Description of document:	Title of Thesis: No Need For Another Mi-5: Countering The Homegrown Terrorist Threat Through A Regulated Domestic Intelligence Surveillance Act, 2009. Released by the Office of The Director of National Intelligence (ODNI)
Requested date:	18-September-2017
Release date:	04-December-2024
Posted date:	23-December-2024
Source of document:	FOIA Request Director, Information Management Office ATTN: FOIA/PA Office of the Director of National Intelligence Washington, D.C. 20511 Email: ODNI_FOIA@odni.gov

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

3 December 2024

Reference: ODNI Case No. DF-2022-00321

This letter provides an interim response to your Freedom of Information Act (FOIA) request to the Defense Intelligence Agency (DIA), dated 18 September 2017, requesting 18 specific theses written by students at the National Intelligence University. As previously noted by DIA, DIA transferred these cases to the Office of the Director of National Intelligence (ODNI) in 2022.

ODNI processed this request under the FOIA, 5 U.S.C. § 552, as amended and located 17 of the theses requested. Note, despite a thorough search, "Rationing the IC: The Impact of Private American Citizens on the Intelligence Community" was not located.

This interim response provides a response on ten of the theses. During the review process, we considered the foreseeable harm standard and determined that certain information must be withheld pursuant to the following FOIA exemptions:

- (b)(3), which applies to information exempt from disclosure by statute. Specifically, the National Security Act of 1947, as amended:
  - Section 102A(i)(l), 50 U.S.C. § 3024(i)(1), which protects information pertaining to intelligence sources and methods; and
  - Section 102A(m), as amended, 50 U.S.C. § 3024(m), which protects the names and identifying information of ODNI personnel.
- (b)(6), which applies to information that, if released, would constitute a clearly unwarranted invasion of personal privacy.

Be advised, we continue to process your request. If you are not satisfied with this response, a number of options are available. You may contact me, the FOIA Public Liaison, at ODNI_FOIA_Liaison@odni.gov, or the ODNI Requester Service Center, at ODNI_FOIA@odni.gov or (703)-275-1313. You may also submit an administrative appeal to the Chief FOIA Officer, c/o Chief, Information Management Office, Office of the Director of National Intelligence, Washington, DC 20511 or emailed to ODNI_FOIA@odni.gov. The appeal correspondence should be clearly marked "Freedom of Information Act Appeal of Adverse Determination" and must be postmarked or electronically transmitted within 90 days of the date of this letter.

Lastly, the Office of Government Information Services (OGIS) of the National Archives and Records Administration is available with mediation services and can be reached by mail at 8601

Adelphi Road, Room 2510, College Park, MD 20740-6001; telephone (202) 741-5770; toll-free (877) 684-6448; or email at ogis@nara.gov.

Sincerely,

Erin Morrison
Chief, Information Review and Release Group
Information Management Office

This thesis has been accepted by the faculty and administration of the National Intelligence University to satisfy a requirement for a Master of Science of Strategic Intelligence or Master of Science and Technology Intelligence degree. The student is responsible for its content. The views expressed do not reflect the official policy or position of the National Intelligence University, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government. Acceptance of the thesis as meeting an academic requirement does not reflect an endorsement of the opinions, ideas, or information put forth. The thesis is not finished intelligence or finished policy. The validity, reliability, and relevance of the information contained have not been reviewed through intelligence or policy procedures and processes. The thesis has been classified in accordance with community standards. The thesis, in whole or in part, is not cleared for public release

NO NEED FOR ANOTHER MI-5: COUNTERING THE HOMEGROWN TERRORIST THREAT THROUGH A REGULATED DOMESTIC INTELLIGENCE SURVEILLANCE ACT

by

(b) (6)
Federal Bureau of Investigation
NDIC Class 2009

Submitted to the faculty of the
National Defense Intelligence College

in partial fulfillment of the requirements for the degree of
Master of Science of Strategic Intelligence

July 2009

The views expressed in this paper are those of the author and
do not reflect the official policy or position of the
Department of Defense, Federal Bureau of Investigation or the U.S. Government

ABSTRACT

TITLE OF THESIS: No Need for Another MI-5: Countering the Homegrown Terrorist Threat through a Regulated Domestic Intelligence Surveillance Act

STUDENT: (b) (6) Master of Science in Strategic Intelligence, 2009

CLASS NUMBER: NDIC 2009 **DATE:** July 2009

THESIS COMMITTEE CHAIR: (b) (6)

COMMITTEE MEMBER: (b) (6)

After September 11, 2001, the institutional failures of the Intelligence Community (IC) prompted debate about creating an American MI-5. These debates were premature when Congress has untapped legal resources available to combat terrorism. The absence of a legal framework for domestic surveillance collection, however, exposes the United States to an escalating homegrown terrorism threat. Congress must enact a Domestic Intelligence Surveillance Act (DISA) to close intelligence gaps created by legal

constraints while ensuring protection of civil liberties. This thesis seeks to answer the following question: How will the creation of DISA enable the IC to conduct domestic intelligence collection against homegrown terrorists while respecting the rights of U.S. citizens in general?

A review of the constitutional basis for domestic surveillance collection revealed that the Separation of Powers doctrine precludes the President from making unilateral domestic intelligence decisions. This is so because Congress previously enacted surveillance legislation (Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Foreign Intelligence Surveillance Act (FISA) of 1978). Thus, Congress has the sole power to enact DISA and to incorporate constitutional safeguards into DISA.

An evaluation of the history of electronic surveillance law prior to FISA's enactment revealed that the Supreme Court and Congress disfavor warrantless domestic surveillance. The Church Committee hearings in the early 1970s uncovered domestic intelligence abuses that led to the codification of FISA. Such abuses grossly violated the First and Fourth Amendments. Prior judicial review and the warrant requirement are favored because they are checks on civil liberties violations.

FISA's history rendered it an ineffective tool for domestic intelligence collection against the homegrown terrorist threat. FISA is effective as a monitoring mechanism for identified subjects, but does not facilitate the detection of terrorists. An appraisal of FISA's operation before the September 11th leads to the conclusion that FISA was riddled with systemic failures, thereby creating intelligence gaps. Post-September 11th remedial measures, such as the enacting the Patriot Act and the Lone Wolf Amendment as well as fixing "The Wall" and the primary purpose test, lead to the conclusion that FISA's

remedial measures cannot address the nascent homegrown terrorism threat. FISA continues to employ domestic surveillance for foreign intelligence purposes, but fails to target the homegrown terrorism threat.

An examination of two nodes of Islamist radicalization, the U.S. correctional system and the Internet, revealed a relationship between Islamist radicalization and the homegrown terrorism threat. Citizenship and legal residency in the United States serve as sanctuaries for radicalized individuals because surveillance laws are too rigid to identify such terrorists.

Further analysis exploited FISA's inadequacies to address the homegrown threat as it is outdated. Additionally, recent good-faith executive attempts to synchronize domestic and foreign intelligence fall short because such attempts still prohibit collection on U.S. citizens.

The foregoing findings lead to the conclusion that DISA is a constitutionally sound apparatus that is effective for targeting potential homegrown terrorists. Congress has the constitutional authority to enact DISA and can narrowly tailor DISA to protect civil liberties.

CONTENTS

ACKNOWLEDGEMENTS

This thesis is the culmination of an arduous journey, a journey I did not take alone for the past two years. I am blessed to have an infinite amount of love and support from many friends and family. They know who they are.

However, I must give special recognition to several people who not only supported me through this process, but who also inspired me to do my best. First and foremost, I send my eternal love and appreciation to my family. They have always encouraged me to pursue my academic ambitions, sometimes to their detriment. Mom, you made these past two years so memorable as you gave me temporary shelter, never-ending support, and a constant ray of sunshine. I love you always. (b) (6), (b) (6), and (b) (6) my Marathon Sisters, thank you so much for being so unselfish and allowing me to be so. The sanity checks and the little notes and e-mails of inspiration always made me smile and I always knew where to go when life got complicated. All three of you inspire me to reach for the stars (but that doesn't mean I am running in any races with you…I'll stay the cheerleader, thank you very much). (b) (6), (b) (6), and (b) (6), over the past two years, all three of you have been the gracious souls who I love and adore and who made sure that big sister never had to worry about "the little ones." (b) (6), thank you for always making me feel like I can do no wrong…it's just what I needed at those low moments. I know (b) (6) would be giving a hearty smirk and chuckle as we all knew he could never do wrong! And to our latest addition, my dearest (b) (6) I never imagined my heart could be so filled with so much love for such a little guy. Years from now, I'll relish telling you stories about how you got me through this process.

Commander (b) (6) my thesis chair, this thesis is complete thanks to you. I owe you a debt of gratitude for your guidance and patience with me during this process. You handled my stress levels with utter grace. I also thank you for narrowing the focus of this thesis and just telling me to "go for it." I now think of intelligence surveillance in a new way. You also challenged me like I have not been challenged since law school, and I am a better person for it.

(b) (6), my committee member and dear friend, thank you so much for working through this process with me. Not only did your humor and poignant "isms" push me forward, but your ability to listen allowed me to vent without repercussion. Any positive output that comes from this thesis is all a credit to you, as you are the one who came up with the grander idea for this thesis and encouraged me to research it further.

To my classmates of 2009 (and I know some of you are bound for 2010, but you are 2009 to me), all of you exposed me to worlds I never imagined. I walked into NDIC to challenge my intellectual curiosity and to meet professional colleagues from whom I could learn. Learn I did! I have made wonderful friends with whom I am forever joined. Thanks to all of you! And a special thank you to those who called, wrote, and checked in on me while completing this process. You'll never know how it sustained me.

Finally, I send a hearty thank-you to (b) (6), my supervisor, mentor, and dear friend. Your experience and insight is invaluable, but it is your support and friendship that helped me reach the finish line! Thank you always.

INTRODUCTION

Several U.S. national security laws encumber domestic collection capabilities. The Foreign Intelligence Surveillance Act (FISA), for instance, principally authorizes warrants to conduct electronic surveillance against foreign nationals located within U.S. borders. The limited scope of FISA collection, however, overlooks the inherent risks of the nascent homegrown terrorism threat. Consequently, this thesis calls for the creation of a Domestic Intelligence Surveillance Act (DISA) to combat potential terrorist acts planned by radicalized U.S. citizens. Expanding the scope of national security law to include surveillance collection against select U.S. citizens facilitates early detection of terrorist threats against the United States. That the thesis is unique is underscored by the homegrown threat, which illustrates the widening of an intelligence gap created by legal constraints.

The Issue

Congress must provide collectors and investigators with a legal predication for domestic intelligence surveillance, which is necessary to identify those who wish to do harm to the United States. The absence of a legal framework for domestic surveillance collection exposes the United States to unnecessary risk in light of an escalating homegrown terrorism threat. . Although al-Qa'ida (AQ) continues to be a centralized organization, its influence materialized into a social movement of people who grew up in and became radicalized in the United States. These homegrown extremists now pose an imminent threat. However, FISA facilitates domestic surveillance collection against only foreign nationals or entities located within the United States. Both the intelligence and

law enforcement communities need to be equipped with updated tools to detect radicalized homegrown terrorists. Creating a Domestic Intelligence Surveillance Act (DISA) that authorizes limited surveillance of U.S. citizens would provide the intelligence community (IC) with a valuable domestic collection capability.

Congress passed FISA in 1978 to provide a procedure whereby the Attorney General (AG) could conduct electronic surveillance for collecting foreign intelligence within the United States upon obtaining prior judicial authorization. Designed to limit intelligence collection of U.S. citizens, FISA statutorily limited case precedent that recognized the Executive Branch's inherent power to conduct warrantless surveillances without approval. FISA provides a statutory framework for electronic surveillance of U.S. persons when there is probable cause to believe the target is an "agent of a foreign power," and thus, FISA is useful for monitoring *known or suspected* agents of an enemy power. However, FISA fails to recognize the problem of identifying U.S. persons or residents who have been radicalized in the United States and who engage in acts of terrorism.

In 2000, Congress expanded the FISA definition of "foreign power" to include "a group engaged in international terrorism or activities in preparation therefore." (*see* 50 U.S.C. § 1801(a)(4) (2000)). Yet, investigators found that definition insufficient in the Zacharias Moussaoui investigation. A FISA application to review the computer files of Moussaoui, a non-U.S. citizen, was rejected due to the lack of an apparent tie to a terrorist group. Consequently, Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, amended the definition of "agent of a foreign power" in FISA, 50 U.S.C. 1801(b)(1), to add lone wolves. A lone wolf is a non-U.S.

person who engages in *international* terrorism. The FISA court no longer needs to connect the lone wolf to a foreign government or terrorist group, but the provision does not reach far enough. FISA collection against U.S. citizens continues to be prohibited for identifying citizens who engage in domestic terrorism plots.

This thesis will advocate that DISA provides a robust domestic intelligence collection capability necessary for combating the homegrown terrorism threat. Moreover, Congress can narrowly tailor DISA to protect civil liberties. The topic is relevant because it directly impacts the IC's ability to protect national security. Recent arguments advocate eliminating or overhauling FISA altogether, but these issues are not examined here. This thesis is limited to the efficacy of DISA as a domestic intelligence collection tool. The thesis will prove that: 1) an intelligence collection gap exists as to the homegrown terrorism threat; 2) Congress has the constitutional authority to enact DISA to address the threat; and 3) Supreme Court precedent also supports the enactment of DISA.

The Chapters

Chapter 1 begins with an overview of national security and intelligence law to frame an understanding of why DISA is necessary. Specifically, the chapter provides a constitutional framework from which to begin an assessment of domestic intelligence surveillance collection. National security responsibilities and intelligence law are rooted in the Constitution. The Executive Branch's authority to conduct intelligence activities as well as restrictions on that power derives ultimately from the Constitution. This chapter thus provides an analysis of the Separation of Powers Doctrine as it applies to national security, particularly intelligence surveillance. Together all three branches

possess the requisite powers for creating, implementing, and enforcing a comprehensive, constitutional DISA. This chapter also considers the relationship between intelligence collection and the civil liberties protections enumerated in the First and Fourth Amendments. Any analysis of domestic intelligence law necessarily requires a fundamental understanding of civil liberties.

