability to choose which lawyer will represent his or her interests.

The introduction of a public advocate is especially needed in the FISC because, as *Clapper v. Amnesty International USA* made clear, it is very difficult for plaintiffs to meet the standing requirements in order represent their interests in front of the FISC.[268] Another reason that a public advocate should be an essential component of FISC proceedings is that the fundamental function of the court has developed over time and now the FISC "regularly assesses 'broad constitutional questions' and establishes 'important judicial precedents, with almost no public scrutiny.'"[269] Because of the impact these decisions have on the everyday lives of U.S. citizens, it is essential that FISC proceedings become more adversarial to improve judicial decision making.

264. NOLAN ET AL., *supra* note 173, at 24–25.

265. *Id.* at 25–26.

266. *Id.* at 28.

267. USA FREEDOM Act, H.R. 3361, 113th Cong. § 902(b)(2) (1st Sess. 2013); FISA Court Reform Act of 2013, H.R. 3228, 113th Cong. § 3(b)(2) (1st Sess. 2013); FISA Court Reform Act of 2013, S. 1467, 113th Cong. § 3(a)(2) (1st Sess. 2013); Privacy Advocate General Act of 2013, H.R. 2849, 113th Cong. § 901(b)(1) (1st Sess. 2013).

268. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013); s*ee* Butler, *supra* note 180, at 55 ("If the *Clapper* plaintiffs lacked standing, it could be nearly impossible to find better-suited plaintiffs to challenge the constitutionality of [NSA] . . . surveillance activities and to pursue a litigation solution to intelligence surveillance reform.").

269. *Id.* at 64 (citing Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 7, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all&_r=0).

B. En Banc Review

I recommend that the current process of having one FISC judge hear a case with the option for *en banc* review when necessary should remain untouched. This process allows for efficient decision making, while still allowing for the option to have more judges look at a particular application when it is absolutely necessary. This format is consistent with other courts of first impression, and is thus a format we are familiar with in our judicial system. "[I]t remains anomalous for a court of first impression to review a matter by all the judges on that court."[270] Further, the use of three-member panels outside of federal appellate courts is very unusual as there is no general statutory authority allowing "federal trial judges to reach decisions as a panel."[271]

Additionally *en banc* review is traditionally used "to promote the finality of decisions and to resolve internal circuit splits."[272] The FISC does not encounter the issues of dealing with inconsistent decisions equivalent to a "circuit split." Additionally, if a public advocate were introduced to FISC proceedings as mentioned above, the advocate would aid the judge in his decision making process, and thus there would be less of a need for a multiple-judge panel. Further, if the FISCR is amended in the ways suggested below, the appellate process would be much more accessible and thus should serve as an appropriate avenue to determine the difficult borderline cases that may require more than one judge's viewpoint.

C. FISC Judge Selection

I recommend that the current process of the Chief Judge appointing members of the FISC and the FISCR remain unaltered. The main concern resulting in a cry for change is that currently the FISC is dominated by Republican-appointed judges.[273] This, however, is just by coincidence, and the political mood of the court can change at any time, just as it can for any other court in the United States. There is evidence of this change with the recent Democratic appointments to the court as mention above in Part III. Additionally, political pressures should not impact federal judges as much as critics of FISA would have us believe, because these judges are given life tenure and their salary cannot be diminished under the Constitution.[274] It is unlikely a judge on the FISC will bend to political pressures because his temporary assignment may be revoked.[275] Further, the proposed solutions do nothing to prevent these political pressures, as they are an inherent aspect of our justice system.

270. NOLAN & THOMPSON II, *supra* note 68, at 21.
271. *Id.* at 20.
272. *Id.*
273. Stone, *supra* note 129.
274. United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987).
275. *Id.* at 792.

