

Is Uncle Sam Stalking You? Abandoning Warrantless Electronic Surveillance to Preclude Intrusive Government Searches

J. Alexandra Bruce*

ABSTRACT

The Founders drafted the Fourth Amendment foreseeing immense governmental abuse likely to stem from intrusive, unlimited searches. The Fourth Amendment bars any government investigative efforts absent a warrant grounded in a showing of probable cause. Further, the Fourth Amendment specifically protects the “papers” of U.S. citizens. This is interpreted to extend to all private communication whether conducted through traditional or electronic channels.

This article argues the Fourth Amendment mandates oversight in all surveillance conducted by the intelligence community. Administrations have made continuous efforts to conduct massive collections of electronic data—including private communications of U.S. citizens—without obtaining a warrant. The foreign surveillance exception was recognized to provide the Executive with an exception to the Fourth Amendment’s warrant requirement where the investigation was centered on national security. The numerous abuses stemming from the recognition of an

* J. Alexandra Bruce author graduated *summa cum laude* from The University of Mississippi School of Law in 2017 and serves as a judicial law clerk to the Honorable Rhesa H. Barksdale of the United States Fifth Circuit Court of Appeals for the 2017-2018 term. The author wishes to thank Professor Ronald Rychlak for his integral role in developing this Article. Additionally, the author would like to thank her mother, Elisa Bruce, for her continued support and encouragement in academic endeavors.

JOURNAL OF LAW AND CYBER WARFARE

Special Comment

- I. Instegogram: A New Threat and Its Limits for
Liability1
Jennifer Deutsch & Daniel Garrie

Articles

- II. A Democracy of Users8
John Dever & James Dever
- III. Is Uncle Sam Stalking You? Abandoning
Warrantless Electronic Surveillance to Preclude
Intrusive Government Searches51
J. Alexandra Bruce
- IV. Cyber Enhanced Sanction Strategies: Do
Options Exist?95
Mark Peters

Country Briefings

- V. North Korea: The Cyber Wild Card 2.0155
Rhea Siers
- VI. Privacy and Data Protection in India166
Dhiraj R. Duraiswami

Volume 6 | Summer 2017 | Issue 1

(c) 2012-2017. Journal of Law and Cyber Warfare.

All Rights Reserved.

Editor-in-Chief

Daniel B. Garrie, *Neutral at JAMS*

Managing Editor

Brandon J. Pugh

Executive Editor

Michael Mann

Digital Content Editor

Dhiraj Duraiswami

Staff

Irene Byhovsky
Benjamin Dynkin
Jonathan Grekstas
John Kilgore
Cody Valdez

Jennifer Deutsch
John Foulks
Bryan Horen
Alex Medoway
Julia Yang

Richard Diorio
Brian Gilligan
Geoff Kalendar
Patrick Severe

Editorial Board

Prof. Richard Andres

National War College

Prof. Diana Burley

George Washington University

Roland Cloutier

CSO, ADP

Parham Eftekhari

Co-Founder, ICIT

Will Hudson

Senior Advisor for
International Policy, Google

Jean-Claude Knebler
Ambassador of Luxembourg
to the Russian Federation

Dr. Larry Ponemon

Chairman, Ponemon Institute

Lt. Col. Shane Reeves

Professor, West Point

David Shonka

Principal Deputy General
Counsel, FTC

William Spernow

CISO, Forensic Scan

Sheryl Ann Yamuder

VP of Business & Legal
Affairs, Roku, Inc.

Robert Bair

Lieutenant Commander, Navy

Christopher Burgess

CEO, Prevendra

John Dever

Head of AML/Sanctions,
Wells Fargo

Deborah Housen-Couriel

Special Counsel, ZEK

Prof. Eric Jensen

Brigham Young University

Jeremy Kroll

CEO, K2 Intelligence

Dr. James Ransome

Senior Director of Product
Security, McAfee

Prof. Michael Schmitt

U.S. Naval War College

Prof. Rhea Siers

John Hopkins University

Dr. Joseph Weiss

Managing Partner, ACS

Amit Yoran

Chairman & CEO,
Tenable Network Security

Richard Borden

Chief Privacy Officer/Partner,
White & Williams LLP

Uma Chandrashekar

Head, Global Info. Security
Office, Edwards Lifesciences

James Dever

Chief of Intelligence Law,
Army Intelligence

Jane Horvath

Senior Director of Global
Privacy, Apple

Joseph Johnson

CISO, Premise Health

David Lawrence

Co-Founder, RANE

Dr. J.R. Reagan

Vice Dean,
Woosong University

Maj. Gen. Ami Shafran

Director, Evigilo

Mitchell Silber

Senior Managing Director, FTI

Jody Westby

CEO, Global Cyber Risk LLC

Elad Yoran

CEO, Security Growth Partners

exception, led Congress to draft the Federal Intelligence Surveillance Act. This statute mandated judiciary and legislative oversight of the Executive's previously unchecked power to conduct intelligence surveillance.

This article is the first to consider completely abandoning the foreign intelligence exception, to maintain all national security electronic surveillance with the oversight of the Federal International Surveillance Court.

The Federal International Surveillance Court, organized through FISA, provides a tribunal for an independent judiciary to consider the constitutionality of the intelligence community's electronic surveillance procedures. The court scrutinizes the particular intelligence purpose; the reasonableness of the surveillance; and maintains minimization procedures.

This article scrutinizes the constitutionally problematic investigations rendered through warrantless searches. Lastly, the article provides evidence to demonstrate vulnerable privacy rights best preserved by foregoing the problematic "foreign intelligence exception" to subject all searches—even those centered on the security of the nation—to the oversight of a neutral judiciary.

INTRODUCTION

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time.¹

George Orwell

¹ George Orwell, *1984*, 1 (1949).

For decades the courts and legislature have grappled over the appropriate balance of the preservation of constitutionally protected privacy rights and national security intelligence surveillance.² Despite the Fourth Amendment's clear preference for warrants,³ administrations have repeatedly employed electronic surveillance—absent a warrant—for the purported goal of obtaining national security intelligence.⁴ Conflicts in the Government's right to protect the security of the nation and citizens' rights to privacy continue to frustrate the legal system.⁵

Insufficient standards for constitutional intelligence gathering and immense opportunity for unreasonable investigatory searches generated by the “foreign intelligence

² See generally, *U.S. v. U.S. Dist. Court for the Eastern Dist. of Mich. (Keith)*, 407 U.S. 297, 314–15 (1972) (holding “As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression.”).

³ *State v. Edman*, 281 Conn. 444, 454 (Conn. Feb. 27, 2007) (discussing “both the state and federal constitution evince a preference for obtaining search warrants to protect the individual rights of our citizens. ‘[I]t is a cardinal principle that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions.’”) (citing *Mincey v. Arizona*, 437 U.S. 385, 390 (1978); *Katz v. United States*, 389 U.S. 347, 357 (1967)).

⁴ *Keith*, 407 U.S. at 311 n.10. (citing Br. for Pet’r at 16-18; Br. for Resp’t at 51-56; 117 Cong. Rec. 14056.).

⁵ See generally, *Keith*, 407 U.S. at 297; see also James E. Meason, *The Foreign Intelligence Surveillance Act: Time for Reappraisal*, 24 Int’l Law. 1043 (1990) (hereafter “24 Int’l Law”); see also 50 U.S.C.A. § 1801 (West 2015); see also *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006); In re. Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008).

exception”⁶ encouraged the passing of the 1978 Foreign Surveillance Act (FISA).⁷ Centered on facilitating efficient intelligence gathering and preserving citizens’ constitutional privacy rights,⁸ FISA designed a court to administer warrants in the unique circumstances of foreign intelligence surveillance.⁹ The Foreign Intelligence Surveillance Court (FISC), provides a judicial oversight procedure sufficient to satisfy the Fourth Amendment’s reasonableness mandate — the process is considered a “warrant within the meaning of the Fourth Amendment”¹⁰—the court administers these “warrants” for the majority of the Government’s FISA surveillance efforts.¹¹ The FISA was drafted with the intention of structuring a procedure to enforce judicial

⁶ *Keith*, 407 U.S. 297; see also Nola K. Breglio, *Leaving Fisa Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 Yale L.J. 179 (2003) (stating “The foreign intelligence exception [] remained a large window for *totally unsupervised* government surveillance.”).

⁷ Rep. No. 604, 95th Cong., 1st Sess. at 7 (1977); see also S. REP. 95-604(I).

⁸ Alan Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of Fisa Surveillance*, 48 New Eng. L. Rev. 55 (2013).

⁹ S. REP. 95-604(I).

¹⁰ *United States v. Megahey*, 553 F. Supp. 1180, 1190 (E.D.N.Y. Dec. 1, 1982) (“[T]he FISA warrant is a warrant within the meaning of the Fourth Amendment, since it provides for the interposition of independent judicial magistrates between the executive and the subject of the surveillance which the warrant requirement was designed to assure.”).

¹¹ Butler, *supra* note 8 at 55.

oversight and maintain the limitations of the Fourth Amendment.¹²

The Supreme Court holds “warrantless electronic surveillance” proves unreasonably intrusive, and extends beyond what is constitutionally permitted by the Fourth Amendment.¹³ Though the Court’s holding was clear that criminal investigations employing warrantless electronic surveillance proved unconstitutionally intrusive, the Court left open the question of whether or not an exception existed for investigations centered on national security threats.¹⁴

This article argues that the FISC should not only be maintained, but continue as the sole remedy for the Government to obtain approval of electronic national security surveillance. The prevailing constitutional validity provided through FISC-approved investigations is conveyed through both Court precedent— holding warrantless searches unreasonable even where conducted for national security¹⁵— and the overwhelming post FISA opinions

¹² *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. N.Y. Aug. 8, 1984) (“The procedural safeguards laid out in the Act ‘are necessary to insure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the Fourth Amendment.’”) (citing S. Rep. No. 701, 95th Cong., 2d Sess. 13, reprinted in 1978 U.S. Code Cong. & Ad. News 3973, 3982 (“Senate Report 95-701”)).