Chapter 2 places the Separation of Powers Doctrine and electronic surveillance law into historical context. This contextual analysis includes an overall review of the major legal developments that led up to and formed the basis for the enactment of the Foreign Intelligence Surveillance Act (FISA). Major developments include seminal Supreme Court decisions, such as *Olmstead v. United States*, *Nardone v. United States*, *Irvine v. California*, *Katz v. United States*, *United States v. United States District Court (*also known as the *Keith* case). These cases are analyzed in conjunction with the presidential and congressional surveillance policies that led to Supreme Court review. A notable policy includes Congress' enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III). The Act established procedures by which the government could obtain judicial warrants that permit wiretapping in the criminal context. Finally, the chapter discusses the Church Committee, which investigated the dark history of domestic intelligence abuses that resulted from unchecked warrantless surveillance.

Chapter 3 focuses on how FISA has become an impediment to effective domestic intelligence surveillance. The chapter first discusses how FISA was the result of a great compromise between Congress, the Executive Branch, and civil libertarians to codify domestic surveillance for the purpose of collecting foreign intelligence. The chapter then

discusses FISA's applications as well as its significant hurdles prior to the attacks on September 11, 2001. Following those tragic events, Congress enacted remedial legislation to close gaping intelligence hurdles caused by FISA. Thus, the chapter discusses the Patriot Act, the Lone Wolf Amendment, "The Wall", and the primary purpose test and concludes that such remedies measures are ineffective to address the nascent homegrown terrorism threat.

Chapter 4 involves the relationship between violent Islamist radicalization and the homegrown terrorism threat. The chapter illustrates how citizenship and legal residency in the United States can serve as a sanctuary for radicalized individuals because legal roadblocks prevent intelligence and law enforcement agencies from detecting them. The chapter analyzes two nodes of radicalization, the U.S. correctional system and the Internet, to demonstrate why FISA is inadequate and why DISA is necessary to dismantle the threat.

The final chapter, Chapter 5, shows how DISA is an invaluable and necessary tool for targeting the homegrown terrorism threat. It begins by further examining FISA's inadequacies. The chapter then acknowledges recent good-faith attempts to synchronize domestic and foreign intelligence through The Attorney General's Guidelines for Domestic FBI Operations, but also explains how those attempts fall short. The chapter concludes with an analysis of the standards set forth in DISA. The proposed statute also includes constitutional and procedural safeguards to ensure that civil liberties are protected and respected in the context of domestic intelligence surveillance.

CHAPTER ONE

Overview of Law and Intelligence

Preventing a homegrown terrorism attack requires Congress to provide federal agencies with the requisite legal tools and intelligence apparatus to identify such terrorists before they strike. The U.S. Government needs a domestic intelligence surveillance law that will facilitate the detection of homegrown terrorists who wish to do harm to the United States. Advocates cannot dutifully promote intelligence reform; however, unless they understand the constitutional basis for modifying national security policy. This chapter provides that constitutional framework.

National security responsibilities and intelligence law are rooted in the Constitution. The Executive Branch's authority to conduct intelligence activities as well as restrictions on that power derives ultimately from the Constitution. This chapter thus provides an analysis of the Separation of Powers Doctrine as it applies to national security, particularly intelligence surveillance. The Separation of Powers doctrine as well as the Fourth Amendment, and to a lesser degree, the First Amendment provides the basic framework for limitations on the Executive Branch's domestic intelligence practices. To understand the limits of the government's power to conduct surveillance, one must assess the interplay between the three branches of federal government – The Executive Branch, Congress, and The Judiciary - before reaching any conclusion about the legality of domestic intelligence surveillance. All three branches have contributed to intelligence successes and failures that have created the laws in existence today. All three branches draw a line between domestic and foreign intelligence. All three branches play a role in developing, interpreting, and responding to events that have led to the creation of the

Foreign Intelligence Surveillance Act (FISA). Together all three branches possess the requisite powers for creating, implementing, and enforcing a comprehensive, constitutional Domestic intelligence Surveillance Act (DISA).

Any analysis of domestic intelligence law necessarily requires a fundamental understanding of civil liberties. This chapter also considers the relationship between intelligence collection and the civil liberties protections enumerated in the First and Fourth Amendments. Once exposed to the legal underpinnings of national security law in this chapter, advocates of intelligence reform will understand why they should appeal to Congress for such change. Congress has the authority to tailor legislation to bolster the U.S. national security apparatus while enforcing the freedoms accorded by the First and Fourth Amendments. Only Congress has the power to enact the proposed DISA. Although national security reform should not be limited to the enactment of laws, providing collectors and investigators with a legal predication for domestic intelligence surveillance is necessary. The malleable nature of the Constitution provides the framework from which Congress can construct a balanced and adaptable DISA.

The Constitution

> "In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself. A dependence on the people is no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions." - Federalist #51.[1]

[1] James Madison, "The Federalist No. 51: The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments," *Independent Journal*, February 6, 1788. http://www.constitution.org/fed/federa51.htm (accessed July 1, 2009).

Federalist #51 lays out the basic tension between the government and its people. A government needs to take the necessary steps to control the governed, but yet the people are the primary control on the government. In the United States, the relationship between the government and the people is laid out in the U.S. Constitution. The U.S. Constitution defines the government, describes how the government should be organized, and provides the government with enumerated powers. The Constitution is an adaptable document that can adjust to changing conditions inherent in human affairs and national policymaking, including deliberations about the appropriateness of electronic surveillance.

. The Constitution endures because of its dynamic and powerful nature. The basic premise of the Constitution creates a national government and divides power between the Executive, Legislative, and Judicial Branches of government.[2] The Founding Fathers created a national government with the belief that governmental authority applied to everyone throughout the nation. Yet, they also devised a government that limited the exercise of such authority.[3] That authority emanates from the Constitution, which endows the three branches of government with distinct powers and which also places restrictions on those powers.[4] Each branch is separate but coequal; yet, the workings of each are integrated as a whole.[5] The Constitution is preserved best when each branch respects both the Constitution and the proper actions and decisions of the

---

[2] Erwin Chemerinsky, *Constitutional Law: Principles and Policies*, 2nd ed. (New York: Aspen Law & Business, 2002), 1-5.

[3] *Doe v. Gonzales,* 500 F. Supp. 2d 379, 409-410 (S.D.N.Y. 2007).

[4] A discussion of the Separation of Powers doctrine appears in the following sub-chapter.

[5] *Doe v. Gonzales,* 409-410.

other branches.[6] In the context of modern terrorism, electronic surveillance, and national security, the three branches face a constitutional challenge to act together and strike a workable balance between a liberty interest in freedom from government restraint and the interest of ensuring public safety.[7]

Constitutional Powers to Collect Intelligence

Constitutional issues regarding domestic intelligence collection necessarily implicate the enumerated powers of the executive, legislative, and judicial branches. The Constitution grants each branch enumerated powers. Article I creates and vests legislative power in Congress.[8] Article II vests executive authority in the President of the United States.[9] Article III instills judicial power in the Supreme Court and such inferior courts as fashioned by Congress.[10] The Constitution, however, enumerates neither domestic nor foreign intelligence collection as a congressional power under Article I or as an executive function under Article II.[11] Instead, Congress and the Executive Branch conduct intelligence collection through their respective implied and inherent constitutional powers. Implied powers are those not specifically enumerated in

[6] *City of Boerne v. Flores*, 521 U.S. 507, 535-536 (1997).

[7] Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York: Oxford University Press, 2006), 31-32.

[8] Chemerinsky, *Constitutional Law*, 1.

[9] Chemerinsky, *Constitutional Law*, 1.

[10] Chemerinsky, *Constitutional Law*, 1.

[11] *See* U.S. Constitution. Article I and Article II.

the Constitution, but are implied through the Necessary and Proper Clause (The Elastic Clause) of the Constitution for Congress.[12]

Intelligence collection falls under the domain of both foreign affairs and war powers, two areas in which Congress and the President share authority under the Constitution.[13] The President's enumerated war and foreign affairs powers under Article II grant the President with the authority to act as Commander-in-Chief of the armed forces and to be the U.S. representative for foreign affairs.[14] Both of these powers imply a duty to protect U.S. citizens from foreign enemies. Enumerated war powers under Article I equip Congress with the power to declare war and to raise and support the army and the navy. In addition to its war powers, Congress has the power to regulate commerce with foreign nations, to provide for the common defense, to tax and spend, and to "make all laws which shall be necessary and proper for carrying into execution the foregoing powers..."[15] Thus, Congress and the President share overlapping authority regarding matters of national security and foreign affairs. This status creates an obvious tension in the national security realm.

Predictably, the Constitution's ambiguous language sets the President and Congress on a collision course to battle over who governs intelligence collection. The Supreme Court provides guidance in this area. As applied to national security and foreign affairs, the intelligence collection authority emanates from the Supreme Court's interpretation in a seminal case, *Youngstown Sheet and Tube Co. v. Sawyer (The Steel*

[12] U.S. Constitution. Article. I, §8, cl. 18.

[13] U.S. Constitution. Article I, §§ 8-9 and Article II § 2.

[14] U.S. Constitution. Article II, §§ 2-3.

[15] U.S. Constitution. Article I, § 8.

Seizure Case).[16] The *Steel Seizure Case* is influential in that it facially curbed the reach of presidential authority. The Court held that the President did not have the inherent authority to seize private property in an emergency in the absence of a specifically enumerated authority under Article II of the Constitution when Congress has opposed such a step.[17] The case arose during the Korean War when President Truman seized control over U.S. steel mills, which ceased production due to labor disputes. President Truman justified his action as a wartime measure exercised under his Article II power as Commander-in-Chief to stop a steel shortage.[18] The Supreme Court rejected this argument and noted that the president acted in contravention of Congress' earlier rejection of the legislation that would have authorized the president's actions.[19] Moreover, the Court found that Congress enacted other legislation that could address the steel shortage.[20] According to the Court, presidential authority must be found in some provision of the Constitution, which is not expressly implicated in this case. The Court also stated that such authority is not implied from the aggregate of presidential powers, especially when Congress already spoke to the issue.[21] Thus, the Court declared the presidential order unconstitutional.[22]

---

[16] *Youngstown Sheet and Tube Co. v. Sawyer (Steel Seizure Case)*, 343 U.S. 579 (1952).

[17] *Steel Seizure Case*, 582-585.

[18] *Steel Seizure Case*, 582.

[19] *Steel Seizure Case*, 585-587.

[20] Ibid. at 585-587.

[21] Ibid. at 587.

[22] Ibid. at 587-589.

Writing for the majority, Justice Hugo Black rendered a decision that appears clear and simple in design. However, five concurrent opinions further qualified the decision, which actually blurred the limits of the President's power to act unilaterally in emergencies. Justice Robert Jackson wrote the defining concurrence that is most important in a separation of powers analysis.[23] Justice Jackson grouped the presidential powers into a formulaic method to define the extent of presidential authority and circumstances under which each method applies.

Justice Jackson defined three areas that explain the scope of presidential authority when Congress has authorized, failed to act in light of, or passed legislation that is incompatible with executive actions. First, presidential authority reaches its maximum when the President acts pursuant to express or implied powers authorized by Congress.[24] Congress also may delegate some of its legislative authority to the president. Second, the President can only act upon his own independent powers in the absence of a congressional grant or denial of authority.[25] However, Justice Jackson described that situations in this instance may implicate a "zone of twilight" whereby the President and Congress share concurrent authority. Thus, congressional action or even inaction may wield its effects on independent presidential responsibilities. In those cases, the test of power likely will depend on events of the times, rather than abstract theories of law.[26]

---

[23] Stephen Dycus, Arthur L. Berney, William C. Banks and Peter Raven-Hansen, *National Security Law*, 4th ed. (New York: Aspen Publishers, 2007), 47.

[24] *Steel Seizure Case*, 637-638. (Jackson, J., concurring).

[25] Ibid. at 637-638.

[26] Ibid. The Supreme Court later addressed this second method, which illustrates how the President and Congress encounter and react to conflict in the absence of explicit presidential and in light of congressional acquiescence or indifference. In *Dames & Moore v. Regan*, then-Associate Justice William Rehnquist analyzed Justice Jackson's formula regarding the "zone of twilight" in the context of another

The third scenario finds presidential power at "its lowest ebb" when the President acts against the expressed or implied will of Congress. In those instances, the President only can act upon his own presidential powers absent Congress' constitutional powers or delegation. The only remedy available to the President is judicial intervention, which invites heightened scrutiny.[27]

The *Steel Seizure Case* did not articulate a rigid standard by which to assess presidential and congressional authority over electronic surveillance issues. However, the Court did provide guidelines and circumstances which define the limits of presidential and congressional power that apply to domestic intelligence collection. Any claim of presidential authority, for instance, would require a review of the Constitution's allocation of enumerated powers between the President and Congress. If the Constitution bars such a claim, such authority would be unconstitutional regardless of whether the President and Congress agreed to it. Furthermore, claims to presidential authority also require an examination of legislative intent to determine whether Congress previously supported such a claim or acquiesced in the President's actions. Where Congress does

---

national security matter. According to Justice Rehnquist, "It is doubtless the case that executive action in any particular instance falls, not neatly in one of three pigeonholes, but rather at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition. This is particularly true as respects cases such as the one before us, involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail." Justice Rehnquist further explored the notion of congressional acquiescence: "As we have noted, Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take or every possible situation in which he might act. Such failure of Congress specifically to delegate authority does not, "especially . . . in the areas of foreign policy and national security," imply "congressional disapproval" of action taken by the Executive. On the contrary, the enactment of legislation closely related to the question of the President's authority in a particular case which evinces legislative intent to accord the President broad discretion may be considered to "invite" "measures on independent presidential responsibility." At least this is so where there is no contrary indication of legislative intent and when, as here, there is a history of congressional acquiescence in conduct of the sort engaged in by the President." *Dames & Moore v. Regan,* 453 U.S. 668, 669, 678-679 (1981).