Under 28 U.S.C. §§ 291—96, the Chief Justice is given the power to designate federal judges to temporary assignments on other courts.[276] The Chief Justice has invoked this power in several instances and appoints lower federal judges to serve on several special courts such as the Court of International Trade, the Temporary Emergency Court of Appeals, and the judicial panel on multidistrict litigation.[277] Thus, the process used by the FISA court is not without precedent. Additionally, "[c]oncentration of the power of appointment in one person can make the process more orderly and organized."[278] Therefore, the current judicial appointment system should remain in place. Any changes would unnecessarily and unjustifiably complicate the system, and would waste resources that could be expended on making more effective changes elsewhere to the statue.

D. Appellate Process

> I recommend that 50 U.S.C. § 1803(b) be amended in part to read: The Chief Justice shall publicly designate three judges, *residing within 20 miles of the District of Columbia*, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial *or approval* of any application made under this Act.

This recommendation essentially makes two changes to current FISA procedures. First, this recommendation changes the court's jurisdiction from hearing only denials of surveillance applications to hearing approvals as well. This recommendation better protects civil liberties in a way that is consistent with the rest of our judicial system. Where defendants in a criminal case are allowed to appeal guilty verdicts, so too should a surveillance target, or someone representing his or her best interests, be allowed to appeal a potentially invasive surveillance request against his or her privacy interests. Thus, each defendant (surveillance target) should have equal treatment under our justice system.

Second, this would require that all three members of the FISCR reside within twenty miles of the District of Columbia. This is similar to the requirement of section (a), requesting that three members of the FISC reside near the District of Columbia.[279] While this does not seem like a very significant amendment, the goal of this proposal is to make the FISCR a more permanent entity. If the court's jurisdiction is to be greatly increased from the first proposed change, then the court will need to be able to handle a much larger case load. The FISCR would no longer be an elusive entity with only two public decisions during the thirty-six

276. 28 U.S.C. §§ 291–296 (2012).

277. *Cavanagh*, 807 F.2d at 792 (citing 28 U.S.C. § 292(e); 28 U.S.C. § 1407(d); Economic Stabilization Act Amendments of 1971, Pub. L. No. 92-210, § 211(b)(1), 85 Stat. 743, 749 (1971)).

278. PRESIDENT'S REVIEW GROUP REPORT, *supra* note 10, at 207.

279. 50 U.S.C. § 1803(a).

years of its existence. Its operation would become more similar to that of other federal appeals courts, and thus become a full-time position for FISCR judges. This would allow the court to more adequately carry out its duties to preserve the privacy and security of U.S. citizens.[280]

V. CONCLUSION

While many improvements continue to be made on the substantive issues involved with FISA, such as moving the storage of metadata out of government hands,[281] we must also improve the procedural structure of our foreign intelligence courts to create a lasting impact. Because of the way FISA rules are currently applied, individual liberty is being unnecessarily sacrificed in the name of "foreign" intelligence surveillance. In order to better protect the privacy of U.S. citizens and to direct our surveillance resources at true national security threats, fundamental procedural changes must be made to FISA. First, FISC proceedings should be amended to allow for a more adversarial process so that individual freedom is adequately represented in hearings before both the FISC and the FISCR. Second, two fundamental changes should be made to the current FISA appellate process. FISA should be amended to allow both denials and approvals of surveillance applications to be "final decisions" which can be appealed to the FISCR. Further, the FISCR should become a more permanent entity with full-time judges.

Only by amending FISA, can the United States move past the security leaks that occurred during 2013 and ensure that this massive breach of individual privacy does not occur again in the future. However we must keep in mind that history has shown us that we tend to overact by improving national security at the expense of civil liberties during times of crisis involving threats of violent attacks against the nation.[282] It is important that as we face this current crisis of attacks on individual privacy, we do not make the opposite mistake and promote civil liberty at the expense of national security. The United States must seek the appropriate balance between these two competing concerns.

280. Gewirtz, *supra* note 256.

281. Adam Schiff, *Rep. Schiff Statement on FISA Court Approval on NSA Telephone Metadata Program*, HOUSE.GOV (Feb. 7, 2014), http://schiff.house.gov/press-releases/rep-schiff-statement-on-fisa-court-approval-of-limits-on-nsa-telephone-metadata-program/.

282. Northouse, *supra* note 1, at 6.