¹³ *Katz*, 389 U.S. at 347 (1967).

¹⁴ “Whether 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.” *Id.* at 358 n.23.

¹⁵ See generally, *Katz*, 389 U.S. at 347 (1967); see also *Keith*, 407 U.S. at 297, 314–15 (1972); but see *Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).

holding the FISC and FISA procedures constitutionally sound.¹⁶

Previous articles have argued “warrant-free” intelligence procedures prove more effective, and more protective of the target’s Fourth Amendment rights.¹⁷ Similarly, articles find that the targets of these warrantless investigations are better suited to challenge the searches’ reasonableness “after the fact in normal Article III courts.”¹⁸

This article argues completely foregoing constitutionally prohibited warrantless searches—even within the delicate climate of national security threats—to rely solely on FISC approved electronic surveillance and

¹⁶ See generally, *United States v. Abu-Jihaad*, 630 F.3d 102, 120 (2d Cir. 2010); see also *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007); see also *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); see also *In re Sealed Case*, 310 F.3d at 742–46; *United States v. Johnson*, 952 F.2d 565, 573 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790–92 (9th Cir. 1987); *United States v. Kashmiri*, No. 09 Cr. 830–4, 2010 WL 4705159, at 3–5 (N.D. Ill. Nov.10, 2010); *United States v. Warsame*, 547 F.Supp.2d 982, 993 (D. Minn. 2008); *United States v. Mubayyid*, 521 F.Supp.2d 125, 135–41 (D. Mass. 2007); *United States v. Holy Land Found. for Relief & Dev.*, No. 04 Cr. 240, 2007 WL 2011319, at 5–6 (N.D. Tex. July 11, 2007); *United States v. Jayyousi*, No. 04 Cr. 60001, 2007 WL 851278, at 1 (S.D. Fla. Mar.15, 2007); *United States v. Benkahla*, 437 F.Supp.2d 541, 554 (E.D. Va. 2006); *United States v. Marzook*, 435 F.Supp.2d 778, 786 (N.D. Ill. 2006); *United States v. Nicholson*, 955 F.Supp. 588, 590–91 (E.D. Va. 1997); *In re Kevork*, 634 F.Supp. 1002, 1014 (C.D. Cal. 1985); *United States v. Falvey*, 540 F.Supp. 1306, 1312 (E.D.N.Y. 1982).

¹⁷ Breglio, *supra* note 6 (arguing to “revive the constitutional viability of foreign intelligence surveillance [by] forego[ing] the FISA warrant procedure entirely”); see also Carol M. Bast (FNd1) & Cynthia A. Brown, *A Contagion of Fear: Post-9/11 Alarm Expands Executive Branch Authority and Sanctions Prosecutorial Exploitation of America’s Privacy*, 13 Cardozo Pub. L. Pol’y & Ethics J. 361 (2015) (arguing, “under FISA and the contagion of fear of terrorism is a lethal combination leading to an almost necessary loss of protection for civil liberties.”).

¹⁸ Breglio, *supra* note 6.

intelligence gathering procedures. The first section considers the FISC's efficiency through scrutiny of the court's ability to preserve both the Fourth Amendment's clear prohibition of warrantless searches, and encourage efficient foreign intelligence gathering procedures. The second section argues the FISC proves sound public policy by serving to better preserve civil liberties, vulnerable to increased security threats. The third section considers the Executive overreach procured through the FISC's oversight and scrutiny of intelligence operations.

In conclusion, the FISC is demonstrated to serve as the most effective to combat the constitutionally problematic nature of balancing the Government's right to protect the nation, and citizens' constitutionally protected privacy rights.¹⁹ Additionally, modifications to the court's structure to increase judicial oversight, and a complete abandonment of the foreign intelligence exception will be explored as the most effective mode for the preservation of civil liberties.

I. BACKGROUND OF THE FISA COURT

Prior to the drafting of the Federal Intelligence Surveillance Act (FISA), the Executive's constitutional authority to protect the nation was interpreted to accord an "inherent power" to conduct warrantless searches

¹⁹ *Duggan*, 743 F.2d at 74 (finding that FISA procedures "provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information"); see also *Pelton*, 835 F.2d at 1075 ("FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment").

purportedly sustained for national security purposes.²⁰ These Government-orchestrated intelligence gathering efforts were argued as “reasonable” under the theory the President and Attorney General sustain an exemption to the Fourth Amendment when working to protect the nation’s security.²¹ The abuse inherent to this exemption is conveyed through the “sixty-five thousand *domestic* intelligence investigations” that were conducted by the FBI—absent obtaining a warrant or judicial oversight—within just one year.²²

These Government actions offend the intention of the Fourth Amendment’s limitations on intrusive Executive power obtained through unreasonable searches.²³ A regimen of unchecked Executive actions to carry out warrantless

²⁰ Br. for Resp’t at 30, *Keith*, 407 U.S. at 297 (1972) (No.135521); *see also Duggan*, 743 F.2d at 72; *See also Truong*, 629 F.2d at 912-14, *cert. denied*, 454 U.S. 1144 (1982); *see also United States v. Buck*, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir.) (*en banc*), *cert. denied*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *but see Zweibon v. Mitchell*, 516 F.2d 594, 633-651 (D.C. Cir. 1975), (dictum), *cert. denied*, 425 U.S. 944 (1976).

²¹ *Duggan*, 743 F.2d at 59, 72 (“Prior to the enactment of FISA, virtually every court that had addressed the issue had concluded that the President had the inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment.”); *see also Keith*, 407 U.S. at 301 (“the Government argued the warrantless electronic surveillance was lawful as a “reasonable exercise of Presidential power.”); *see also Truong*, 629 F.2d at 908.

²² SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755 at IV, V (1976), available at https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

²³ *See Br. for Resp’t*, *supra* note 4 at 12 (citing *Boyd v. United States*, 116 U.S. 616, 635 (1885)); *Marcus v. Search Warrant*, 367 U.S. 717 (1961); *Stanford v. Texas*, 379 U.S. 476 (1965).

searches amounts to the “hallmark of a police state.”²⁴ Watergate exposed the nation to the abuse possible where the Executive is left unchecked.²⁵ This led to judicial and legislative action reigning in, previously unrestrained, Executive intelligence efforts.²⁶

In 1972, the Supreme Court considered the constitutionality of domestic intelligence gathering methods.²⁷ Writing for the majority, Justice Powell held that warrantless *domestic* surveillance, absent prior judicial approval, failed to maintain the reasonableness standard mandated by the Fourth Amendment.²⁸ The decision narrowly considered solely “internal security matters,” avoiding any determination of the Executive’s power to investigate the “activities of foreign powers or their agents” absent a warrant.²⁹ Consequentially, the Executive remained uncertain of the constitutionality of its efforts to obtain foreign intelligence.³⁰

The legislature’s drafting of FISA was in response to Congressional awareness of the Intelligence Community’s increased encroachment on Americans’ civil liberties.³¹ The Church Committee—a Senate committee organized to investigate unconstitutional intelligence gathering schemes—discovered abuses including “warrantless break-

²⁴ See Br. for Resp’t, *supra* note 16 at 12 (citing *Shuttlesworth v. Birmingham*, 382 U.S. 87 (1969)).

²⁵ See 24 Int’l Law. at 1043.

²⁶ See generally, Breglio, *supra* note 5 at 7; see also 24 Int’l Law. at 1043.

²⁷ *Keith*, 407 U.S. at 310.

²⁸ See *Id.* (holding the “Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive.”).

²⁹ See *Id.*, at 322.

³⁰ See generally, Breglio, *supra* note 6 at 7; see also 24 Int’l Law. 1043.

³¹ Assistant Attorney General John P. Carlin Delivers Opening Remarks at the National Security Division 10 Year Anniversary Conference, JUSTICE NEWS (Dep’t of Just.), Sep. 14, 2016.

ins, excessive surveillance of politically “subversive” groups, and indiscriminate opening of citizens' mail.”³² The Committee's findings led Congress to draft FISA, reigning in the Executive's broad intelligence gathering powers and mandating legislative and judicial oversight of the Executive's investigative schemes.³³ American's civil liberties remain vulnerable today as warrantless searches remain valid under the “foreign intelligence exception.”³⁴ Reasonable, constitutionally valid search efforts demand judicial oversight to properly protect American's constitutional privacy rights.

*A. The FISC Proves Necessary to Prevent
Unreasonably Intrusive Electronic Surveillance*

The Supreme Court holds “individual freedoms” most effectively preserved through judicially administered warrants.³⁵ Further, intelligence gathering efforts’ require balancing “the legitimate need to safeguard domestic security” and the harm of impeding on “individual privacy and free expression.”³⁶ The fear of the “erosion of our sense of privacy and independence” was held to far outweigh the fear that “upheaval will modify our form of government.”³⁷

Prior to the passing of FISA, warrantless investigations were employed by numerous administrations

³² *Id.*

³³ *Id.*; see also 24 Int'l Law. at 1043.