[27] *Steel Seizure Case*, 637-638. (Jackson, J., concurring).

not speak to the issue or indicate its will, in some cases, the President may have the authority to make unilateral decisions. However, in those rare circumstances, Congress retains its ability to encroach upon the President's unilateral decisions in those spheres where both branches share concurrent power.

As applied to electronic surveillance, Justice Jackson's framework underscores the importance of determining whether Executive Branch actions are authorized by or incompatible with the express or implied will of Congress. The result should demonstrate that Congress is the authority who must enact domestic intelligence legislation and that the President has the autonomy to enforce it within the parameters of the statute. The Supreme Court stated that Congress can regulate electronic surveillance to investigate national security threats from domestic organizations.[28] The Court has also recognized that Congress has significant foreign relations power through its foreign commerce power and national defense matters.[29] Yet, the Court also recognized the President's significant foreign affairs powers that exist independently of Congress' power. One such power includes matters of foreign intelligence. Further confusing the issue is that precedent doesn't establish to what extent the President has either independent power or plenary power.[30] With input from the Executive Branch, Congress

[28] *United States v. U.S. Dist.Ct. (Keith)*, 407 U.S. 297, 324 (1972).

[29] Richard H. Seamon, "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits," *Hastings Constitutional Law Quarterly* 35 (Spring 2008): 469-470.

[30] Plenary power is a power that has been granted to a body in absolute terms, with no review of, or limitations upon, the exercise of the power. When the President possesses plenary power, Congress cannot encroach upon or usurp that power.

attempted to remove power-sharing ambiguities associated with domestic surveillance when it enacted the Foreign Intelligence Surveillance Act (FISA) in 1978.[31]

National emergency powers illustrate how Congress limits presidential power in the domestic intelligence realm because precedent delineates legislative and congressional roles in this area. The President possesses plenary power to make necessary and immediate responses to genuine national security emergencies.[32] That power has limitations in practice, however, because the power "depends upon the legislative framework in which it is exercised."[33] First, any unilateral executive action in times of national emergency must be limited in time and scope to protect civil liberties.[34] Second, the President can defy an Act of Congress only if the defiance is necessary to respond to the national emergency. The President cannot defy the Act of Congress if the President can effectively respond to that emergency while obeying the statute.[35] Paradoxically, Congress actually has the ability to regulate the President's power by enacting legislation that gives the President the sufficient latitude to exercise the President's plenary power, but within the confines of the legislation. Thus, only when existing legislation is inadequate can the President defy an Act of Congress to respond to national emergencies.

---

[31] Chapter Two lays out the historical framework that led to the passage of FISA. Chapter Three demonstrates how FISA operates and why Congress must codify domestic surveillance intelligence legislation.

[32] Seamon, "Domestic Surveillance for International Terrorists," 480.

[33] Ibid. at 480.

[34] Ibid.

[35] Ibid.

The Executive Branch tested its emergency powers when it circumvented the FISA statute by instituting the Terrorist Surveillance Program (TSP). In 2005, journalists revealed that the U.S. government conducted warrantless surveillance on its citizens without prior judicial review.[36] The Bush Administration initially cited its inherent national emergency powers as justification for implementing the program after the attacks on September 11, 2001. As public criticism of the TSP grew, the Executive Branch claimed constitutional and statutory authorization under the President's Article II powers and the 2001 Congressional Authorization for the Use of Military Force (AUMF). The discovery of the program raised three issues: 1) whether the TSP violated FISA; 2) whether the TSP violated the Fourth Amendment; and 3) whether the President had the authority under his Article II foreign affairs powers and his inherent national emergency powers to override FISA and the Fourth Amendment.

The President's authority to authorize the TSP necessarily implicated his constitutional powers because legislation barred the President's claim to statutory authority for two reasons. First, by enacting FISA in 1978, Congress precluded any domestic surveillance outside of FISA.[37] Second, Congress almost universally rejected presidential authority under the AUMF because the term "force" cannot be reasonably construed to authorize domestic surveillance.[38] Thus, the President had to rely on his constitutional powers, which were validly reduced by FISA, to justify the TSP program.[39]

---

[36] Seamon, "Domestic Surveillance for International Terrorists," 456.

[37] Ibid. at 456.

[38] Ibid. at 457.

[39] *See previous page.* "Validly reduced" means that the President possessed plenary power to respond within the parameters defined by Congress in FISA.

Congress already defined the Executive Branch's authority within the parameters of FISA, so it appeared that the Executive Branch conducted warrantless surveillance on citizens in contravention of the FISA statute.

The Executive Branch announced in January 2007 that it would not reauthorize the TSP because such surveillance thereafter would be subject to judicial review in the Foreign Intelligence Surveillance Court (FISC), which conforms to FISA procedures.[40] However, in March 2007, a FISC judge questioned whether the government could rely on its decision when the government intercepted foreign-to-foreign communications that used facilities, such as witching stations, located on U.S. soil.[41] Congress responded and enacted the Protect America Act (PAA) in August 2007. The PAA clarified that FISA electronic surveillance did not encompass surveillance directed at a person who is reasonably believed to be located outside the United States, and thus, freed the government from obtaining FISA orders for foreign-to-foreign intercepts.[42] The PAA implicitly recognized that the President has surveillance power independent of a statutory framework, and thus, the PAA implies that the Constitution endows the President with

[40] "In January 2007, the Justice Department persuaded a judge on the Foreign Intelligence Surveillance Court (FISC) to issue orders that blessed the TSP. The orders were, and remain, secret. It appears, however, that the orders do not take the form of traditional FISA warrants issued by the FISC, for Attorney General Alberto Gonzales described them as "innovative" and "complex." He also told the Senate Judiciary Committee that the January 2007 FISC orders "authorize[e] the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agency of al Qaeda or an associated terrorist organization." Thus, according to Gonzales, these orders caused "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program" to be "conducted subject to the approval of the Foreign Intelligence Surveillance Court."" Richard H. Seamon, "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits," *Hastings Constitutional Law Quarterly* 35 (Spring 2008): 459-460.

[41] Seamon, "Domestic Surveillance for International Terrorists," 461.

[42] Ibid. at 462-463.

surveillance power. Congress' response, however, also illustrates how it has the power to define the scope of the President's surveillance power.

The history of intelligence surveillance law in Chapter Two will show how each branch exerts its authority in the national security context. The Constitution does not bar either branch from intelligence collection authority and the two branches share authority in this national security sphere. Thus, the two branches appear to operate in the "zone of twilight" described by Justice Jackson in the national security realm. However, this zone becomes restrictive in the area of domestic surveillance collection where Congress has spoken.

Given the foregoing analyses, the passage of the proposed Domestic Intelligence Surveillance Act (DISA) would require Congress to act. The *Steel Seizure Case* and the TSP program illustrate how each branch plays a role in the domestic intelligence surveillance realm. Pre-existing legislation combined with case precedent implies that Congress is the only one who can act, thereby giving the Executive Branch the latitude to enforce it.

Constitutional Rights of Americans

Even if Congress and the President agree to intelligence surveillance collection methods, they have a duty to protect the rights of the people. Another utility of the Constitution creates a mechanism to protect civil liberties. Civil liberties focus on protecting the rights of individuals. The Constitution enumerates these special freedoms in the Bill of Rights.[43]

[43] U.S. Constitution. Amendments I-X.

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 or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[44]

Domestic surveillance demands a continual check and balance system between the government's legitimate national security interests and the protections guaranteed under the Fourth Amendments. The Constitution separated the executive, legislative, and judicial powers to protect liberty.[45] One such liberty under the Fourth Amendment is the right of the people to be free from unreasonable searches and seizures.[46] Like the separation of powers doctrine, the Fourth Amendment supports legislative and judicial checks on the Executive Branch to prevent executive abuse of individual rights.[47] The separation of powers doctrine and Fourth Amendment issues also overlap when determining what the Executive Branch can and cannot do.[48] It is in Fourth Amendment jurisprudence where the Supreme Court exerts its constitutional authority regarding surveillance intelligence collection. The Court balances the government's legitimate interest in conducting surveillance against the extent of intrusion into an individual's

[44] U.S. Constitution, Amendment IV.

[45] Seamon, "Domestic Surveillance for International Terrorists," 503.

[46] Ibid. at 503.

[47] Ibid. at 466-467.

[48] Ibid. at 466.

privacy. In conducting the balancing test, the Court measures the effectiveness of Fourth Amendment guarantees by the reasonableness standard and the Warrant Clause.

The issue of whether an Executive Branch domestic intelligence policy violates the Fourth Amendment requires a reasonableness analysis that strikes a balance between governmental and individual interests.[49] Reasonableness is that point at which the government's interest advanced by a search or seizure also advances the public interest and outweighs the severity of the interference with individual liberty.[50] As applied to purely domestic intelligence surveillance, the reasonableness standard would require an analysis of whether a potentially existing homegrown terrorism threat ensures the safety of the United States and whether that threat outweighs the potential intrusiveness into an individual's privacy.

What is deemed reasonable in terms of a search and seizure derives content and meaning through reference to the Warrant Clause of the Fourth Amendment.[51] The Fourth Amendment's requirement of judicially issued warrants protects Americans from baseless searches through review by an independent judiciary. The probable cause requirement to obtain warrants also ensures that U.S. citizens are not subject to unreasonable searches and seizures.[52]

Exceptions to the warrant requirement exist in the context of electronic surveillance, thereby suggesting that a warrant is not a constitutional absolute in intelligence collection. For instance, electronic surveillance conducted under exigent

[49] Seamon, "Domestic Surveillance for International Terrorists," 466.

[50] *Illinois v. Lidster*, 540 U.S. 419, 427 (2004).

[51] Coolidge v. New Hampshire, 403 U.S. 443, 473–84 (1971).

[52] Seamon, "Domestic Surveillance for International Terrorists," 487.

national security circumstances will satisfy the Fourth Amendment even if the surveillance does not meet the traditional Fourth Amendment requirements of probable cause and prior judicial approval.[53] Moreover, before Congress enacted FISA in 1978, several courts upheld warrantless electronic surveillance for national security purposes.[54] In those cases, the courts created an exception to the Fourth Amendment warrant requirement for searches conducted for foreign intelligence purposes.[55]

The constitutional parameters of electronic surveillance are not clearly delineated despite Fourth Amendment jurisprudence. The Fourth Amendment is designed to prevent any of the three branches of government from abusing its respective authority.[56] Each branch tests that authority even in the context of the Fourth Amendment and conflicts continue between the Executive Branch and Congress regarding electronic surveillance. The Fourth Amendment originally applied to tangible things, such as people, property, and documents.[57] With the advent of electronic communications in the early twentieth-century, the Supreme Court expanded the reach of the Fourth Amendment to include conversations.[58] Moreover, the advancement of communications technology also prompted government efforts to conduct and exploit surveillance operations for both law enforcement and national security purposes. Over time, Congress created legislation that it deemed sufficient for engaging in legitimate national security and law enforcement

---

[53] Seamon, "Domestic Surveillance for International Terrorists," 487.

[54] Ibid. at 493.

[55] Ibid.

[56] Ibid. at 486.

[57] *Olmstead v. United States,* 277 U.S. 438, 465-469 (1928).

[58] *Socialist Workers Party v. United States*, 642 F. Supp. 1357, 1390 (S.D.N.Y. 1986).

purposes while protecting the privacy interests of American citizens.[59] The Supreme Court expanded the scope of Fourth Amendment protections over such surveillances. Yet, ambiguity remains about the extent to which electronic surveillance is appropriate and the extent to which such surveillance actually intrudes on civil liberty interests.

Congress must remove any remaining ambiguity by enforcing the Fourth Amendment through legislation. Congress should enact a domestic intelligence surveillance law that is durable enough to advance national security interests and responsible enough to promote civil liberties interests. Against this backdrop is where DISA is appropriate and necessary. Congress should promote extensive deliberations and should incorporate constitutional safeguards into the DISA statute to ensure respect for rights to privacy, free speech, and assembly. The FISA statute is relevant in this regard notwithstanding its inapplicability to the operational aspect of domestic intelligence collection. For instance, despite its imperfections, FISA represents Congress' careful regard to enforce the Fourth Amendment.[60] Congress studied foreign intelligence for six years prior to enacting FISA and they invited the Department of Justice into the process. Additionally, Congress can create specific standards of procedure that articulate guidelines and expectations about protecting civil liberties. These legislative standards would facilitate consistent judicial enforcement, rather than ambiguous judicial interpretation. Not only do clear standards provide a mutual understanding between all three branches of government, but also provide courts with a justification to give

---

[59] *See* Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A. §§ 1801-1862 (West 2003 & Supp. 2005) and Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20.

[60] Seamon, "Domestic Surveillance for International Terrorists," 496-498.

significant weight to well-reasoned legislation that enforces Fourth Amendment limitations and protects Fourth Amendment rights.

First Amendment

> Congress shall make no law respecting an establishment if religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right to the people peaceably to assemble, and to petition the government for a redress of grievances.[61]

Even if a domestic surveillance operation satisfies the Fourth Amendment, the U.S. government also must ensure that the surveillance does not violate the First Amendment. Domestic intelligence surveillance issues necessarily implicate the First Amendment because such surveillance may infringe upon freedoms of expression and the right to assembly. The Supreme Court has recognized that while the government has a legitimate interest in protecting national security, the interest must be weighed against the burden of an unreasonable surveillance on First Amendment rights.[62] This balancing test curbs against executive abuses.

Concerns about abuses of power are understandable given that the dark history of domestic intelligence reveals a series of domestic intelligence abuses prior to the enactment of FISA. From the 1950s to the early 1970s, federal U.S. government agencies engaged in surveillance activities under the guise of national security purposes that actually violated the First Amendment. For instance, presidential administrations from Presidents Franklin D. Roosevelt through Nixon encouraged federal agencies to conduct political intelligence. Such agencies conducted warrantless surveillance on

[61] U.S. Constitution. Amendment I.

[62] *United States v. U.S. Dist. Ct (Keith)*, 407 U.S. 297, 320-322 (1972).

members of Congress, Supreme Court Justices, and political figures, such as Martin Luther King.[63] Intelligence agencies, law enforcement agencies, and U.S. Army counterintelligence also collected information on political groups, such as the Black Panthers and Ku Klux Klan, and leveraged negative information against those groups in the interest of national security.[64] Such activities had a chilling effect on First Amendment freedoms.[65] Extensive investigations into executive abuses of power against U.S. citizens prompted Congress to exert its legislative power.

In 1978, Congress enacted FISA, thereby curbing the Executive's power over domestic surveillance for foreign intelligence purposes and the invasion of the First and Fourth Amendment rights. Congress recognized that the Executive Branch has a legitimate national security need to conduct domestic surveillances for foreign intelligence purposes. However, Congress prohibited domestic intelligence surveillance against U.S. citizens for any other purpose. No longer could the government conduct domestic intelligence surveillance on U.S. citizens without a warrant and absent a connection to a foreign entity. Congress recognized the compatibility between the First and Fourth Amendments when it incorporated the warrant requirement into FISA. First Amendment rights would be vulnerable in the absence of prior judicial review. The FISA statute specifically states that no person may be deemed an agent of a foreign

---

[63] U.S. Congress. Senate. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book II, § I, Book III, Warrantless FBI Electronic Surveillance (April 23, 1976), *available at:* http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book3.htm (last visited March 1, 2009) {hereinafter *Final Senate Report*}.

[64] *Final Senate Report.*

[65] *Final Senate Report.*

power based solely on activities protected by the First Amendment.[66] Therefore, to obtain a FISA warrant, the U.S. government cannot establish probable cause solely based on a U.S. person's association with a particular political group or a U.S. person's rhetoric. In FISA, Congress thus created a secure framework that would allow the executive branch to conduct legitimate electronic surveillance for foreign intelligence purposes.

Congress also has the ability to develop similar legislation for domestic intelligence purposes, but thus far, has failed to act. Enacting the proposed Domestic Intelligence Surveillance Act (DISA) would not unduly infringe upon First Amendment freedoms if Congress narrowly tailored the scope of DISA. For instance, prior to initiating any surveillance, Congress may require the U.S. government to articulate facts that ensure domestic surveillance activity is not solely predicated on First Amendment activity. Congress can once again refine domestic intelligence surveillance activities while protecting First Amendment freedoms. Congress has the authority to tailor legislation to bolster the U.S. national security apparatus while enforcing the freedoms accorded by the First Amendment.

Constitutional Power Struggles and DISA

A careful reading of Chapter Two will reveal that Congress and the Executive Branch are historically in a constant state of flux regarding their respective powers regarding intelligence surveillance collection. The Executive Branch generally contends that conducting intelligence surveillance is a purely executive function and claims broad authority for intelligence collection. Conversely, Congress generally claims authority

[66] "The Foreign Intelligence Surveillance Act of 1978," 50 U.S.C. § 1805(a)(3)(A) (2000).

over such national security issues and seeks to impose restrictions on the Executive Branch's intelligence collection activities.

Congress did just that when it asserted authority over the domestic surveillance intelligence realm with the passage of FISA and the Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III). The President, therefore, is restricted by statutory authority from creating a domestic intelligence program that directly contravenes Congress' actions and intent. Yet, Congress did not reach far enough given the problems associated with modern-day terrorism and the homegrown terrorism threat. The FISA and Title III statutes address domestic surveillance issues that center on proactive boundary-based threats and reactive criminal conduct. Neither statute comprehensively addresses proactive targeting of domestic threats, thereby leaving open a dangerous intelligence gap.

The U.S. Government has the authority to create domestic intelligence surveillance legislation that is constitutional and narrowly tailored to respect civil liberties. However, as illustrated by the TSP debate, the President's authority is not extensive enough to make unilateral domestic intelligence decisions. Yet, the absence of congressional legislation invites continual debate until Congress steps in to act. Only Congress can close the intelligence gaps created by the lack of a domestic intelligence surveillance mechanism. Congress must once again exert its authority in the national security sphere and enact DISA to ensure the safety of American citizens.

CHAPTER 2

The Waxing and Waning of 20th Century Intelligence Law Before FISA

A careful review of the history of electronic surveillance law is required before delving into any advocacy of domestic intelligence reform. To understand how the statute can be changed, one must first understand all the developments that led up to and formed the basis for FISA. The statute addresses domestic surveillance in the context of both foreign and domestic intelligence policy. This chapter reviews the history of electronic surveillance law up to the enactment of the Foreign Intelligence Surveillance Act in 1978.

Pre-World War II Domestic Intelligence Policy

Intelligence and law enforcement surveillance policies necessarily demanded attention in the early twentieth century with the increasing use of wiretaps. Wiretaps existed in the early twentieth century at the time the world witnessed the birth of the Federal Bureau of Investigation (FBI) in 1908. The original policies of both the FBI and the Department of Justice (DOJ) prohibited any use of wiretapping.[67] Conversely, the Treasury Department used wiretaps to prosecute crimes related to the Volstead Act's prohibition on liquor sales and possession as well as other domestic crimes.[68]

[67] *Socialist Workers Party v. United States*, 642 F. Supp. 1357, 1390 (S.D.N.Y. 1986) (explaining the history of FBI's original policies as to wiretapping).

[68] G. Jack Benge, Jr., "Partners in Crime: Federal Crime Control Policy and the States, 1894-1938" (Ph.D. diss., Bowling Green State University, December 2006), 352-63.

In 1928, the Supreme Court expanded the scope of domestic intelligence when it ruled on the constitutionality of wiretaps in *Olmstead v. United States*.[69] Roy Olmstead, a bootlegger, was convicted of violating the National Prohibition Act, which federal authorities discovered from wiretaps of Olmstead's phone. Authorities placed those wiretaps on lines that ran outside of Olmstead's home. At trial, Olmstead sought to have his conviction overturned based on a violation of his Fourth Amendment rights. The Supreme Court disagreed and found that telephone wiretaps on phone lines placed outside of Olmstead's house did not constitute a search or seizure, and thus, did not violate the Fourth Amendment.[70] Writing for the Court, Chief Justice Taft reasoned that the Fourth Amendment only protects "persons, houses, papers, and effects."[71] Conversations did not qualify as any of those protected entities.[72] Although courts could not prohibit such wiretaps by expanding the reach of the Fourth Amendment, the Court acknowledged that Congress could bar wiretaps as evidence in federal criminal trials.[73]

The *Olmstead* decision and administrative changes likely influenced the executive branch to change the course of history in the law enforcement realm. The Bureau of Prohibition, a sub-agency of the Treasury Department, merged with the FBI in 1930. The Bureau of Prohibition continued its previously authorized use of wiretaps despite the FBI's policy against it. The merger resulted in an eventual policy change at both the FBI and the DOJ: wiretapping would be allowed upon approval by the FBI Director as well

---

[69] *Olmstead v. United* States, 277 U.S. 438 (1928).

[70] *Olmstead,* 438..

[71] Ibid.

[72] Ibid. at 465-469.

[73] Ibid. at 465-466.

as the Attorney General.[74] However, in reversing the FBI and DOJ policy against electronic monitoring of domestic targets, Attorney General William Mitchell limited the use of wiretaps to "cases involving…espionage and other cases considered to be of major law enforcement importance."[75]

All three branches of government engaged in an interpretative struggle following the change in FBI-DOJ policy. Congress spoke to the electronic surveillance issue and acted upon the *Olmstead* Court's proposition by passing the Federal Communications Act of 1934.[76] The law prohibited all unauthorized and nonconsensual interception as well as disclosure of all electronic communications.

The DOJ developed its own interpretation of the Act as it continued to use wiretaps because the DOJ did not believe the Act applied to government situations. The DOJ took the position that wiretapping would be illegal only if three conditions are met: the government 1) intercepted a communication; 2) disclosed the communication; and 3) disseminated the information to some person outside of the Executive Branch.[77] Thus, the DOJ believed that interception and disclosure within the Executive Branch did not violate the statute.

Predictably, DOJ's permissive interpretation of the Act prompted review by the Supreme Court in *Nardone v. United States* in 1937.[78] Although the Court recognized the

---

[74] *Socialist Workers Party v. United States*, 642 F. Supp. 1357, 1390 (S.D.N.Y. 1986) (explaining the history of FBI's original policies as to wiretapping).

[75] Jason A. Gonzalez, "Article, Essay and Note: Constitutional Aspects of Foreign Affairs: How the War on Terror Has Changed the Intelligence Gathering Paradigm," *Naval Law Review* 51 (2005): 292.

[76] Federal Communications Act, 47 U.S.C. § 151 (1934).

[77] *Socialist Workers Party,* 1390.

[78] *Nardone v. United States*, 302 U.S. 379 (1937).

tension that exists between balancing strict criminal law enforcement and a citizen's right to privacy, the Court nevertheless held that the Act prohibited electronic wiretapping and barred wiretaps as evidence at trial[79] Moreover, in 1939, the Court ruled in *Nardone v. United States* (*Nardone II*) that the Act also expressly forbade the government from using the fruits of wiretap evidence at trial.[80] Attorney General Jackson subsequently suspended wiretap use throughout the DOJ, but the suspension did not last very long.

The Executive branch leveraged judicial silence into policy. In 1940, President Franklin D. Roosevelt instructed Attorney General Jackson to approve electronic surveillance on domestic targets for national security purposes.[81] The President reasoned that the *Nardone* Court did not intend to apply its decision to grave matters involving the defense of the nation.[82] The assertion was timely given global events prior to U.S. involvement in World War II, and President Roosevelt noted that foreign powers were engaging in sabotage and anti-American activities within the United States. Accordingly, President Roosevelt re-instituted electronic surveillance in order to secure potentially adverse information that might affect national security interests. However, these operations were to be limited insofar as possible to aliens who could be potential spies.[83]

---

[79] *Nardone v. United States*, 302 U.S. 379 (1937).

[80] *Nardone v. United States,* 340-342.

[81] *Socialist Workers Party*, 1390.

[82] Ibid.

[83] Ibid.

This policy remained in place for several years throughout and immediately after World War II.[84]

A New Era of Peacetime Intelligence Policy

Post-World War II intelligence policy choices reflect a national peacetime security environment. Following World War II, Congress re-focused its attention to policies that treated national security interests as an expression of political power. Congress passed the National Security Act of 1947, which reorganized the armed forces, the Intelligence Community (IC), and foreign policy entities.[85] The Act mandated a major reorganization of the foreign policy and military establishments of the U.S. Government, and thus, resulted in the creation of the Department of Defense (DoD), the Joint Chiefs of Staff, National Security Council (NSC) in the Executive Branch, and the Central Intelligence Agency (CIA).[86] A notable aspect of the Act codified an accountability structure for intelligence activities.[87] Still, nothing in the Act expressly prohibited or encouraged electronic surveillance.

Warrantless electronic surveillance gained prominence as fears of Communism emerged in the 1950s. Similar to the pre-World War II concerns about subversive

---

[84] *See Socialist Workers Party v. United States*, 642 F. Supp. 1357, 1390 (S.D.N.Y. 1986) ("In 1946 President Truman affirmed the policy of having the FBI use wiretaps in cases 'vitally affecting domestic security.' A similar policy developed regarding the FBI's use of microphone surveillance – *i.e.*, this technique could be used to protect against persons or entities thought to be subversive of the national security.").

[85] National Security Act, ch. 343, Title I, § 103 (1947) (currently codified as 50 U.S.C. § 403-3(d)(1)(2004)).

[86] National Security Act, ch. 343, Title I, § 103, et seq. (1947) (currently codified as 50 U.S.C. § 403-3(d)(1)(2004)).

[87] National Security Act, ch. 343, Title V, §§ 501-507 (1947) (currently codified as 50 U.S.C. §§ 413-415 (2004)).

activity, the Executive Branch determined that the ability to monitor communications of Cold War domestic targets was paramount. Attorney General Brownell advocated warrantless surveillance as an important intelligence tool for national security purposes and determined that the U.S. government should not be restricted from using it.[88] Brownell argued that barring law enforcement from confronting subversives about their communications was unreasonable, especially when subversives could freely use U.S. communications systems to continue unlawful activity.[89] Brownell did not seek unbridled use of warrantless surveillance, however. He believed that the Attorney General should be the central coordinating entity that determined the appropriate circumstances for applying warrantless surveillance to a case.[90]

Fifteen years after its *Nardone* ruling, the Supreme Court moved closer toward holding warrantless wiretapping unconstitutional when the Court restricted the Executive Branch from conducting warrantless surveillance in *Irvine v. California.*[91] Although not a traditional wiretap case, the issue involved police officers entering the defendant's home and placing microphones throughout the house in order to capture the defendant's incriminating statements.[92] The Court held that surreptitious installation of bugs and eavesdropping devices violates a criminal defendant's Fourth Amendment rights.[93]

---

[88] Jason A. Gonzalez, "Article, Essay and Note: Constitutional Aspects of Foreign Affairs: How the War on Terror Has Changed the Intelligence Gathering Paradigm," *Naval Law Review* 51 (2005): 294.

[89] William P. Rogers, "The Case for Wire Tapping," *Yale Law Journal* 63 (April 1954): 796.

[90] Jason A. Gonzalez, "Constitutional Aspects of Foreign Affairs,"294.

[91] *Irvine v. California*, 347 U.S. 128 (1954).

[92] *Irvine*, 131.

[93] Ibid. at 132-134.

However, on a pro-prosecutorial note, the Court also stated that courts are not required at trial to exclude evidence obtained by such means.[94]

The Executive Branch expanded its warrantless surveillance prowess through its interpretation of the *Irvine* decision. The DOJ interpreted the ruling as only applying to domestic criminal cases. Responding specifically to the *Irvine* ruling, Attorney General Brownell once again framed the warrantless surveillance issue against the backdrop of intelligence and national security interests. He claimed that warrantless surveillance techniques must be allowed for the FBI's domestic intelligence and national security apparatus.[95] Thus, the DOJ policy of allowing telephone wiretaps for national security purposes remained in place while the recognition of microphone surveillance as a national security tool materialized.[96] The policies would not remain free from debate, however.