³⁴ *In re Directives*, 551 F.3d at 1013.

³⁵ Redacted, 2011 WL 10945618 at 26 (Foreign Intel. Surv. Ct. Oct. 3, 2011).

³⁶ *Keith*, 407 U.S. at 314.

³⁷ *Id.*

for the purported purpose of protecting national security.³⁸ Since the 1940s, administrations have exploited the preservation of national security to conduct intrusive surveillance efforts, void of judicial oversight.³⁹ Administrations employing these “warrantless wiretapping activities” did not consider the failure to obtain a warrant a bar to the pursuit of criminal prosecution.⁴⁰ The targets of these constitutionally invalid searches were prosecuted with evidence obtained through the warrantless investigations.⁴¹

Through the passing of FISA, Congress orchestrated the Federal Intelligence Surveillance Court.⁴² This Article III court is composed of 11 U.S. district judges, maintaining the power to grant approval for particular electronic surveillance efforts where the government maintains “probable cause to believe” the targets of their surveillance efforts are “foreign power[s] or agent[s] of a foreign power.”⁴³

FISA’s specific inclusion of an “agent of a foreign power” affords opportunity for the oversight of electronic surveillance, targeted at U.S. citizens.⁴⁴ An “agent of a

³⁸ See *Keith*, 407 U.S. at 314; see also *Katz*, 389 U.S. at 364 (Justice White concurring) (“Wiretapping to protect the security of the Nation has been authorized by successive Presidents... We should not require the warrant procedure and the magistrate’s judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.”).

³⁹ *Keith*, 407 U.S. at 311 n.10 (Past administrations have employed electronic surveillance in cases concerning organized crime and other various “domestic security cases” since at least 1946.) (citing Br. for Pet’r 16-18; Br. for Resp’t 51-56; 117 Cong. Rec. 14056.).

⁴⁰ Br. for Resp’t, *supra* note 15 at 100.

⁴¹ *Id.*

⁴² 50 U.S.C.A. § 1801 (West).

⁴³ See Br. for Pet’r at n.1, *Wikimedia Foundation v. NSA* (2015) (No. 5025551) (citing 50 U.S.C. § 1803(a); *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007)); see also *In re Sealed*, 310 F.3d at 722 (citing 50 U.S.C. § 1805(a)(3)).

⁴⁴ See Br. for Pet’r, *supra* note 35 (citing 50 U.S.C. § 1805(e)(1)).

foreign power” includes U.S. citizens who “knowingly engage in clandestine intelligence gathering activities” or “knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof.”⁴⁵ Though the FISC presents an opportunity for the government to obtain judicial approval to conduct investigations with a less stringent standard of probable cause,⁴⁶ judicial approval remains necessary.⁴⁷

1. The Foreign Intelligence Exception is Insufficient to Constitutionally Maintain Electronic Foreign Intelligence Surveillance

The Court has acknowledged the “legitimate need” for intelligence gathering through electronic surveillance,⁴⁸ yet failed to expressly determine what foreign surveillance actions maintain constitutional validity.⁴⁹ The lack of Court precedent led various circuit courts to find a “foreign intelligence exception” rendering the recognition of the Government exemption from the Fourth Amendment’s Warrant Clause.⁵⁰

⁴⁵ See *Id.* (citing 50 U.S.C. § 1805(b)(2)(A)).

⁴⁶ 50 U.S.C. § 1805(a)(3)(A)(2000).

⁴⁷ *Id.*

⁴⁸ See generally, *Katz*, 389 U.S. at 347.

⁴⁹ *Keith*, 407 U.S. at 297, 314. (Holding that “prior judicial approval” was necessary for the type of surveillance in the particular case and that the mandate on warrants for searches applies solely to domestic investigations and intelligence gathering); see also *Katz*, 389 U.S. at 347.

⁵⁰ See *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974); see also *Truong*, 629 F.2d at 913-16; see also *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973); see also *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977).

Courts recognizing the foreign surveillance exception to the general warrant requirement cited the “procedural hurdle” that could potentially hinder vital national security investigations.⁵¹ Additionally, the opinions convey an overall concern that the judiciary lacks the necessary knowledge to make determinations regarding appropriate foreign intelligence measures.⁵² This exception is considered appropriate only where the executive conveys the particular surveillance is administered “‘primarily for foreign intelligence reasons.’”⁵³ This presents both procedural and prosecutorial burdens, as should it be determined the particular investigation was “‘primarily a criminal investigation,” all evidence discovered through the warrantless procedure will be appropriately excluded.⁵⁴

2. The FISC Approved Foreign Surveillance Efforts are Sustained within the Limitations of the Fourth Amendment

The judiciary considers the “totality of the circumstances” in order to determine whether or not a particular search effort maintains the reasonableness mandated by the Fourth Amendment.⁵⁵ When employing this analysis, the judiciary considers the “nature of the government intrusion and how the intrusion is

⁵¹ *Truong*, 629 F.2d at 913.

⁵² *See Id.* (arguing, “the judiciary is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance.”).

⁵³ *See Id.*

⁵⁴ *Truong*, 629 F.2d at 913.

⁵⁵ *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (citing *Samson v. California*, 547 U.S. 843, 848, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006); *Tennessee v. Garner*, 471 U.S. 1, 8–9, 105 S.Ct. 1694, 85 L.Ed.2d 1 (1985)).

implemented.”⁵⁶ This is particularly influential in intelligence gathering efforts targeted at national security. Courts have consistently struggled to balance the constitutional limitations and the necessity of national security, as more intrusive search efforts are permitted where the government’s interest in conducting a search holds greater importance and preserving national security is of “the highest order of magnitude.”⁵⁷

The lacking specificity of the foreign surveillance exception resulted in sizable opportunities for unrestrained surveillance.⁵⁸ Concerned for the lacking standards in foreign surveillance and opportunity for intrusive, constitutionally invalid searches, Congress considered statutory procedures to procure constitutionally invalid surveillance, while securing foreign intelligence.⁵⁹

Recognizing the constitutional abuses inherent to unchecked Executive surveillance capability, Congress extended the Fourth Amendment’s protection against unreasonable searches to intelligence gathering.⁶⁰ With the passing of FISA, Congress took an active role in scrutinizing the Executive’s national security investigation techniques.⁶¹ Additionally, when considering the “inconvenience” judicial approval imposes on the Attorney General’s ability to investigate national security matters, the Court has held it “justified in a free society to protect constitutional values.”⁶²

⁵⁶ See *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1012.

⁵⁷ See *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1012.

⁵⁸ See Breglio, *supra* note 6 at 7.

⁵⁹ S. REP. 95-604(I).

⁶⁰ 24 Int’l Law. at 1043.

⁶¹ See *Id.*

⁶² *Keith*, 407 U.S. at 301.

B. FISA Provides for Efficient Foreign Surveillance While Preserving Civil Liberties

In 1978, Congress passed FISA with the intention of “provid[ing] further safeguards for individuals subjected to electronic surveillance.”⁶³ This Act served to maintain a level of judicial oversight of foreign intelligence gathering in order to preserve vulnerable civil liberties, while maintaining the flexibility necessary in these particular investigations.⁶⁴ The Act provided for the designation of judges to consider these specific foreign intelligence surveillance efforts.⁶⁵ These judges make up the Foreign Intelligence Surveillance Court (FISC), which serves to authorize a majority of the government’s FISA surveillance efforts.⁶⁶

The FISC considers the government’s methods for foreign intelligence gathering, and determines whether or not the actions comply with the Fourth Amendment.⁶⁷ FISA explicitly forbids “contents of any communication to which a United States person is a party . . . be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.”⁶⁸ The legislation is centered on facilitating effective gathering of crucial intelligence while

⁶³ S. REP. NO. 95-604(I).

⁶⁴ See Breglio, *supra* note 6 at 7.

⁶⁵ See generally, S. REP. NO. 95-604(I).

⁶⁶ See Butler, *supra* note 8 at 55.

⁶⁷ See 50 U.S.C.A. § 1881(a) (West).

⁶⁸ 50 U.S.C.A. § 1801(h)(4) (West).

protecting Americans' privacy rights.⁶⁹ Additionally, FISA has proven successful in prosecuting individuals discovered to be actively involved in carrying out acts of terrorism against the United States.⁷⁰

The FISC is criticized as insufficiently balancing the privacy rights of U.S. citizens and the vital need for homeland security surveillance,⁷¹ yet this court serves as the only government body with power to administer any judicial oversight. Arguments for the abolition of the FISC largely ignore the immense lack of protections available to defendants subjected to warrantless searches that are conducted absent any judicial oversight.⁷²

C. Judicial Approval through FISC Accords the Government Certainty that their Efforts Maintain Constitutionality and Evidence Obtained Will Not be Subject to Exclusion

FISA created a judicial procedure to oversee surveillance efforts and reign in unreasonable investigations utilized by the intelligence community.⁷³ The court, organized within FISA, acts independently "to review requests from intelligence professionals about tools or

⁶⁹ Senate leaders clarify the intentions of the legislation as creating a "more explicit...statutory intent, as well as to provide further safeguards for individuals subjected to electronic surveillance." S. REP. NO. 95-604(I).

⁷⁰ See generally, *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999).

⁷¹ Breglio, *supra* note 6 at 185.

⁷² Breglio, *supra* note 6 at 186 (noting the opportunity for "totally unsupervised government surveillance" under the foreign surveillance exception) (emphasis added).