As the Executive Branch expanded its policies in the 1950s and 1960s, several subordinate agencies engaged in practices circumventing AG Brownell's precedence establishing the Attorney General as the central point of authority for warrantless electronic surveillance. For example, a foreshadowing of Fourth Amendment controversy is embodied in the National Security Agency's (NSA) watch list program. In the early 1960s, the NSA instituted a watch list from which the NSA culled information

---

[94] Gonzalez, "Constitutional Aspects of Foreign Affairs," 294.

[95] *Socialist Workers Party,* 1391 (S.D.N.Y. 1986) (Attorney General Memorandum to the FBI Director assessing the weight of the *Irvine* case regarding national security investigations).

[96] In 1954, when Attorney General Brownell issued a sweeping authorization for microphone surveillance, which included instances of physical trespass and which did not require the Attorney General's approval in cases where surveillance was in the national interest. The policy continued until 1965, when microphone surveillance was placed on equal footing with telephone surveillance, and thus, the policies for both of these forms of surveillance remained identical since that time.

from the communications of domestic targets, interpreted the signals from the intercepts, and provided related intelligence to other agencies. The watch list, which contained approximately one thousand names, targeted American citizens and organizations who purportedly participated in questionable and potentially subversive activity. Such targets included those who participated in the anti-war and civil rights movements.[97] The NSA did not seek prior approval from the Attorney General, which was contrary to Attorney General Brownell's original intent of a centralized approval mechanism for warrantless surveillance. For many years, Attorneys General were unaware of the NSA watch list.[98] Yet, as discussed in this chapter, the NSA watch list program is neither the first nor the last domestic intelligence program that escaped centralized oversight.

In the mid-1960s, the Johnson Administration instituted a self-regulating policy that effectively placed limits on the use of domestic warrantless surveillance. Specifically, President Johnson issued a directive that prohibited government personnel from intercepting nonconsensual telephone communications.[99] The president viewed the interception of such communications as a highly intrusive invasion of privacy. Importantly, President Johnson carved out a noteworthy exception to his directive. He

---

[97] Gonzalez, "Constitutional Aspects of Foreign Affairs," 295.

[98] U.S. Congress. Senate. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book II, § I, Book III, Warrantless FBI Electronic Surveillance (April 23, 1976), *available at:* http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book3.htm (last visited March 1, 2009) {hereinafter *Final Senate Report*}.

[99] *Final Senate Report*.

authorized the government to collect nonconsensual communications for matters related to national security, but only upon written approval of the Attorney General.[100]

The Supreme Court ruled on the constitutionality of warrantless surveillance when it reversed the *Olmstead* decision in the seminal case, *Katz v. United States.*[101] The Court found that the FBI's warrantless wiretap of a public phone booth violated the defendant's Fourth Amendment rights. In *Katz*, the government attached an electronic recording device to the outside of a public telephone booth and listened to Charles Katz' conversations. Evidence from those recordings resulted in Katz's conviction. According to the Court, "the Fourth Amendment protects people, not places" and private conversations unintended for public broadcast are constitutionally protected.[102] The Court reversed Katz's conviction.[103] Had the government sought judicial review prior to the surveillance, the Court noted that a neutral magistrate could have properly authorized the surveillance because it was so narrowly focused.[104] Consequently, the *Katz* Court further held that warrantless surveillance violates the Constitution when the government conducts such searches without the prior judicial sanction and appropriate safeguards such as those found in the Fourth Amendment's warrant requirement.[105]

Despite the restrictive holding, the Court expressly reserved the question of national security surveillance. Relying upon the Fourth Amendment's reasonableness

---

[100] *Final Senate Report*.

[101] *Katz v. United States*, 389 U.S. 347 (1967).

[102] *Katz,* 351-352.

[103] Ibid. at 359.

[104] Ibid. at 354.

[105] Ibid. at 356-358.

requirement, Justice White stated in a concurring opinion that national security surveillances should be free from the warrant procedure.[106] However, he also cautioned that such surveillances are reasonable only if the President of the United States or the Attorney General considered the elements of national security purposes and that either the president or his chief legal officer authorized surveillance as a reasonable method to protect the nation.[107] Thus, the Supreme Court left open the question of whether cases involving national security issues required a judicial warrant.

Following the *Katz* holding, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[108] The Act established procedures by which the government could obtain judicial warrants that permit wiretapping in the criminal context. In order to initiate surveillance under Title III, for instance, Section 2518(1)(b), (3)(a) of the Act requires the government to articulate probable cause to believe that an individual is committing, has committed, or is about to commit a particular criminal offense, and that "particular communications concerning that offense will be obtained."[109] Significantly, the Act criminalized all wiretaps initiated outside of the Act, but Congress still left open the degree to which national security surveillances would or would not fall within the Act's reach.

Similar to the Supreme Court in *Katz*, Congress avoided the national security applications of electronic surveillance. Instead, Section 2511(3) of the Act stated that

---

[106] *Katz,* 363-364.

[107] Ibid. at 364.

[108] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20.

[109] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20.

neither the Omnibus Crime Control Act nor the Federal Communications Act of 1934 shall limit the constitutional powers of the President in certain areas:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143, 47 U.S.C. 605) shall limit the constitutional powers 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. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.[110]

Although the Act provided a statement that acknowledged the existence of the President's constitutional power, it failed to define the scope of such power in the context of national security surveillance. Once again, judicial silence as well as the lack of congressional guidelines prompted the President and the rest of the Executive Branch to define and implement its own policies as to warrantless electronic surveillance in the national security realm. Thus, without specific language that addressed national security concerns, the Executive Branch reasonably viewed the restrictions contained in the Act as applicable to matters that did not involve national security concerns.

The Omnibus Crime Control Act obliged the DOJ to comply with the warrant procedures defined in the statute as to criminal cases, but left open the question of how to apply warrantless electronic surveillance in national security matters. The Act prohibited

[110] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511 (3).

neither the DOJ procedures for warrantless wiretaps that required prior written authorization of the Attorney General, nor the subsequent reauthorization after 90 days of such surveillance. Moreover, the Act did not forbid the DOJ policies of national security warrantless surveillance if the surveillance met one or more of the following criteria:

1. That it is necessary to protect the nation against actual or potential attack or any other hostile action of a foreign power;

2. That it is necessary to obtain foreign intelligence information deemed essential to the security of the United States;

3. That it is necessary to protect national security information against foreign intelligence activities;

4. That it is necessary to protect the United States against the overthrow of the Government by force or unlawful means; or

5. That it is necessary to protect the United States against a clear and present danger to the structure or the existence of its Government.[111]

One could construe the fourth and fifth criteria to facilitate warrantless surveillance in the context of today's homegrown terrorism threat given the intent to attack the homeland. However, actions subsequent to the Omnibus Crime and Control Act further hampered intelligence capabilities within the United States. Subsequent precedents and policies make apparent that both Congress and the Supreme Court failed to contemplate the possibility of homegrown terrorism or how to disrupt such activity.

Electronic surveillance for domestic security purposes requires a judicial warrant, according to the Supreme Court in the landmark case *United States v. United States District Court (*also known as the *Keith* case).[112] Decided in 1972, the *Keith* case recognized that the President's power is broad when applied to collecting foreign

[111] *Final Senate Report.*

[112] *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972).

intelligence. The *Keith* case evolved after the United States charged three individuals with conspiracy to destroy government property and also charged one of the individuals with bombing an office of the Central Intelligence Agency (CIA) in Ann Arbor, Michigan. Defense attorneys requested disclosure of all electronic surveillance, but the Attorney General claimed he was not required to disclose sources because he authorized the wiretaps pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The United States District Court for the Eastern District of Michigan disagreed and ordered disclosure of the surveillance. The government appealed, but the appellate court upheld the lower court order. Thus, the use of domestic surveillance against domestic threats became the central issue to be decided before the Supreme Court.

The Court recognized that "successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees without guidance from the Congress or a definitive decision of this Court." [113] Additionally, the *Keith* Court acknowledged that the *Katz* Court left open the question of whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in situations involving the national security.[114] The *Keith* Court answered the question and drew a bright line in domestic intelligence cases. Weighing the government duty to protect domestic security against the potential danger posed by unreasonable surveillance to individual privacy and free expression, the Court held that the Omnibus Crime Control and Safe Streets Act does not constitute a grant of power to the President with respect to

[113] *Keith*, 299.

[114] Ibid. at 309.

domestic surveillance.[115] However, the "Act does not attempt to define or delineate the powers of the President to meet domestic threats to the national security."[116] The Court also established an important precedent by holding that the government must obtain a judicial warrant prior to implementing electronic surveillance against domestic organizations even when domestic security issues are at stake. The precedent still controls today, and *Keith* is the last case in which the Supreme Court spoke to the issue.

Despite the apparently restrictive *Keith* ruling, the Court did not entirely preclude warrantless surveillance in domestic security cases. Warrantless surveillance that is impermissible in domestic security cases may be constitutional when such surveillance connects a target to a foreign power.[117] Moreover, the Court recognized that additional procedures apart from judicially approved warrants could be "compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the

---

[115] *Keith*, 315-320.

[116] Ibid. at 322.

[117] *Keith*, 309. (*see FN 8:* "Section 2511(3) (of Title III) refers to 'the constitutional power of the President' in two types of situations: (i) where necessary to protect against attack, other hostile acts or intelligence activities of a 'foreign power'; or (ii) where necessary to protect against the overthrow of the Government or other clear and present danger to the structure or existence of the Government. Although both of the specified situations are sometimes referred to as 'national security' threats, the term 'national security' is used only in the first sentence of s 2511(3) with respect to the activities of foreign powers. This case involves only the second sentence of s 2511(3), with the threat emanating-according to the Attorney General's affidavit-from 'domestic organizations.' Although we attempt no precise definition, we use the term 'domestic organization' in this opinion to mean a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies. No doubt there are cases where it will be difficult to distinguish between 'domestic' and 'foreign' unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case." *See also FN 20*: "For the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved, see *United States v. Smith,* 321 F.Supp. 424, 425-426 (CDCal.1971); and American Bar Association Project on Standards for Criminal Justice, Electronic Surveillance 120, 121 (Approved Draft 1971 and Feb. 1971 Supp. 11). See also *United States v. Clay*, 430 F.2d 165 (CA5 1970).")

Government for intelligence information and the protected rights of our citizens."[118] The *Keith* Court recognized that "exact targets of such surveillance may be more difficult to identify" and stated "Congress may wish to consider protective standards for…[domestic security] which differ from those already prescribed for specified crimes in Title III."[119] Despite the warrant requirement for domestic security cases, such a statement suggests that the Court would be amenable to non-criminal domestic intelligence surveillance provided Congress enacted legislation that contained the appropriate safeguards.

Congress and the Supreme Court embraced a less permissive stance on warrantless surveillance in the 1960s and 1970s, an era clouded in suspicious intelligence activity. According to his concurring opinion in *Keith*, for example, Justice Douglas expressed that "we are currently in the throes of another national seizure of paranoia, resembling the hysteria which surrounded the Alien and Sedition Acts, the Palmer Raids, and the McCarthy era. Those who register dissent or who petition their governments for redress are subjected to scrutiny by grand juries, by the FBI, or even by the military."[120] Such an assertion is not entirely without merit when assessed against events described below.

Domestic Intelligence Goes to Church

Events in the early 1970s marked an era of scandal. At the time, the United States epitomized a nation in crisis as the unpopularity of the Vietnam War reached its precipice

[118] *Keith*, 322-323.

[119] Ibid. at 322-323.

[120] Ibid. at 329.

and the far-reaching scandals of Watergate emerged. Executive intelligence activities became the focus of congressional and media inquiries. For example, Christopher Pyle wrote a 1970 article about military intelligence abuses after he discovered in the late 1960s that the U.S. Army spied on civilians.[121] In the late 1960s, Pyle served in the Army and taught law at the Army's intelligence school at Fort Holabird, Maryland.[122] One of his classes focused on CONUS intelligence and spot reports, the Army's shorthand for intelligence in the continental United States.[123] While compiling teaching materials, Pyle learned that the Army's CONUS intelligence section regularly developed reports from some fifteen hundred Army operatives about anti-war activists and demonstrations with twenty people or more. Pyle's story prompted hearings by Senator Sam Ervin, and as a result of the scrutiny, the Army soon shut down its domestic surveillance efforts.[124] The Senate held similar hearings just a few years later as Watergate revealed questionable intelligence operations, including those run by the FBI, CIA, and other agencies. These hearings eventually resulted in the initial passage of FISA in 1978.

Only in the wake of the Watergate scandal and the resignation of President Nixon did Congress and the public gain insight into the scope of domestic intelligence abuse. The days of minimal congressional oversight over the Executive Branch abruptly ended as allegations of abuse escalated in the public. Chaired by Senator Frank Church of

---

[121] *See* Christopher H. Pyle, "CONUS Intelligence: The Army Watches Civilian Politics," *Washington Monthly* I, January 1970, 4; reproduced in *Congressional Record,* 91st Cong., 2nd sess., 2227-2231.

[122] Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (New York: Free Press, 2005), 17-20.

[123] O'Harrow, *No Place to Hide,* 17-20.

[124] Ibid. at 17-20.

Idaho in 1975, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("The Church Committee") investigated the U.S. government's history of domestic intelligence abuses. The Church Committee conducted hundreds of interviews and examined thousands of documents to assess the extent to which U.S. intelligence agencies participated in illegal intelligence activities.[125] The Committee determined that the FBI, the CIA, and other agencies conducted intrusive and often unnecessary surveillance of politicians, religious organizations, women's rights advocates, anti-war groups, and civil liberties activists. Such violations necessarily implicated First and Fourth Amendment concerns in constitutionally protected areas, such as the right to free speech, the right to freedom of assembly, and the right to privacy. As applied to warrantless surveillance, the Committee opined that abuse reached its maximum when the government conducted surveillance against American citizens and domestic organizations.[126] Despite legitimately stated predicates in some instances, intelligence agencies unfairly targeted Americans who posed no national security threat and who violated no criminal law.[127]

Properly authorized warrantless surveillance against foreigners is unreasonable when such surveillance results in possible abuses against American citizens, according to the Committee. When properly applied, intelligence information can provide decision makers with much needed information about risks to national security. The Church Committee found, however, that intelligence agencies also warped intelligence to

[125] O'Harrow, *No Place to Hide*, 18.

[126] *Final Senate Report.*

[127] *Final Senate Report.*

influence politics.[128] Although foreign agents and entities are legitimate targets for electronic surveillance, any conversations that the foreign targets held with American citizens incidentally could implicate information irrelevant to the purpose of the foreign surveillance.[129] Moreover, the Committee found that the government obtained essentially political information unrelated to the surveillance and subsequently disseminated that information to senior administration officials. For example, Attorney General Robert F. Kennedy legitimately authorized electronic surveillance of foreign targets suspected of engaging in unlawful attempts to influence congressional discussions over sugar quota legislation for their respective governments. Not only did surveillance provide the Attorney General with information about likely foreign influence, but also revealed the reactions of the House Agriculture Committee to the Kennedy Administration's sugar quota proposal.[130]

The Church Committee findings revealed intelligence abuses that permeated throughout U.S. government agencies nationwide. For example, FBI headquarters developed over 500,000 domestic intelligence files and the FBI opened 65,000 domestic intelligence files in 1972.[131] However, the FBI was not alone. The Church Committee assembled ominous statistics that revealed the extent to which the government infringed upon the civil rights of American citizens:

---

[128] Peter P. Swire, "The Future of Internet Surveillance Law Symposium: A Symposium to Discuss Internet Surveillance, Privacy, and the USA Patriot Act; Surveillance Law: Reshaping the Framework," *George Washington Law Review* 72 (August 2004): 1320.

[129] *Final Senate Report.*

[130] *Final Senate Report.*

[131] *Final Senate Report.*

- The CIA opened and photographed nearly a quarter million first class letters in the United States from 1953-1973. The CIA used the results to produce a computerized index of almost one and one-half millions names.

- The National Security Agency (NSA) obtained millions of private telegrams sent from, to, or through the United States from 1947-1975. The NSA accomplished this mission through secret arrangements with three U.S. telegraph companies.

- The U.S. Army created intelligence files on an estimated 100,000 Americans throughout the 1960s up to 1971.

- The Internal Revenue Service (IRS) opened intelligence files on more than 11,000 individuals from 1969-1973. The IRS also initiated tax investigations based on political criteria, rather than tax purposes. For instance, the IRS conducted tax investigations on Vietnam War protestors on the basis of their protesting status.

- The FBI maintained a list of at least 26,000 individuals to be rounded up should a national emergency occur.[132]

The statistics appear more worrisome when assessed against the circumstances under which intelligence abuses occurred. For example, the Committee discovered that administrations from Presidents Franklin D. Roosevelt through Nixon sometimes encouraged government agencies to conduct political intelligence. Such agencies conducted surveillance on members of Congress, Supreme Court Justices, and political figures.[133] Another case in point involves the FBI counterintelligence program, commonly known as COINTELPRO. Originally designed to disrupt groups and neutralize individuals who posed a threat to national security, COINTELPRO cast a wide net in its targeting strategies throughout the 1960s and early 1970s. Examples of targets include the Ku Klux Klan, the Black Panthers, and Martin Luther King.[134] The program

[132] *Final Senate Report.*

[133] *Final Senate Report.*

[134] *Final Senate Report.*

also tried to create "paranoia endemic" as it targeted speakers, teachers, writers, and publications that reportedly espoused messages antithetical to the government.[135] Such activities had a chilling effect on First Amendment freedoms. The Church Committee concluded that the most basic harm arising out of such intelligence operations involved the harm to the values of privacy and freedom which the Constitution seeks to protect.[136]

A Summary Segue to FISA

The history of pre-FISA electronic surveillance illustrates many of the problems and concerns that arise when a government attempts to collect information on its own people. Prominent throughout this history is the tension that exists between all three branches of government on the role surveillance plays in both the domestic and foreign intelligence realm. National security surveillance law has its origins in Fourth Amendment jurisprudence regarding law enforcement wiretaps. Traditionally, the Executive Branch operated with broad authority and little congressional oversight in the foreign intelligence realm. Early in the twentieth century, the Executive Branch asserted an inherent authority to authorize warrantless national security wiretaps. At first, the Supreme Court held that such wiretaps were constitutional.

Over time as the Executive branch sought to expand its warrantless wiretap authority, the Court ruled the Fourth Amendment required judicial warrants for both domestic security and law enforcement wiretaps. The Court recognized that the President's foreign intelligence power is broad, but the Court didn't articulate standards

---

[135] *Final Senate Report*

.

[136] *Final Senate Report.*

of foreign intelligence collection that would or would not be required by the Fourth Amendment, leaving that task for Congress. After the world became aware of how the government circumvented the law by conducting domestic security surveillances under the pretext of national security purposes, Congress responded by enacting the Foreign Intelligence Surveillance Act of 1978, thereby changing the course of domestic and foreign intelligence practices. Congress incorporated the principles outlined in this chapter into FISA, making it the sole authority for intelligence surveillance within the United States.

CHAPTER 3

The Foreign Intelligence Surveillance Act (FISA) of 1978

Congress tried to resolve the complex issues with regard to intelligence surveillance within the United States by passing FISA. To appreciate the necessity of a DISA statute, one must first understand how FISA has become an impediment to effective domestic intelligence surveillance. When it enacted FISA, Congress did not anticipate the transnational, globalized nature of the current threats that endanger national security. Patchwork legislative remedies following the September 11th attacks closed intelligence gaps in the FISA statute in the foreign intelligence realm, but did nothing to address domestic intelligence needs. This chapter demonstrates the applications of FISA and considers why Congress should pass domestic intelligence legislation to close the intelligence gaps that FISA leaves open.

The Great Compromise

The history of electronic surveillance in the United States evolved from domestic intelligence abuses and culminated in the Foreign Intelligence Surveillance Act (FISA). In 1978, Congress passed FISA, which established protocols for securing a court order authorizing electronic surveillance in national security intelligence investigations. The statute represented a great compromise between proponents and opponents of warrantless surveillance.[137] Supporters gained congressional approval expressly authorizing foreign intelligence wiretaps that would not meet the requirements of traditional Fourth

[137] Peter P. Swire, "The Future of Internet Surveillance Law Symposium: A Symposium to Discuss Internet Surveillance, Privacy, and the USA Patriot Act; Surveillance Law: Reshaping the Framework," *George Washington Law Review* 72 (August 2004): 1306-71.

Amendment searches. Critics gained a congressionally institutionalized system of checks and balances on the Executive Branch's overarching discretion to conduct warrantless surveillance.[138]

The challenge in any legislation regarding intelligence surveillance is to strike a balance between national security interests and individual civil liberties. After the abuses of the 1970s, Congress was determined to enact law regulating foreign intelligence surveillance. Neither the Ford nor Carter Administrations objected to this congressional oversight of the Executive Branch with regard to FISA.[139] Indeed, the Executive Branch actually collaborated with Congress due to political pressure arising from the disclosure of intelligence abuses. In addition, the Executive Branch feared judicial encroachment upon its wiretapping power.[140] By cooperating with Congress, the Executive hoped to limit further judicial restrictions on its wiretapping authority.

The FISA statute is limited in scope in that FISA surveillance requires a foreign nexus, but does not address domestic surveillance absent a foreign nexus. Congress authorized electronic surveillance against "foreign powers," which included "foreign governments or any component thereof," a "faction of a foreign nation," or a "foreign based political organization, not substantially composed of United States persons."[141] Congress also contemplated the statute's application to the national security concerns of today as the foreign power definition also included a "group engaged in international

---

[138] Swire, "The Future of Internet Surveillance Law Symposium," 1308.

[139] Richard Henry Seamon and Willaim Dylan Gardner, "The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement," *Harvard Journal of Law and Public Policy* 28 (2005): 336-337.

[140] Seamon and Gardner, "The Patriot Act and the Wall," 333-34.

[141] "Foreign Intelligence Surveillance Act," 50 USC § 1801(a)(1),(2),(5) (2000).

terrorism or activities in preparation therefore."[142] The statute further characterized international terrorism as: 1) violent actions that violate criminal laws; 2) intent to influence a government policy by intimidation; and 3) actions that transcend national boundaries.[143]

The FISA statute further hamstrings domestic surveillance collection by according U.S. persons special status. The foreign intelligence focus of the FISA statute draws an important distinction between U.S. persons and non-U.S. persons.[144] The distinction grew out of the Church Committee's concern with domestic intelligence surveillance abuses. Congress fashioned stricter surveillance standards for U.S. persons than for non-U.S. persons. The FISA statute considers U.S. persons as agents of a foreign power only if they knowingly participated in foreign power activities that "involve or may involve a violation of the criminal statutes of the United States."[145] Thus, in order to get a wiretap, not only must the government show a nexus between a U.S. person and a foreign power, but it also must demonstrate that the targeted U.S. person intended to act in concert with that foreign power. In this scenario, FISA is unworkable for the purpose of domestic intelligence surveillance. Such surveillance necessarily would focus on U.S. persons, thereby eliminating any special status. Congress must commit to developing a domestic surveillance law that promotes the U.S. Government's legitimate interest in preventing homegrown terrorism attacks and prevents infringement of civil liberties.

---

[142] "Foreign Intelligence Surveillance Act," 50 USC § 1801(a)(4) (2000).

[143] "Foreign Intelligence Surveillance Act," 50 USC § 1801(c) (2000).

[144] "Foreign Intelligence Surveillance Act," 50 USC § 1801(i) (2000).

[145] "Foreign Intelligence Surveillance Act," 50 USC § 1801(b)(2)(A) (2000).

The FISA Formula

With the passage of FISA, Congress focused on FISA's application to domestic elements of international terrorism. Congress failed to incorporate, however, processes that acknowledged the potential for homegrown terrorism and the need to identify such terrorists. Congress enacted FISA in the spirit of *Keith*, the case where the Supreme Court limited warrantless surveillance in domestic security wiretaps. In *Keith*, the Supreme Court invited Congress to develop a new mechanism for the oversight of domestic national security surveillance.[146] With FISA, Congress responded. However, the congressional response was limited to national security surveillances tied to foreign agents and power. Congress did nothing to alleviate the U.S. Government's inability to identify homegrown terrorists.

Congress made clear its intent to limit domestic surveillance to a foreign nexus when it prescribed specific procedures to obtain a FISA order. To initiate FISA surveillance, the government must submit a FISA application, which is first approved by the Attorney General and then later submitted to the Foreign Intelligence Surveillance Court (FISC) for approval.[147] The applications must specify: 1) the identity of the target; 2) the basis for the government to believe the target is a foreign power or agent of a foreign power; 3) evidence that the facility of surveillance is used or expected to be used

---

[146] *United States v. U.S. Dist. Court (Keith),* 407 U.S. 297, 321-322 (1972); *see also* Chapter Two, infra.

[147] "Foreign Intelligence Surveillance Act," 50 USC § 1804(a) (2000). Another player in the FISA application process is the Department of Justice's Office of Intelligence (OI), formerly known as the Office of Intelligence Policy and Review (OIPR). In the 1970s, the Justice Department assumed oversight over the FBI, and specifically, the Office of Intelligence Policy and Review (OIPR), policed FISA applications upon the enactment of FISA. The OI acts as the gatekeeper of FISA applications prior to submission to the Attorney General.

by the foreign power or agent of a foreign power; 4) an explanation of the minimization procedures to be used; 5) a general description of the information expected to be obtained from surveillance; and 6) certification from a high-level branch official that a purpose of the surveillance is to acquire foreign intelligence information.[148] If the government establishes probable cause to believe that the target of surveillance is an agent of a foreign power and the court deems the FISA application complete, the FISC judge will issue a FISA order.[149]

Title III versus FISA

When enacting FISA, Congress treated domestic surveillance as two mutually exclusive kinds of surveillance and failed to account for viable intelligence scenarios in which the two kinds of surveillance merged. Rather than address surveillance in the overall national security realm in FISA, Congress authorized two kinds of domestic electronic surveillance: traditional criminal law enforcement surveillance and foreign intelligence surveillance. Title III procedures apply to crimes and domestic security wiretaps, and FISA applies only to agents of a foreign power.[150] The 1978 standards remain in place today in that Title III and FISA "shall be the exclusive means by which

[148] "Foreign Intelligence Surveillance Act," 50 USC §§ 1804(a)(3)(4)(A)(B)(5)(A)(6)(7) (2000). In 2004, Congress passed the Lone Wolf Amendment, which expanded the definition of agent of a foreign power to include non-U.S. persons who act independently of a foreign power. The Lone Wolf Amendment is discussed, supra, Chapter 3 in "Congressional and Executive FISA Actions in a Post 9/11 World." Minimization procedures are imposed on government investigators to ensure that they "minimize the acquisition and retention, and prohibit the dissemination" of information collected that does not have foreign intelligence value." 50 U.S.C. § 1801(h). Minimization procedures are discussed throughout Chapter 3. The Patriot Act changed "a purpose" to "significant purpose" as applied to the acquisition of foreign intelligence information. The significant purpose language is discussed, supra, Chapter 3 in "Congressional and Executive FISA Actions in a Post 9/11 World" and "FISA Jurisprudence in the Wake of 9/11).

[149] "Foreign Intelligence Surveillance Act," 50 USC § 1805(a)(3)(A) (2006).

[150] *See* Chapter 2, infra, for the history of Title III.

electronic surveillance and the interception of domestic wire and oral communications may be conducted."[151] Yet, this dichotomy is not the only distinction between Title III and FISA.