⁷³ 50 U.S.C.A. § 1801 (West).

tactics that they intend to employ.”⁷⁴ The intelligence community is subject to additional congressional oversight under FISA mandates.⁷⁵

Following the September 11, 2001 terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“PATRIOT ACT”) to expand and improve the nation’s homeland security endeavors.⁷⁶ The Act expanded FISA and its function in monitoring foreign surveillance.⁷⁷ Specifically, the PATRIOT ACT altered the standard for obtaining a FISA warrant from demonstrating “the purpose” of the investigation to be the procurement of foreign intelligence, to only a government showing that the “significant purpose” of the investigation is collecting foreign intelligence.⁷⁸

The mere addition of the word “significant” provided the government with greater liberty to use information obtained through a FISA warrant in criminal prosecutions.⁷⁹ These changes have been heavily criticized as leaving defendants “virtually powerless to challenge the legitimacy of any such evidence.”⁸⁰ Additionally, those parties who are investigated through FISA approved intelligence gathering

⁷⁴ PRESS BRIEFING BY PRESS SECRETARY JOSH EARNEST, 2016 WL 5844916, at 3, 120 (Oct. 5, 2016).

⁷⁵ *Id.*; see 50 U.S.C. § 1801; see also Attorney General Loretta E. Lynch Delivers Keynote Address on Counterterrorism and International Cooperation, JUSTICE NEWS (Dep’t of Just.) Dec. 19, 2015; Butler, *supra* note 8 at 55.

⁷⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. (2001).

⁷⁷ *Id.*

⁷⁸ *Id.* (striking the Foreign Intelligence Surveillance Act of 1978’s language, “the purpose” and inserting “a significant purpose”).

⁷⁹ Breglio, *supra* note 6 at 15.

⁸⁰ *Id.*

procedures are able to challenge these searches in the FISC.⁸¹

II. THE FISC IS ESSENTIAL FOR ELECTRONIC INTELLIGENCE GATHERING METHODS TO MAINTAIN CONSTITUTIONALITY

Courts have struggled with the constitutionality of electronic surveillance for nearly a century. In the early 1900s, the United States Supreme Court analyzed the Fourth Amendment's limitations on the Government's ability to conduct investigations through wiretapping.⁸² In his dissent, Justice Brandeis recognized the harmful reality of unreasonable searches stemming from validation of Government efforts to intercept private citizens' communications.⁸³ Justice Brandeis' ominous dissent considers the probability that intrusive investigations would "not likely [] stop with wiretapping" to eventually lead to government intrusion into multiple facets of Americans' personal lives.⁸⁴

Over eighty years after Justice Brandeis' *Olmstead* dissent, a National Security Agency (NSA) electronic data collection procedure was challenged as effectively allowing a "government agent [to] open every letter that comes

⁸¹ See *In re Directives Pursuant to Sec. 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008).

⁸² *Olmstead v. United States*, 277 U.S. 438, 474 (1928).

⁸³ *Id.*

⁸⁴ In his dissent, Brandeis predicts the current difficulties surrounding the constitutionality of foreign surveillance efforts through interceptions of internet data. Brandeis states, "[w]ays may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Id.* at 473.

through a mail processing center to read its contents before determining which letters to keep.”⁸⁵ The constitutional obstructions extending from unchecked Executive power to employ electronic investigations is congruent with America’s ever expanding dependence on electronic communication.

A. Increased Electronic Communication and National Security Threats Proves FISA a Sound Public Policy

The digital economy and Americans’ economic and societal dependence on electronic communication continues to rapidly expand.⁸⁶ Increases in electronic communications have perpetuated the NSA’s elaborate schemes, using the newest technologies to intercept communications and gather intelligence worldwide.⁸⁷ With every aspect of American life currently touched by electronic communication,⁸⁸ there is an even greater need for judicial oversight in these intelligence-gathering efforts.⁸⁹

Arguing that the necessity to “protect the country” promulgates a presidential power to conduct warrantless investigations of both “agents of foreign powers” and

⁸⁵ Brief for Petitioner at 1–2, *Wikimedia Found. v. Nat’l Sec. Agency* (2016) (No. 703452).

⁸⁶ See generally, J. Alexandra Bruce, *A Billion Dollar Investment: The Profitability of Modifying the Current Energy Regulations to Secure the Nation’s Energy Supply*, 17 *Appalachian J.L.* (2017).

⁸⁷ Meason, *supra* note 6.

⁸⁸ Bruce, *supra* note 82.

⁸⁹ Though Silicon Valley innovators did not create technologies “so that people who want to harm innocent people can be more violent,” but rather because of their commitment to “making people freer to communicate or express their views,” terrorist organizations have employed social media to “propagate their hateful ideology.” Earnest, *supra* note 74 at 3.

“domestic organization[s],”⁹⁰ the Government contends warrantless searches, orchestrated by the Executive, prove reasonable when undergone to protect the security of the nation.⁹¹ Considering the government’s efforts to secure unchecked power for gathering intelligence through electronic surveillance, and Americans’ increased use of electronic communications, it is vital that judicial oversight into these intrusive searches be maintained and strengthened.⁹²

FISA, and the government actors working to implement FISA, have continued to generate “effective and civil liberties-protective foreign intelligence collection in the digital age.”⁹³ Modifications to FISA and its regulatory agents have coincided with the immense evolution of communication and modes of organizing terrorist activity.⁹⁴

Increasingly innovative forms of communication within the United States induced the intelligence and tech communities to coordinate efforts.⁹⁵ While maintaining both “statutory and constitutional limits,” these newly created entities facilitate “intelligence collection authorities that enable critical FBI counterintelligence and counterterrorism investigations.”⁹⁶ Nonetheless, these

⁹⁰ *Id.*

⁹¹ Brief for Petitioner at 2, *U.S. Dist. Court for the Eastern Dist. of Mich. (Keith)*, 407 U.S. 297 (1972) (No. 135522).

⁹² Brief for Petitioner at 2, *U.S. Dist. Court for the Eastern Dist. of Mich. (Keith)*, 407 U.S. 297 (1972) (No. 135522).

⁹³ Assistant Attorney General John P. Carlin Delivers Opening Remarks at the National Security Division 10 Year Anniversary Conference, JUSTICE NEWS (Dep’t of Just.), Sep. 14, 2016.

⁹⁴ *Id.*

⁹⁵ Earnest, *supra* note 70 at 3.

⁹⁶ Carlin, *supra* note 93.

innovative communications prove to be both constitutionally protected free speech and private speech.⁹⁷

In 2016, the Government worked with Twitter to shut down extremists employing the channel to propagate their message and “radicalize people.”⁹⁸ The continued cooperation of these entities, with competing interests, is vital to the future of intelligence gathering. The tech community is committed to innovation that increases the freedom of expression and ideas, whereas the Government is committed to protecting the nation from increased vulnerability to foreign terrorist organizations.⁹⁹

The balance of national security and free communication is effectively considered where these two communities cooperate.¹⁰⁰ Continuing oversight of electronic investigations, while including necessary private-sector parties, is essential to protecting vulnerable privacy rights and national security.

1. FISA’s Internal Review Process Provides Accountability

Protection of civil liberties, and the continued intelligence efforts necessary to homeland security, proved

⁹⁷ “The First Amendment protects anonymous online speech, which can be as necessary to democratic self-governance as the anonymous pamphlets our Founders wrote.” Brief for Petitioner, *supra* note 87, at 5 (citing *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997); *Taylor v. John Does*, 1-10, 2014 WL 1870733, at 2 (E.D.N.C. May 8, 2014).

⁹⁸ Earnest, *supra* note 70, at 3.

⁹⁹ *Id.*

¹⁰⁰ *Id.*

the central purpose for FISA.¹⁰¹ The NSA has utilized the FISC to aide in their efforts to internally police their practices, and remain within constitutional limits.¹⁰² Additionally, the FISC has conveyed a direct effort to be a greater force than merely a “rubber stamp” for any surveillance sought by the government.¹⁰³ The court has determined various government practices to be illegally conducted outside the limits of the Fourth Amendment.¹⁰⁴

The Department of Justice (DOJ) reports that the average time necessary to maintain FISA approval for gathering business records is 115 days.¹⁰⁵ FBI Agents, disproportionately those orchestrating cyber investigations, describe the FISC approval process as “lengthy,” and criticized the procedural burdens as having a “negative impact on their investigations.”¹⁰⁶ In particular, those agents conducting cyber investigations have found the process to be burdensome.¹⁰⁷ Though these procedural limitations may

¹⁰¹ S. REP. NO. 95-604(I) (quoting Attorney General Bell while noting “for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect”).

¹⁰² *In re Prod. of Tangible Things from [Redacted]*, No. BR 08–13, 2009 WL 9150913, at 3 (FISA Ct. Mar. 2, 2009).

¹⁰³ See generally, Michael T. Francel, *Rubber-Stamping: Legislative, Executive, and Judicial Responses to Critiques of the Foreign Intelligence Surveillance Court One Year After the 2013 NSA Leaks*, 66 Admin. L. Rev. 409 (2014); see also Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really A Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate*, 66 Stan. L. Rev. Online 125 (2014).

¹⁰⁴ See *First Direct Evidence of Illegal Surveillance Found by the FISA Court*, WASH. POST (Oct. 12, 2011), <http://apps.washingtonpost.com/g/page/national/first-direct-evidence-of-illegal-surveillance-found-by-the-fisa-court/393>.

¹⁰⁵ See generally, *OJ OIG Releases Report on the FBI's Use of Section 215 of the Patriot Act*, DEP'T OF JUSTICE (September 29, 2016), <https://oig.justice.gov/press/2016/2016-09-29.pdf>.

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

occasionally prove burdensome to the intelligence community, these safeguards are vital as innovative technologies are employed.¹⁰⁸ The agents, conducting electronic surveillance, perceiving the process as burdensome, further demonstrates the procedural safeguards employed to protect the privacy rights impacted by electronic communications.

Dissimilar from pre-FISA administrations, the Obama administration pledged to center the intelligence communities' determination of proper use of new technologies on the balancing of privacy rights, while effectively avoiding attacks on the nation.¹⁰⁹ This continued Executive focus on the balancing of privacy rights and effective intelligence gathering, whether or not effectively carried out, further conveys the more conservative approach maintained post-FISA.

2. The FISC Provides Judicial Oversight to Prevent Prosecutorial Abuses and Executive Overreach

Prior to the passing of FISA, Congress “deferred to presidential authority” for decisions related to intelligence,¹¹⁰ and the legislature avoided maintaining any active role in intelligence for more than a century.¹¹¹ Without any clear limitations, the government orchestrated lawful, warrantless intelligence gathering methods for the purported endeavor of “protect[ing] national security.”¹¹² Challenges to the admission of evidence obtained through these warrant-

¹⁰⁸ See Earnest, *supra* note 74, at 3.

¹⁰⁹ See *Id.*

¹¹⁰ See Meason, *supra* note 83.

¹¹¹ *Id.*

¹¹² *Keith*, 407 U.S. at 300.

free searches, forced Government criticism of the lacking standards “to authorize national security intelligence wiretaps,” and any “meaningful or appropriate guideline[s]” for constitutional surveillance.¹¹³

Under FISA, Executive surveillance schemes are subject to judicial and legislative oversight.¹¹⁴ FISA stemmed reform of the Executive’s approach to maintaining both foreign and domestic electronic surveillance. Dissimilar from previous administrations’ interpretation of an Executive exemption to the Fourth Amendment,¹¹⁵ the Obama administration supported intelligence subject to “rigorous oversight by all three branches.”¹¹⁶

B. Utilizing the Significant Purpose Test to Determine the Appropriateness of a FISA Warrant Proves Consistent with the Fourth Amendment

Overwhelmingly, the controversy surrounding the FISC, and the court’s decisions are centered on recent FISA provisions expanding the legally permitted aggregate of intelligence surveillance conducted within the United States.¹¹⁷ Though much criticism centers on the FISC, one of the most challenged portions of FISA is the FISA Amendments Act of 2008 (FAA), which effectively expands

¹¹³ Brief for Respondent, *supra* note 16, at 3-4.

¹¹⁴ 50 U.S.C.A. § 1801 (West).

¹¹⁵ See generally Brief for Respondent, *supra* note 16.

¹¹⁶ Earnest, *supra* note 70, at 3.

¹¹⁷ See Butler, *supra* note 7, at 55 (citing USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. §§ 1861-62 (2006)) (citing FISA Amends. Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2438 (2008) (codified as amended at 50 U.S.C. § 1881a (2006 & Supp. III 2010))).

the power of the intelligence community by suppressing the oversight power of FISA and the FISC.¹¹⁸

Though controversial, the PATRIOT Act's addition of a "significant purpose" test has been considered and determined to be within the limits of the Fourth Amendment.¹¹⁹ The 3rd Circuit holds the "significant purpose" renders the government unable to obtain foreign surveillance for the "sole objective of criminal prosecution."¹²⁰ Additionally, the court determined that the government must convey a "broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses" in order to maintain the "significant purpose" necessary to obtain a FISA warrant.¹²¹

FISA's implementation of the "significant purpose" test proves more protective of individual rights than an unchecked foreign intelligence exception. Prior to the creation of the FISC, the Government maintained evidence procured through warrantless foreign surveillance, appropriately excluded only where "the purpose of the particular surveillance was not intelligence gathering but obtaining evidence of crime."¹²² The amended FISA statute, by modifying the standard of the "primary purpose" for conducting foreign intelligence to the "significant purpose,"¹²³ mandates the "government have a measurable foreign intelligence purpose, other than just criminal

¹¹⁸ Butler, *supra* note 7, at 55 (citing 50 U.S.C. § 1881a(a)).

¹¹⁹ See *In re Sealed Case*, 310 F.3d 717, 735 (2002); see also *United States v. Duka*, 671 F.3d 329, 344 (3d Cir. 2011) ("FISA's 'significant purpose' standard is reasonable in light of the government's legitimate national security goals.").

¹²⁰ 310 F.3d 717, 735.

¹²¹ *Id.*

¹²² *Id.*

¹²³ 50 U.S.C.A. § 1804(a)(6)(B) (West).

prosecution of even foreign intelligence crimes.”¹²⁴ Though criminal prosecution cannot amount to the primary objective of the investigation, evidence uncovered through a legally sound foreign intelligence investigatory search is admissible in criminal prosecutions.

Where a law enforcement officer is legally on the premises conducting a lawful search, any violations of law discovered are appropriately considered permissible evidence.¹²⁵ Courts are consistent in upholding the “significant purpose test” as constitutionally within the limits of the Fourth Amendment.¹²⁶ This renders evidence, acquired through an appropriately conducted FISA search, admissible in domestic criminal prosecutions.¹²⁷

Conveying the “probable cause to believe that a foreign agent is communicating with his controllers outside our borders makes an interception reasonable” under the constitutionally valid FISA requirements.¹²⁸ Therefore, should an agent uncover evidence related to a domestic crime, while conducting a FISA investigation, this evidence

¹²⁴ *United States v. Abu-Jihaad*, 630 F.3d 102, 128 (quoting *Sealed Case*, 310 F.3d at 735); *see also* *United States v. Duka*, 671 F.3d 329, 344 (3d Cir. 2011).

¹²⁵ “Inspectors lawfully on the premises under such warrants may report any violations of law that they find; evidence in plain view need not be overlooked, even if that evidence concerns a different statute.” *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007); *see also* *United States v. Hartwell*, 436 F.3d 174, 181 n.13 (3d Cir. 2006) (“[T]he fruits of the search need not be suppressed so long as the search itself was permissible.”).

¹²⁶ *Abu-Jihaad*, 630 F.3d at 128; *see also* *Sealed Case*, 310 F.3d at 735; *Duka*, 671 F.3d at 344 (3d Cir. 2011); *Hartwell*, 436 F.3d at 181.

¹²⁷ *Ning Wen*, 477 F.3d at 898 (holding that the principles alloying “[i]nspectors lawfully on the premises under such warrants [to] report any violations of law that they find” appropriately extend to FISA, and under this context “evidence in plain view need not be overlooked, even if that evidence concerns a different statute”); *see also* *Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

¹²⁸ *Id.*

may be appropriately considered “in plain view” and admissible in a domestic criminal prosecution.¹²⁹

The process of maintaining FISA warrant procedures, and the FISC serves to protect prosecutors who may otherwise be forced to exclude evidence determined to have been unlawfully discovered. Dissimilar from the vulnerability to exclusion that evidence—procured in warrantless investigations failing to maintain a consistent intent of intelligence gathering—is subject to, all evidence procured through these FISA approved investigations will not be subject to exclusion.¹³⁰

*C. National Security Investigations Demand a
Warrant Process and the Judiciary is Qualified
to Administer Oversight*

Constitutionally protected privacy rights are extremely vulnerable to the government’s collection of the “personal communications of U.S. persons.”¹³¹ The Fourth Amendment specifically protects “papers” of U.S. citizens from “unreasonable search and seizure.”¹³² Because a person’s private communication is “akin to personal papers,” this protection extends to letters “transmitted by letter, telephone or e-mail.”¹³³ It follows that judicial oversight and Fourth Amendment limitations appropriately reach all government data-collection initiatives.

¹²⁹ *Id.*

¹³⁰ Evidence uncovered through a reasonable intercept “may be used in a domestic prosecution whether or not the agents expected to learn about the domestic offense.” *Id.*

¹³¹ Redacted, 2011 WL 10945618, at 26 (FISA Ct. Oct. 3, 2011)

¹³² *Id.*; see also *Truong Dinh Hung*, 629 F.2d at 915 (discussing how “individual privacy interests are severely compromised any time the government conducts surveillance without prior judicial approval”).

¹³³ *Id.*

Previous courts have held the Executive maintains the power to execute warrantless *foreign* intelligence gathering under its “Article II authority over foreign affairs.”¹³⁴ The constitutional vulnerability rendered through the recognition of this narrow exception is conveyed through the Government’s purported interpretation of the exception to extend to permit even warrantless domestic surveillance.¹³⁵

Unsurprisingly, government intrusion into the private lives of Americans, even under judicial governance, renders angst amongst the citizenry.¹³⁶ Determining the appropriate balance between the government’s responsibility to maintain domestic security, and the constitutional rights of its citizens, proves increasingly difficult in the hostile climate of foreign terrorist threats.¹³⁷

The FISC and Title III courts each serve to authorize electronic surveillance.¹³⁸ The courts differ on the standards of probable cause necessary to obtain an authorization for electronic surveillance.¹³⁹ Title III mandates a showing of “probable cause for belief that an individual is committing, has committed, or is about to commit” a particular crime.¹⁴⁰

¹³⁴ *Abu-Jihaad*, 630 F.3d at 121 (citing *Truong*, 629 F.2d at 908).