Congress also failed to imagine scenarios that would necessitate a flexible standard to secure a surveillance warrant. An important difference between Title III and FISA centers on the probable cause standard. Probable cause means something different in each case. For instance, Title III requires probable cause to believe that a person "is committing, has committed, or is about to commit a particular offense."[152] Conversely, FISA requires probable cause to believe that the target of surveillance is a foreign power or an agent of a foreign power.[153] Despite the different requirements, both of these standards require particularized facts about the target and the nature of facilities to be placed under surveillance. Such standards can be problematic when trying to institute surveillance as a targeting mechanism regardless of domestic or foreign distinctions. For example, as applied to U.S. persons, a FISA judge must find probable cause only if the proposed surveillance satisfies one of four conditions:

(1) The target knowingly engages in clandestine intelligence activities on behalf of a foreign power which "may involve" a criminal law violation;

(2) The target knowingly engages in other secret intelligence activities on behalf of a foreign power under the direction of an intelligence

---

[151] Wire and Electronic Communications Interception and Interception of Oral Communications, "Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited," 18 U.S.C. § 2511(2)(f) (2000).

[152] Wire and Electronic Communications Interception and Interception of Oral Communications, "Procedure for Interception of Wire, Oral, or Electronic Communications," 18 U.S.C. § 2518(3)(a) (2000).

[153] "Foreign Intelligence Surveillance Act," 50 USC § 1805(a)(3)(A) (2000).

network and his activities involve or are about to involve criminal violations;

(3) The target knowingly engages in sabotage or international terrorism or is preparing for such activities; or

(4) The target knowingly aids or abets another who acts in one of the above ways.

Thus, the FISA probable cause standard requires the identification of an individual and requires a demonstration of intent prior to the initiation of surveillance. This requirement essentially creates a higher threshold.

The FISA statute does not support an intelligence apparatus as it is geared toward traditional criminal standards. Congress incorporated the Title III probable cause standard into certain aspects of FISA, which illustrates how FISA derives from a reactive criminal law enforcement tradition. For example, both statutes require high-level approval within the Department of Justice.[154] Minimization procedures exist in both statutes to reduce adverse effects on people incidental to the surveillance target. Both statutes also contain emergency procedures whereby the government can initiate surveillance without judicial approval, but which requires quick subsequent approval by a judge.[155] Thus, FISA draws some of its authority from statutory law enforcement practices focused on criminal action, thereby blurring any sharp lines drawn between foreign and domestic intelligence.

---

[154] The high-level approval in FISAs must come directly from the AG, and thus, the AG must authorize all FISA approvals. Although the requirement implements an accountability structure, it also creates an additional procedural hurdle at the expense of efficiency. The implication is that the FBI cannot institute national security wiretaps, thereby creating an additional step for procuring surveillance orders. This may not seem to be significant hurdle on the surface, but time-sensitive issues may become subordinate to potential backlogs as well as ongoing discussions to provide context and to justify the prioritization and urgent nature of a particular surveillance order.

[155] Swire, "The Future of Internet Surveillance Law Symposium," 1322.

FISA's Emergency Powers

The FISA statute is incapable of truly authorizing real-time surveillance under emergency conditions, particularly in a multiple threat-stream environment. The FISA statute enumerates emergency powers that appear suitable on the surface, but which still burden intelligence collection with timing and procedural roadblocks. Such a situation is untenable for both foreign and domestic intelligence surveillances.

Congress envisaged the need to respond to emergencies in real time, and thus, Congress provided legal routes for warrantless surveillance intended for quick response and prompt judicial oversight. The FISA statute permits emergency wiretaps in situations where the Attorney General (AG) reasonably determines that an emergency situation requires surveillance to begin before a FISA order authorizing the surveillance can be obtained with due diligence and that a factual basis for the surveillance exists.[156] The AG must then submit a FISA application to a judge in the FISC "as soon as practicable, but not more than seventy-two hours after the AG authorizes such surveillance."[157]

As practiced, however, FISA's emergency powers frustrate the purpose of obtaining emergency surveillance because the wait times can become too long. The Attorney General must personally determine the factual basis for an emergency FISA

---

[156] "Foreign Intelligence Surveillance Act," 50 USC § 1805(f) (2000).

[157] The FISA Amendments Act of 2008 expanded the 72-hour timing provision to one week, a provision which is scheduled to sunset in 2012. The Attorney General and the Director of National Intelligence must submit authorized targeting procedures within seven days and the FISC will make a final determination within 30 days. During this period, minimization procedures, the probable cause requirement, and reverse targeting guidelines will apply. U.S. Congress. H.R. 6304--110th Congress (2008): FISA Amendments Act of 2008, *GovTrack.us* http://www.govtrack.us/congress/bill.xpd?bill=h110-6304 (accessed June 1, 2009).

order.[158] Emergency surveillance cannot occur until the Attorney General does so. Yet, the law enforcement and intelligence communities can lose valuable and actionable intelligence while waiting for the authorization.[159] Moreover, the Attorney General can become a bottleneck because he or she may have to personally authorize dozens of such surveillances at a time.[160] The Attorney General does not uphold his or her duty unless he or she gives careful consideration to each order.

FISA also grants the President two key powers in the context of warrantless surveillance. First, the President may authorize warrantless surveillance for up to fifteen days following a declaration of war by Congress.[161] Second, in certain emergency situations, the President may authorize the Attorney General to conduct warrantless electronic surveillance for up to one year when such surveillance is directed solely at communications between or among foreign powers and no substantial likelihood that communications or content of U.S. persons will be acquired.[162] However, the Attorney General must make a certification of these conditions under seal to Foreign Intelligence Surveillance Court (FISC) and report on their compliance to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.[163]

---

[158] Richard Henry Seamon, "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits," *Hastings Constitutional Law Quarterly* 35 (Spring 2008): 488-90.

[159] Seamon, "Domestic Surveillance for International Terrorists," 488-90.

[160] Ibid. at 488-90.

[161] "Foreign Intelligence Surveillance Act," 50 USC § 1811 (2000).

[162] Stephen Dycus, Arthur L. Berney, William C. Banks and Peter Raven-Hansen, *National Security Law*, 4th ed. (New York: Aspen Publishers, 2007), 528-29.

[163] "Foreign Intelligence Surveillance Act," 50 USC § 1802(a)(2)(3) (2000).

The FISC and FISCR

Congress frustrated domestic intelligence efforts when it instituted a warrant requirement subject to judicial review under FISA. As constructed, this aspect of FISA illustrates how FISA is inadequate to address domestic intelligence needs. The warrant requirement for domestic intelligence is unnecessary because it obstructs government access to information necessary for thwarting homegrown terrorist attacks. The warrant requirement serves FISA only to the extent of FISA's effectiveness: to monitor previously identified targets tied to a foreign power.

Congress did consider the specialized nature of FISA surveillance and it created two additional Article III courts dedicated to FISA review. A unique aspect of the FISA statute involves the creation of the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR). Congress responded to the Supreme Court's suggestion in *Keith* that under the Fourth Amendment a judicial warrant might be required to conduct national security related investigations.[164] Thus, Congress created the FISC to ensure FISA applications would be subject to judicial review. The FISA statute requires the Chief Justice of the Supreme Court to designate seven District Court judges to the FISC.[165] The statute granted the FISC judges with jurisdiction to issue orders approving electronic surveillance after reaching five necessary findings. One such finding requires the probable cause standard as applied to agents of a foreign power.

[164] See Chapter 2, infra, for the *Keith* analysis.

[165] The Patriot Act later increased the number of FISC District Court judges from seven to eleven.

Under FISA, the FISCR has jurisdiction to hear appeals when the FISC denies the U.S. government's FISA application.[166] The FISCR consists of three judges named by the Chief Justice of the Supreme Court.[167] The Supreme Court theoretically assumes jurisdiction over FISCR appeals, but the Court has not yet received any certiorari applications for review of a FISCR decision.

Institutionalized Checks on the Secret Nature of FISA

The secret nature of FISA and any domestic intelligence surveillance legislation requires a system of checks and balances to protect civil liberties. Congress created institutional checks on the issuance of FISA orders to curb potential civil liberties abuses that may arise from the secret nature of intelligence operations. Congress recognized that intelligence operations against agents of a foreign power will be successful only if the government can conduct such operations in a cloak of secrecy. The FISA statute supports the secret nature of foreign intelligence by its procedures and by the necessarily *ex parte* nature of procuring FISA applications. Secret intelligence operations, however, are legitimate only to the extent that they are conducted with appropriate oversight.

The Attorney General (AG) must report to the House and Senate Intelligence Committees every six months regarding occurrences of FISA electronic surveillance. Such reports include citing a description of each criminal case in which the government used FISA information for a law enforcement purpose.[168] The AG also must submit an

[166] "Foreign Intelligence Surveillance Act," 50 USC § 1803(b) (2006).

[167] Swire, "The Future of Internet Surveillance Law Symposium," 1337.

[168] "Foreign Intelligence Surveillance Act," 50 USC § 1808 (2000).

annual report to Congress that includes the total number of FISA applications, the number of FISA extensions, and the total number of FISAs granted, modified, or denied. These combined reports provide a roadmap of the extent to which the U.S. government relies upon FISA and illustrate the rationale for instituting systemic checks on the FISA process.

The Original FISA statute

As noted, the 1978 FISA statute represented a great compromise between the Intelligence Community and civil libertarians.[169] Critics of warrantless surveillance, the civil libertarians, gained a legal standard for foreign intelligence surveillance, which required judicial review. However, critics had to give into the nuanced and necessarily secretive nature of foreign intelligence collection by accepting legal standards that diverged from traditional Fourth Amendment warrant requirements. The probable cause standard is one such example. Supporters of intelligence surveillance, mostly the Intelligence Community, also benefited from the institution of FISA. The FISA statute imbued electronic surveillance with congressional legitimacy and arguably standardized the process by which intelligence surveillance could be procured. Like the civil libertarians, however, the Intelligence Community also had to cede part if its ambition. For instance, FISA imposed bureaucratic processes that previously did not exist under the inherent authority of the Executive Branch, and thus dawned an era of procedural hurdles.

[169] Swire, "The Future of Internet Surveillance Law Symposium," 1325.

The text of the original FISA statute demonstrates that Congress intended foreign intelligence to be the purpose of FISA electronic surveillance, not the prevention or prosecution of crime. The Church Committee investigation in the 1970s revealed that the U.S. government frequently used national security concerns as a pretext to investigate varying aspects of domestic activity including domestic electronic surveillance.[170] In the wake of such revelations, Congress required certification that "the purpose of the surveillance is to obtain foreign intelligence information."[171] Although the legal principles of the FISA formula remained largely fixed between 1978 and 2001, this "purpose" language reveals how FISA operated during this timeframe.

The Role of OIPR

In the 1970s, the Justice Department assumed oversight over the FBI, and specifically, through the Office of Intelligence Policy Review (OIPR) policed FISA.[172] Previously, the FBI was able to forum shop throughout the Justice Department to secure domestic intelligence approval. However, the OIPR became the gatekeeper of all FISA applications to the FISC.[173] The intent behind requiring signatures from the intelligence

---

[170] Swire, "The Future of Internet Surveillance Law Symposium," 1325.

[171] "Foreign Intelligence Surveillance Act," 50 USC § 1804(7) (2000). Congress changed this language to "significant purpose" in the Patriot Act. The significance of this change is discussed later in the chapter.

[172] The National Security Division (NSD) of the Justice Department subsumed OIPR into its operations in 2006 and subsequently created the Office of Intelligence (OI) in April 2008. The OI is the successor to OIPR and contains three separate departments within the OI: 1) Operations; 2) Oversight; and 3) Litigation. *See* Department of Justice, "National Security Division Launches New Office of Intelligence," *Department of Justice*, April 30, 2008. http://www.fas.org/irp/news/2008/04/doj043008.html (accessed June 6, 2009).

[173] Swire, "The Future of Internet Surveillance Law Symposium," 1327.

agent, the drafting attorney, the head of the intelligence agency, and the AG relates back to the purpose of FISA:

> "All those signatures serve a purpose, to assure the federal judge sitting in the FISA court that a national security wiretap was being sought for "intelligence purposes" and for no other reason – not to discredit political enemies of the White House, not to obtain evidence for a criminal case through the back door of a FISA counterintelligence strategy."[174]

OIPR, as gatekeeper, added another procedural hurdle by creating an additional layer of approval that thwarted the efficiency of procuring a time-sensitive surveillance order. OIPR also played a role in laying the groundwork for creating "the wall" between criminal law enforcement and foreign intelligence.

"The Wall" and the Purpose Requirement

Well-reasoned and balanced domestic intelligence surveillance legislation would not oblige Congress to implement a purpose requirement. Domestic intelligence, however, would require protective minimization procedures to deter premature dissemination of U.S. person information. FISA's purpose language requires certification of a foreign nexus, a requirement unnecessary for the transparent purpose of domestic intelligence collection. Moreover, such language is inefficient and unduly hampers intelligence and investigative efforts as the history of FISA's purpose language demonstrates below.

[174] Swire, "The Future of Internet Surveillance Law Symposium," 1327. (citing from the chapter "Mary's Law" in Jim McGee & Brian Duffy, *Main Justice* 318 (1996)).

The original language of FISA required that a FISA application include a certification stating "the purpose of the surveillance is to obtain foreign intelligence information."[175] Prior to the September 11th attacks, lower courts tended to construe this language to mean that the "primary purpose" of the order must be to obtain foreign intelligence information.[176] This shift in language laid the foundation for building the now infamous "wall" between criminal and intelligence investigations. Courts that cited the primary purpose language relied upon the primary purpose test in *United States v. Truong Dinh Hung*, the seminal Fourth Circuit case that first drew the distinction between the purposes of criminal and foreign intelligence regarding wiretapping investigations.[177] In *Truong*, the court assessed the government's evidence and found that information primarily related to foreign intelligence purposes was admissible.[178] However, when the government shifted its focus from a foreign intelligence investigation to a criminal prosecution, subsequent evidence was inadmissible.[179] Thus, the admissibility of surveillance evidence in criminal court hinged on the government showing that foreign intelligence collection was the primary purpose for initiating surveillance. The primary purpose test imposed a demanding standard upon the FBI as it conducted its FISA-specific counterintelligence investigations.