¹³⁵ What is defined as an “agent of a foreign power” may include U.S. citizens who are determined to be “knowingly engag[ing] in clandestine intelligence gathering activities” or “knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof.” Brief for Petitioner at 29–34, *United States v. U.S. District Court (Keith)*, 444 F.2d 651, 653 (6th Cir. 1971), *aff’d*, 407 U.S. 297 (1972) (citing 50 U.S.C. § 1805(b)(2)(A)).

¹³⁶ *Keith*, 407 U.S. at 312.

¹³⁷ *See id.*; *see also* Francel, *supra* note 30; Clarke, *supra* note 30; *Sealed Case*, 310 F.3d 717; Earnest, *supra* note 70, at 12 (discussing the balancing of “the need to protect our basic constitutional rights and the need to protect the United States of America”).

¹³⁸ *Sealed Case*, 310 F.3d at 738.

¹³⁹ *Id.*

¹⁴⁰ 18 U.S.C.A. § 2518(3)(a) (West).

Dissimilarly, FISA mandates the government demonstrate “probable cause that the target is a foreign power or an agent of a foreign power.”¹⁴¹

Judicial oversight is vital, as the Government acknowledges evidence procured through foreign surveillance efforts are appropriately utilized in “prosecuting the crime thus disclosed.”¹⁴² Preservation of individual liberties, vulnerable to intrusive government search initiatives, are best protected through judicially administered warrants.¹⁴³

A court specifically designed to scrutinize the constitutionality of intelligence surveillance proves necessary as the technology employed by the intelligence sphere is “extremely complex.”¹⁴⁴ To grasp the complexity of various intelligence surveillance methods, the FISC is briefed by various parties in the intelligence community.¹⁴⁵

The necessity of a warrant process within the intelligence community is conveyed through recent intelligence surveillance methods that fail to maintain FISC approval. One of the most controversial intelligence surveillance programs—upstream surveillance— maintains very little FISC oversight.¹⁴⁶ The NSA employs this procedure, absent a FISC warrant,¹⁴⁷ “to seize[] Americans’

¹⁴¹ 50 U.S.C.A. § 1805(a)(3) (West).

¹⁴² See generally Brief for Petitioner at 1–2, *Wikimedia Found. v. Nat’l Sec. Agency* (2016) (No. 703452).

¹⁴³ *Keith*, 407 U.S. at 311, but see *Truong Dinh Hung*, 629 F.2d at 913 (finding “the judiciary [] largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance”) (citing *New York Times Co. v. United States*, 403 U.S. 713, 727–30 (1971) (Stewart, J., concurring); *United States v. Belmont*, 301 U.S. 324, 330 (1937)).

¹⁴⁴ *United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *11 (D. Or. June 24, 2014)

¹⁴⁵ *Id.*

¹⁴⁶ Reply Brief for Petitioner, *supra* note 87, at 11–12.

¹⁴⁷ *Megahey*, 553 F. Supp. at 1190 (determining the FISC process is a

communications in bulk and review the contents of substantially all international text-based communications--and many domestic communications as well.”¹⁴⁸

III. UTILIZING FISC AND PROHIBITING WARRANTLESS SEARCHES IMPROVES PUBLIC TRUST AND ACCOUNTABILITY OF GOVERNMENT INTELLIGENCE

Since the passing of FISA, the legislature has continued efforts to regulate and oversee intelligence. In 2006, the National Security Division was created to generate “information sharing, coordination and unity of purpose” within the national security sector.¹⁴⁹ This division facilitates information sharing amongst “prosecutors, law enforcement agencies, and the Intelligence Community” in order to more efficiently respond to threats.¹⁵⁰

A. Investigations Maintained Through FISA Warrants Sustain Better Transparency and Accountability than Warrantless Methods

FISA, and the PATRIOT ACT’s modifications to the FISC, regulate and encourage law enforcement agencies in the investigation and prosecution of persons involved in criminal acts of terrorism.¹⁵¹ The methods employed by the

warrant within the context of the fourth amendment).

¹⁴⁸ *Id.*

¹⁴⁹ Assistant Att’y Gen. John P. Carlin Delivers Opening Remarks at the Nat’l Sec. Div. 10 Year Anniversary Conf., (Sept. 14, 2016), 2016 WL 4773001

¹⁵⁰ *Id.*

¹⁵¹ In Re: **** Applicant for Sec. Clearance, ISCR Case No. 04-00540 (Jan. 5, 2007).

intelligence sphere, to ensure our safety, are subject to various FISA mandated oversights.¹⁵²

The PATRIOT ACT's modifications to FISA further support the role of the court to provide judicial oversight for the increased foreign intelligence efforts stemming from the September 11 terrorist attacks.¹⁵³ Nonetheless, American civil liberties remain vulnerable to expanding innovative intelligence gathering schemes.¹⁵⁴ Warrantless searches have proven constitutionally problematic,¹⁵⁵ therefore maintaining the judicial and legislative oversight currently in place and encouraging continued reform—targeted at protecting vital privacy rights—is of the utmost importance.

The court scrutinizes intelligence surveillance efforts' consistency with the Fourth Amendment.¹⁵⁶ Safeguards, maintained by the FISC, to preserve constitutionally protected privacy rights include: scrutinizing the permissibility of the particular intelligence purpose; scrutinizing the procedures' reasonableness under the limitations of the Fourth Amendment; mandating a “significant purpose” for any collection of electronic communications; and minimization procedures which serve to “minimize the acquisition, retention, and dissemination of

¹⁵² Earnest, *supra* note 70, at 3.

¹⁵³ See *In re Sealed Case*, 310 F.3d 717, 735 (FISA Ct. Rev. 2002) (holding section 1804 and section 1805 to provide the FISA court with the authority “to review the government's purpose in seeking the information”).

¹⁵⁴ See *id.*; see also Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 Stan. J. Int'l L. 69 (2015).

¹⁵⁵ See generally Meason, *supra* note 21); see generally *United States v. U.S. Dist. Court*, 407 U.S. 297 (1972) (holding the government's warrantless electronic surveillance procedures, purportedly for national security, amounted to an unreasonable, constitutionally invalid search).

¹⁵⁶ Brief for Petitioner, *Wikimedia Foundation v. NSA* (2015) (No. 5025551).

U.S.-person information.”¹⁵⁷ Proper implementation and consistency of minimization requirements is overseen by the FISC.¹⁵⁸

Through its efforts to prosecute citizens with evidence obtained in warrantless electronic investigations, the Government has clearly conveyed a desire to secure unchecked electronic surveillance.¹⁵⁹ The FISC’s review of these surveillance methods “provides prior review by a neutral and detached magistrate” strengthening the preservation of civil liberties and the Fourth Amendment.¹⁶⁰ The FISC additionally enforces implementation of procedures to maintain constitutional practices within the intelligence sphere.¹⁶¹ Where it is determined that data has been gathered from “an identifiable U.S. person or a person reasonably believed to be located in the U.S.” the court is notified.¹⁶²

An overwhelming amount of FISC criticism stems from recent modifications to the court’s structure that weaken its ability to oversee and scrutinize surveillance techniques.¹⁶³ The FISA Amendments Act of 2008 (FAA) forced substantial changes to the role of the FISC in

¹⁵⁷ Answering Br. for Pl. Appellee at 38, *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016) (No. 14-30217), 2015 WL 8988426; *see also* Br. for Pet’r, *supra* note 132..

¹⁵⁸ Brief for Petitioner, *supra* note 131.

¹⁵⁹ *See generally* Reply Brief for Petitioner, *supra* note 81, at 2. (emphasis added).

¹⁶⁰ *United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *11 (D. Or. June 24, 2014).

¹⁶¹ Redacted, 2011 WL 10947772, at *4 (FISA Ct. Nov. 30, 2011)

¹⁶² *Id.* (citing Amended NSA Minimization Procedures at 6 (§ 3(b)(5)(b)(2)(c)).

¹⁶³ “The basic framework established by FISA remains in effect today, but it has been gravely weakened by the FAA to permit the acquisition of U.S. persons’ international communications without probable cause or individualized suspicion.” Br. for Pet’r, *supra* note 81, at 5.

approving intelligence efforts.¹⁶⁴ The court's authority is narrowed within the statute to expand legally permitted surveillance¹⁶⁵ and permit the court to merely "review[] the general procedures the government proposes to use in carrying ... surveillance."¹⁶⁶ The lacking oversight, though problematic, fails to persuade the need to absolve the court entirely.

Government efforts to increase transparency and accountability have coincided with the implementation of FISA. Both Deputy Attorney General James Cole, and Attorney General Loretta Lynch addressed the Obama administration's efforts to "promote greater transparency" of the intelligence community.¹⁶⁷ Additionally, the administration mandated the Director of National Intelligence's release of reports centered on the "effectiveness of implementing reforms that balance our civil liberties with our national security needs."¹⁶⁸ Consequentially, public knowledge of intelligence practices, and avocation for modifying various procedures has stemmed from this increased transparency.¹⁶⁹

Transparency stemming from FISA and the FISC is further conveyed from the visibility of FISC litigation.¹⁷⁰ In

¹⁶⁴ Br. for Pet'r, *supra* note 79, at 5.

¹⁶⁵ *Id.*, at 5. (citing *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008),

¹⁶⁶ *Id.* (citing 50 U.S.C. § 1881a(i)).

¹⁶⁷ See Lynch *supra* note 71; see also Deputy Att'y Gen. James M. Cole Testifies Before The U.S. House Judiciary Comm., (Feb. 4, 2014), 2014 WL 408411.

¹⁶⁸ Earnest, *supra* note 70, at 3.

¹⁶⁹ See Lee Ferran, *NSA Can Access More Phone Data Than Ever*, (Oct 20, 2016), <http://abcnews.go.com/US/nsa-potentially-access-phone-data/story?id=42892417>; see also Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. TIMES, (Aug. 8, 2013), <http://nyti.ms/1E1nlsi>

¹⁷⁰ Statement By Dir. Of Nat'l Intelligence On The Declassification Of Doc. Related To The Protect America Litig., DOJ 14-971.

a previous court opinion, upholding controversial NSA directives to Yahoo!, the Executive Branch released both the court's opinion and the briefs related to the litigation to the public.¹⁷¹ The documents were made available on the Office of the Director of National Intelligence (ODNI) website.¹⁷² The public is aware of the FISC procedures and their opinions.¹⁷³

Increased awareness invites criticisms. Though public criticism may decrease with the unitization of warrantless, unchecked Executive searches for national security investigations, constitutional violations are likely to increase.

B. FISC Properly Operates as a Necessary Check on the Executive

Prior to the passing of FISA, the Executive routinely fought for unlimited power to investigate citizens without a warrant, absent judicial oversight.¹⁷⁴ The Government argued the President's "need for intelligence information with respect to threats to national security posed by so-called domestic organizations is *no less than* his need for such information with respect to threats posed by foreign ones."¹⁷⁵

The necessity of judicial oversight is demonstrated through Government attempts to present evidence, obtained

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ *Mohamud*, 2014 WL 2866749, at *11, (Declassifying FISC opinions has led to public awareness "that the court meets with senior officials at the Department of Justice to discuss information provided in the submissions.")

¹⁷⁴ See generally Reply Br. for Pet'r, *supra* note 83, at 2.(emphasis added). (note 83 is 24 Int'l Law. 1043)

¹⁷⁵ *Id.* (emphasis added)).

through warrantless “national security surveillance,” to criminally prosecute U.S. citizens.¹⁷⁶ The Government cites the Executive’s power to protect the nation to justify the broad exception to the Fourth Amendment’s warrant requirement.¹⁷⁷ Determining “no sharp and clear distinction can be drawn between ‘foreign’ and ‘domestic’ information” the Government interpretation of the recognized foreign intelligence exception is to exempt surveillance targeted at American citizens domiciled in the U.S. from Fourth Amendment limitations.¹⁷⁸ This rendered all electronic surveillance efforts, purportedly orchestrated for the purpose of “national security” exempt from any “prior judicial authorization.”¹⁷⁹

Congress sought to abate constitutional concerns promulgating from the Executive’s recognition of a “presidential authority to conduct warrantless foreign intelligence surveillance” with the drafting of FISA.¹⁸⁰ FISA mandates electronic investigations, even where aimed towards the collection of evidence related to national security, “be authorized by a warrant from a federal district judge.”¹⁸¹

FISA mandates the FISC to provide “prior judicial scrutiny” of authorizations of electronic surveillance.¹⁸² The

¹⁷⁶ See *Keith*, 407 U.S. 297, 303.

¹⁷⁷ See generally Reply Brief for Petitioner at 2, U.S. v. U.S. Dist. Court for the Eastern Dist. of Mich, 407 U.S. 297 (1972)(No. 135522) .

¹⁷⁸ Br. for Pet’r at *5, United States v. U. S. Dist. Court, 444 F.2d 651 (6th Cir. 1971) (No. 70-153), 1972 WL 135522, *aff’d*, 407 U.S. 297 (1972).

¹⁷⁹ See generally Reply Br. for Pet’r, *supra* note 83, at 2 (citing Article IV, Section 4). (cites to 24 Int’l Law 1043)

¹⁸⁰ United States v. Abu-Jihaad, 630 F.3d 102, at 121 (2d Cir. 2010).

¹⁸¹ United States v. Ning Wen, 477 F.3d 896, at 897 (7th Cir. 2007) (citing 50 U.S.C. § 1803(a) (2012)).

¹⁸² 50 U.S.C. § 1805; 18 U.S.C. § 2518; see also *In re Sealed Case*, 310 F.3d 717, 738.

constitutional validity of the FISC is most accurately conveyed through the numerous court decisions upholding the FISA requirements as constitutionally sound, and valid under the Fourth Amendment.¹⁸³

Though the FISC is continually attacked as protecting unreasonable investigatory schemes, it serves to limit the “broad authority...to gather intelligence information through electronic surveillance in dealing with domestic organizations” sought by the Executive.¹⁸⁴ The FISC serves as a check on the Executive and further provides the judicial oversight necessary for intelligence procedures to comply with the Fourth Amendment.¹⁸⁵ Further, the FISC has even served as a judicial check on warrantless foreign intelligence schemes, maintained post FISA, under the “foreign intelligence exception.”¹⁸⁶

¹⁸³ See *Abu-Jihaad*, 630 F.3d 102, at 120 (stating “all other courts that have considered the issue, both before and after enactment of the PATRIOT Act, have rejected constitutional challenges to FISA”) (citing *Ning Wen*, 477 F.3d at 898; *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir.2005); *In Sealed Case*, 310 F.3d 717, 742–46 (FISA Ct. Rev. 2002); *United States v. Johnson*, 952 F.2d 565, 573 (1st Cir.1991); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir.1987) *United States v. Cavanagh*, 807 F.2d 787, 790–92 (9th Cir.1987); *United States v. Kashmiri*, No. 09 Cr. 830–4, 2010 WL 4705159, at *3–5 (N.D.Ill. Nov.10, 2010); *United States v. Warsame*, 547 F.Supp.2d 982, 993; *United States v. Mubayyid*, 521 F.Supp.2d 125, 135–44; *United States v. Holy Land Found. for Relief & Dev.*, No. 04 Cr. 240, 2007 WL 2011319, at *5–6 (N.D.Tex. July 11, 2007); *United States v. Jayyousi*, No. 04 Cr. 60001, 2007 WL 851278, at *1 (S.D.Fla. Mar.15, 2007); *United States v. Benkahla*, 437 F.Supp.2d 541, 554 (E.D.Va.2006); *United States v. Marzook*, 435 F.Supp.2d 778, 786 (N.D.Ill.2006); *United States v. Nicholson*, 955 F.Supp. 588, 590–91 (E.D.Va.1997); *In re Kevork*, 634 F.Supp. 1002,1014; *United States v. Falvey*, 540 F.Supp. 1306, 1312 (E.D.N.Y.1982).

¹⁸⁴ See generally Reply Br. for Pet’r, *supra* note 172, at 2.

¹⁸⁵ 50 U.S.C.A. § 1881a (West 2015).

¹⁸⁶ *In re. Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

The court continues to hold—even where the FISA procedure is available to secure a warrant— particular circumstances render warrantless intelligence surveillance constitutionally valid.¹⁸⁷ This was conveyed through repeated challenges to the NSA efforts to maintain electronic internet surveillance in order to “target certain non-U.S. persons reasonably believed to be located outside the United States in order to acquire foreign-intelligence information.”¹⁸⁸ In considering these warrantless government investigations, “probable cause and necessity” were scrutinized, and the methods were determined to “resemble[] those associated with traditional warrant requirements.”¹⁸⁹

In 2007 the NSA issued directives to Yahoo! mandating the corporation to provide information believed to be effective in securing foreign intelligence.¹⁹⁰ The NSA maintained this “upstream collection” of internet communications was centered on “targets reasonably believed to be located outside the United States.”¹⁹¹ Yahoo! refused to honor the directives, and the U.S. Government initiated proceedings in the FISC to compel Yahoo!’s compliance.¹⁹² The FISC held these surveillance schemes reasonable under the Fourth Amendment, and Yahoo! was compelled to comply with the directives.¹⁹³ Though

¹⁸⁷ See *Id.* at 1009.

¹⁸⁸ Br. for Pet’r, *supra* note 132; see also *In re Directives*, 551 F.3d at 1013; see also Redacted, 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011).

¹⁸⁹ Br. for Pet’r, *supra* note 132.

¹⁹⁰ See Statement By Dir. Of Nat’l Intelligence On The Declassification Of Doc. Related To The Protect America Litig., DOJ 14-971.

¹⁹¹ *In re Directives*, 551 F.3d at 1013; see also Redacted, 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011); see also *Statement By Dir. Of Nat’l*, DOJ 14-971

¹⁹² *In re Directives*, 551 F.3d at 1013.

¹⁹³ *Id.*

controversial, this decision conveys the vitality of promulgating efficient tribunals to both preserve Fourth Amendment limitations, and provide parties with the opportunity to challenge any intrusive intelligence efforts.¹⁹⁴

Though these warrantless searches remain subject to some form of judicial scrutiny, the failure to secure a warrant, even in limited circumstances, proves increasingly problematic. Just four years following the court's approval of the intelligence gathering scheme, the court reconsidered this particular government request for electronic communication purportedly centered on foreign intelligence.¹⁹⁵ In this subsequent case, the FISC considered the reality of the NSA's "upstream collection" of multi-communication transactions (MCTs).¹⁹⁶ The Government originally maintained the constitutionality of this NSA program arguing that a "relatively small" amount of protected communication would be unintentionally acquired through the expansive data collection.¹⁹⁷

Considering "the totality of the circumstances" the court scrutinized both the "ratio of non-target, Fourth Amendment-protected communications to the total number of communications" and the amount of protected communication collected in "absolute terms" to hold the data collection inconsistent with the Fourth Amendment.¹⁹⁸

With concrete evidence of the data collected, the court determined the ratio of protected communication collected proved small in comparison to all communication intercepted by the NSA program, but the "tens of thousands of non-target, protected communications" in absolute terms

¹⁹⁴ See *Statement By Dir. Of Nat'l*, DOJ 14-971

¹⁹⁵ See Redacted, 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011)

¹⁹⁶ See *Id.*, at 26.

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

proved problematic.¹⁹⁹ The court found the collection of “a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs” amounted to an unreasonable search.²⁰⁰

*C. Completely Foregoing Warrantless Searches
Promotes Constitutionally Valid Intelligence
Gathering Procedures*

Unreasonable Executive surveillance endeavors motivated the drafting of legislation to limit the Executive’s power and enforce oversight in intelligence procedures.²⁰¹ It follows, efforts to maintain the constitutionality of intelligence gathering have increased as recent security threats perpetuate a demand for expanded surveillance.²⁰² Dissimilar from earlier administrations’ endeavors to avoid the Fourth Amendment’s limitations,²⁰³ the passing of FISA brought a continued Executive attempt to implement a “rigorous oversight regime to “maintain national security.”²⁰⁴

The Court’s majority opinion in *Katz* failed to address the constitutionality of foregoing warrants to conducted electronic surveillance where national security

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 26.

²⁰¹ See Meason, *supra* note 21.

²⁰² Setty, *supra* note 149, at 101 & n.186 (“Establishing the Privacy and Civil Liberties Oversight Board (PCLOB) was a recommendation of the 9/11 Commission Report.”)

²⁰³ See *supra*, note 10.

²⁰⁴ Deputy Att’y Gen. James M. Cole Testifies Before The U.S. House Judiciary Comm., *supra* note 162; see also Lynch *supra* note 71 (stating the administration made “protection of civil liberties and privacy a priority in the fight against terrorism.”)

was at issue.²⁰⁵ Nonetheless Justices Douglas and Brennan recognized the potential abuses inherent to an unchecked Executive power to employ warrantless investigations.²⁰⁶ Additionally the Justices stressed the need for judicial oversight, as it is unlikely Fourth Amendment rights maintain appropriate protection where “the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.”²⁰⁷

The implementation of FISA and further creation of the FISC, convey the overwhelming need to abandon the “foreign intelligence exception” to the Fourth Amendment’s warrant clause.²⁰⁸ Despite previous legislative and judicial efforts to procure constitutionally abusive surveillance methods though the passing of FISA and creation of the FISC, the “foreign intelligence exception” continues to be recognized as a reasonable “special needs” search excused from compliance with the Fourth Amendment.²⁰⁹

The oversight implemented through FISA has continued to effect reform to intelligence gathering methods employed by the Executive. Dissimilar from past administration’s continued efforts to advocate for Executive exemptions to the Fourth Amendment, post FISA administrations’ have conveyed an approach to intelligence gathering centered on “balanc[ing] our civil liberties with

²⁰⁵ *Katz v. United States*, 389 U.S. 347, at 359–60.

²⁰⁶ *Id.*

²⁰⁷ *Id.* at 360. (Justices Brennan and Douglas Concurring)(“Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be.”).

²⁰⁸ See 50 U.S.C.A. § 1801 (West 2015); see also Earnest, *supra* note 70, at 3 (discussing the FISC procedure of “review[ing] requests from intelligence professionals about tools or tactics that they intend to employ.”)

²⁰⁹ *In re. Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008).

our national security needs.”²¹⁰ The sharp deviation from earlier practices is demonstrated through the numerous Executive undertakings to increase accountability within the intelligence sphere.²¹¹ The Privacy and Civil Liberties Oversight Board (PCLOB)—created by the Obama Administration—is sustained for the sole purpose of protecting the security of the nation, while concurrently “upholding the liberties” protected by the Constitution.²¹²

The FISC needs to be altered to avoid any mere “rubber stamp” approvals, allow for advocacy of “privacy concerns” and generate a more “genuinely adversarial” procedure.²¹³ Implementing stricter scrutiny in the decisions to issue warrants for the gathering of foreign intelligence, or excluding all information obtained with a FISA “warrant” that fails to pertain to national security threats may prove beneficial to better protect civil liberties. The court continues to uphold the “foreign intelligence exception” though the abuses stemming from this exception prove the very reason for the court’s creation.²¹⁴

Following the September 11 attacks, President George W. Bush authorized the NSA’s implementation of

²¹⁰ Earnest, *supra* note 70, at 3.

²¹¹ See Lynch *supra* note 71. (discussing the creation of the Privacy and Civil Liberties Oversight Board), *see also* Deputy Att’y Gen. James M. Cole Testifies Before The U.S. House Judiciary Comm., 2014 WL 408411 (recognizing the “potential misuse” of data collected for intelligence).

²¹² See Garrett Hatch, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD: NEW INDEP AGENCY STATUS (2012) (“The PCLOB was statutorily authorized in 2007, but only became operational and fully staffed in late 2013 and early 2014, months after the Snowden disclosures.”); *see also* Setty, *supra* note 149, at n.186.

²¹³ Setty, *supra* note 149.

²¹⁴ See Meason, *supra* note 21; *see also* 50 U.S.C.A. § 1801 (West 2015)

warrantless national security surveillance.²¹⁵ The government sought approval from the FISC, following a federal district court's determination the program was unconstitutional because it exceeded the limits of the Fourth Amendment.²¹⁶ The FISC considered an additional warrantless search exception in 2007 when scrutinizing the constitutional validity of the FISA expansion that allowed for "warrantless foreign intelligence surveillance" on persons "reasonably believed" to be located outside the United States."²¹⁷ These particular intelligence methods were conducted for the purposes of obtaining "foreign intelligence information" and maintained the "minimization procedures" mandated by FISA.²¹⁸ This "upstream collection" of internet communications was argued by the NSA as "critical to Government efforts to combat international terrorism and other threats to the United States and its interests."²¹⁹

The FISC decision holding these warrantless investigations constitutionally reasonable where the intent was to protect the security of the nation proves problematic.²²⁰ Though the FISC's creation centers on the constitutionally problematic "foreign intelligence exemption," the court upheld the exception to protect warrantless investigations lacking FISC oversight.²²¹ The FISC determined the particular intelligence gathering efforts within what the Court has previously defined as "special

²¹⁵ See Br. for Pet'r, *supra* note 81, at *6.

²¹⁶ See *Id.* (citing *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006)).

²¹⁷ *In re. Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008).

²¹⁸ *Id.*, at 1010.

²¹⁹ Br. for Pet'r, *supra* note 131.

²²⁰ *In re Directives*, 551 F.3d at 1006.

²²¹ *Id.*

needs” case that maintains an exemption from Fourth Amendment limitations.²²²

The FISC’s upholding of warrantless surveillance and further the “foreign intelligence exception” stands in direct contrast to the Court’s previous rulings. Currently, the Supreme Court has never recognized “special needs” cases to include intelligence gathering efforts, maintained absent judicial oversight.²²³ Previous Court opinions holding the fear of the “erosion of our sense of privacy and independence” to far outweigh the fear that “upheaval will modify our form of government” suggest that the Court would not consider judicial oversight to “materially interfere” with these national security surveillance efforts,²²⁴ but rather that the court would consider these particular investigations to warrant the necessity of judicial oversight.²²⁵

Investigations, orchestrated through solely warrantless searches, absent judicial oversight, remain unreasonably intrusive searches under the Fourth

²²² *Id.*

²²³ *Id.*, at 1006. (citing *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (holding the warrant and probable-cause requirement impracticable for the employment of procedures to drug test high-school athletes. Considering these actions “special needs, beyond the normal need for law enforcement”)(quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873(1987)); *Skinner v. Ry. Labor Execs. Ass’n*, 489 U.S. 602, 620, (1989) (upholding the mandate for drug and alcohol testing of railroad employees for the purposes of safety as constitutional); 1011 cf. *Terry v. Ohio*, 392 U.S. 1, 23–24, (1968) (holding the frisk for weapons in the intent of securing the safety of law enforcement officers proved reasonable, and constitutionally valid absent a warrant).

²²⁴ *In re Directives*, 551 F.3d at 1006.

²²⁵ *Id.*, but see *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) (holding “the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, ‘unduly frustrate’ the President in carrying out his foreign affairs responsibilities.”

Amendment. Following the establishment of the FISC—to administer specialized judicial oversight for unique foreign intelligence procedures—the continued recognition of a constitutional exception for foreign intelligence gathering is unwarranted.

IV. CONCLUSION

Pre FISA administrations' abuse of Constitutional privacy rights conveys the vital need for judicial oversight in the intelligence sphere. An Executive exemption to the Fourth Amendment, absent any judicial oversight leaves Americans' civil liberties vulnerable. The FISC oversight, maintained through FISA warrants, provides both judicial oversight and transparency to the electronic surveillance programs employed by the intelligence sphere.

Dissimilar from previous, unchecked national security surveillance, search powers are properly narrowed through the limitations promulgated by congressional and judicial oversight of the Executive's intelligence gathering procedures. Acquisitions of communications under FISA are scrutinized by the judiciary and challengeable in the FISC.

It is vital that the FISC be maintained and that courts abandon the unreasonably intrusive, warrantless surveillance facilitated through the foreign surveillance exception. A multitude of constitutional safeguards exist to prohibit any government body's exercise of unchecked power. These safeguards convey immense doubt the Framers foresaw an exemption to the Fourth Amendment's limitations, protecting the citizenry from abusive government searches, as constitutionally valid.