---

[175] "Foreign Intelligence Surveillance Act," 50 USC § 1804(7) (2000).

[176] Cases include: 1) *United States v. Johnson*, 952 F.2d 565 (1st Cir. 1991); 2) *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984); and 3) *United States v. Megahey*, 553 F. Supp. 1180 (E.D.N.Y. 1982).

[177] *United States v. Truong Dinh Hung*, 629 F.2d 908, 916 (4th Cir. 1980).

[178] *Truong*, 915.

[179] Ibid. at 915.

Minimization procedures underscore the importance of the purpose language in FISA. Although FISA applications must demonstrate an intelligence purpose for surveillance, courts do allow FISA-obtained information to be used in criminal trials. Given the possibility that secret FISA surveillance could be disseminated in court, Congress sought to ensure that criminal investigators could not use FISA as a pretext for criminal investigations. The effect of this policy resulted in minimizing the contact between those agents who conduct foreign intelligence operations and those who investigate crime. Minimization procedures also included an information-screening wall, which required an official unrelated to a criminal investigation to review FISA information and to forward only those pieces that constituted relevant evidence. Additionally, FISA's minimization requirement mandated the creation of procedures that minimized the collection, retention, and dissemination of information regarding U.S. persons.

The Justice Department apparently tried to avoid running afoul of the primary purpose test by instituting its own minimization guidelines, thereby erecting "the wall" to protect itself. In 1995, Attorney General Janet Reno issued confidential guidelines to formalize minimization procedures for contacts between the FBI, the Criminal Division of the Justice Department, and OIPR in the context of foreign intelligence and counterintelligence investigations.[180] The guidelines placed OIPR in a central role by mandating the FBI and the Criminal Division to notify OIPR of contacts between the two

[180] Janet Reno, "Memorandum from Janet Reno, Attorney General, to Assistant Attorney General Criminal Division, FBI Director, Counsel for Intelligence Policy, and United States Attorneys." (July 19, 1995) http://www.fas.org/irp/agency/doj/fisa/1995procs.html (accessed June 25, 2009).

entities regarding foreign counterintelligence investigations.[181] The FBI also could not contact any U.S. Attorney's Office regarding foreign counterintelligence investigations without express permission from OIPR and the Criminal Division.[182] Moreover, the guidelines required OIPR to inform the FISC regarding the existence of and the basis for contacts between the FBI, the Criminal Division, and a U.S. Attorney's Office for the purpose of keeping the FISC informed about the criminal justice aspects of an ongoing counterintelligence investigation.[183]

These guidelines became unduly restrictive due to the conservative interpretation of procedures for information sharing. However, these guidelines did not occur in isolation. The misapplication of FISA evidence and the amount of significant coordination between the FBI and the Criminal Division almost jeopardized the government's prosecution against Aldrich Ames, the CIA official arrested for spying for the Soviet Union.[184] Although Ames pled guilty, the FBI sought to avoid future occurrences by ensuring compliance with the primary purpose test and by clamping down on information sharing, a measure that required FBI personnel to refrain from contacting prosecutors without permission from OIPR. Thus, Attorney General Janet Reno issued the guidelines to respond to concerns within the Department of Justice and the FBI about the use of FISA in criminal prosecutions.[185] The 9/11 Commission later criticized the

---

[181] Reno, "Memorandum from Janet Reno," (July 19, 1995).

[182] Ibid.

[183] Ibid.

[184] U.S. General Accounting Office, Report 01-780, "FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited," 13 (2001).

[185] Reno, "Memorandum from Janet Reno," (July 19, 1995).

guidelines as a further aggravation of the primary purpose test because the guidelines were "almost immediately misunderstood and misapplied."[186] The implementation of the guidelines effectively created a barrier to coordination between the FBI and the Criminal Division, thereby further reinforcing "the wall."

The original FISA statute addressed only electronic surveillance, but Congress later recognized the need to expand FISA to include additional tools usually reserved for criminal cases. Congress extended FISA's scope in 1998 to include pen registers and trap and trace devices as applied to foreign power or agents of foreign powers.[187] A pen register is an electronic device that records outgoing numbers dialed from a particular phone. Similarly, trap and trace devices records incoming numbers. The FISA statute required the government to establish reason to believe that the telephone line subject to either device was or was likely to communicate with those involved with international terrorism or an agent of a foreign power.[188]

Post-9/11 FISA

At the urging of the Bush Administration, Congress expanded the U.S. Government's FISA powers after the attacks on September 11, 2001. Congress recognized the need to increase communications within the government. Members of Congress and political commentators, for instance, lambasted the FBI and the Central Intelligence Agency (CIA) for their perceived inability to communicate with each

[186] 911 Commission. "911 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." 79 (2004).

[187] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, §601(2), 112 Stat. 2396, 2405-10 (1998).

[188] "Foreign Intelligence Surveillance Act," 50 USC § 1842(c)(3) (2000).

other.[189] Had they communicated, according to critics, these agencies could have "connected the dots" of leads and pieces of information that would have provided a complete picture.[190] But, as the foregoing FISA processes demonstrate, minimization procedures precluded the FBI from sharing within much less with external agencies. Thus, Congress sought to increase the flow of information between agencies as well as to strike down internal information-sharing barriers when it expanded the U.S. Government's FISA powers.[191]

What Congress failed to do, however, is recognize that the Executive Branch needed a more robust domestic intelligence collection tool designed to identify terrorists before they strike. The FISA statute is an effective monitoring mechanism for identified subjects tied to a foreign entity, but it does not and cannot facilitate the detection of terrorists.[192] Although well-intended, the following remedial actions will demonstrate that FISA continues to leave open a widening intelligence gap. Congress must pass legislation that equips the Executive Branch with a domestic intelligence surveillance tool to identify homegrown terrorists.

Legislative Efforts to Tear Down the Wall

Following the tragic events of September 11, 2001, Congress quickly enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to

---

[189] Ronald J. Sievert, "Patriot 2005-2007: Truth, Controversy, and Consequences," *Texas Review of Law and Politics* 11 (Spring 2007): 322-323.

[190] Sievert, "Patriot 2005-2007," 322-323.

[191] Ibid. at 322-323.

[192] Richard A. Posner, "A New Surveillance Act," *Wall Street Journal*, February 15, 2006. http://online.wsj.com/article/SB113996743590074183-search.html (accessed July 4, 2009).

Intercept and Obstruct Terrorism Act of 2001 ("The Patriot Act").[193] The Patriot Act tore down the institutionalized wall that separated foreign intelligence activities from traditional domestic crimes. Prior to the passage of the Patriot Act, the Bush Administration proposed lowering the threshold from "primary purpose" to simply "a purpose" in order to authorize a FISA wiretap.[194] Congress ultimately enacted the Patriot Act with the proviso that a "significant purpose" must exist to obtain foreign intelligence information.[195] Thus, criminal law enforcement and prosecutorial intent could be a purpose of FISA surveillance as long as a significant purpose for collecting foreign intelligence information remained. The change in purpose language effectively served as a n important first step in tearing down "the wall" and creating an information sharing environment between the law enforcement and intelligence communities. Moreover, the language acknowledges the reality that investigators and intelligence professionals cannot predict at the beginning of every investigation whether a FISA order will result in evidence of a crime, foreign intelligence, or both. .

The Patriot Act changed other aspects of FISA. For instance, the Patriot Act simplified the procedures by which the government could obtain authorization for pen registers and trap and trace devices. Rather than require reasonable belief of communications tied to international terrorism or an agent of a foreign power, the Patriot

---

[193] 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.

[194] Swire, "The Future of Internet Surveillance Law Symposium," 1330.

[195] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, §§ 203, 218, Pub. L. No. 107-56, 115 Stat. 272, 291,281.

Act authorized the use of pen registers and trap and trace devices for information that is "relevant to an ongoing investigation."[196]

Congress also authorized "roving" foreign intelligence wiretaps for the first time under the Patriot Act. As in criminal investigations, roving wiretaps allow law enforcement to target an individual not matter what system that person uses, rather than focusing on a particular phone.. This provision demonstrates that Congress recognized the need to adapt to changing technology because targets often use multiple phones, throwaway phones, or other communications facilities. Congress approved the use of roving wiretaps for law enforcement purposes in 1986.[197] Congress expanded FISA to include roving wiretaps in "circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person."[198]

The Lone Wolf Amendment

In 2004 Congress amended FISA again by expanding the definition of "agent of a foreign power" to include the lone wolf provision. Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA) permits surveillance of non-U.S. persons engaged in international terrorism without requiring evidence that links such persons to an agent of a foreign power.[199] The "Lone Wolf" Amendment gave the government

[196] "Foreign Intelligence Surveillance Act," 50 USCA § 1842(c)(2) (West 2003).

[197] Swire, "The Future of Internet Surveillance Law Symposium," 1334.

[198] "Foreign Intelligence Surveillance Act," 50 U.S.C.A. § 1805(c)(2)(B) (West 2003).

[199] Intelligence Reform and Terrorism Protection Act (IRTPA), P.L. 108-458, § 6001(a) (2004).

authority to fight against a new type of threat posed by non-U.S. persons who act independently from foreign direction.

Congress passed the Lone Wolf Amendment as a remedial measure regarding events that came to light in the wake of the September 11th attacks. In August 2001, the FBI and the Immigration & Naturalization Service (INS) arrested Zacarias Moussaoui on immigration charges as Moussaoui overstayed his visa.[200] Reasonably suspecting Moussaoui of terrorist involvement but unable to tie him to any organization, the FBI sought a FISA search warrant to examine the contents of Moussaoui's laptop computer. FISA, as it then existed, authorized such searches if probable cause existed to believe that a foreign power or agent of a foreign power owned or used the laptop.[201] Moussaoui neither qualified as an agent of a foreign power nor overtly tied to a foreign power. Lacking or believing to lack sufficient evidence to establish probable cause, the FBI did not submit a FISA application to the FISC. Thus, the Lone Wolf Amendment closed the legal gap by which nonresident alien terrorists could effectively escape FISA's reach.

Executive Efforts to Tear Down the Wall

The Executive Branch also reacted to events of 9/11 by encouraging an information sharing environment, thereby seeking to tear down any internal remnants of "the wall." On March 6, 2002, Attorney General Ashcroft approved new "Intelligence Sharing Procedures" to implement the Patriot Act's amendments to FISA.[202] The 2002

[200] Moussaoui is often referenced as the "20th Hijacker" in the September 11th attacks.

[201] "Foreign Intelligence Surveillance Act," 50 U.S.C. § 1821-1824 (2001).

[202] *In re Sealed Case (FISCR Decision)*, 310 F.3d 717, 729 (Foreign Intel. Surv. Ct. Rev. 2002).

Procedures superseded prior procedures and were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials. Thus, the new procedures superseded the 1995 Attorney General intelligence-sharing procedures that prohibited contact between the FBI and U.S. Attorney's offices without prior approval. The new procedures eliminated the "direction and control" test and allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance."[203] The guidelines, streamlined the procedures for information sharing between the FBI, the Criminal Division, and OIPR regarding FISA searches and surveillance.[204]

The Judiciary and the Wall

In March 2002, Attorney General Ashcroft filed a motion with FISC and noted that the Department of Justice adopted the 2002 Intelligence Sharing Procedures in conformity with The Patriot Act. The government proposed to follow the new procedures in all matters before the FISC. The Attorney General also asked the FISC to vacate its orders adopting the prior procedures as minimization procedures in all cases and imposing special "wall" procedures in certain cases.[205] In effect, the government

[203] *In re Sealed Case,* 729.

[204] The new guidelines combined with the passage of the Patriot Act led to the first published decisions of the FISC and FISCR. Both cases are discussed in the next sub-chapter, "FISA Jurisprudence in the Wake of 9/11."

[205] *In re Sealed Case,* 729.

asked the FISC to adopt the new procedures, thereby superseding the previous intelligence sharing procedures iterated in the 1995 Attorney General Guidelines.[206]

In its first published opinion, *In re All Matters to Foreign Intelligence Surveillance*, the FISC adopted the 2002 minimization procedures, but with modifications that essentially revamped the purpose and scope of the 2002 guidelines.[207] The FISC focused on the statutory basis for minimization procedures in rendering its decision, which effectively resulted in preserving the primary purpose test as well as "the wall." The court stated that The Patriot Act did not amend the FISA definition of minimization procedures, which required the Attorney General to create procedures:

> "…that are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." [208]

Citing prior information sharing violations under the 1995 Guidelines, the FISC suggested that relaxing the existing procedures would open the door to an increase in violations.

The FISC endorsed the "the wall" because it served as an appropriate safeguard for ensuring that the government initiated surveillance for the primary purpose of foreign intelligence. Specifically, the court wrote that the 1995 Guidelines, which implemented

---

[206] *In re Sealed Case,* 729. Interestingly, the FISC formally adopted the 1995 guidelines in November 2001 and called them "minimization procedures" to be followed by all subsequent FISA cases. Perhaps the FISC decided to adopt the older procedures in anticipation of a future litigation regarding The Patriot Act.

[207] *In re All Matters to Foreign Intelligence Surveillance (FISC Decision)*, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002).

[208] "Foreign Intelligence Surveillance Act," 50 USC §§ 1801(h)(1), 1821(4)(A) (2000).

"the wall", were "an integral part of the minimization process."[209] According to the FISC, the primary purpose of FISA surveillance must be foreign intelligence in light of FISA's mandate that the government must demonstrate the need "to obtain, produce, and disseminate foreign intelligence information."[210] Intelligence derived from surveillance later could be used in criminal prosecutions, but only if foreign intelligence collection served as the initial and primary purpose for obtaining the intelligence in the first place. The new guidelines did not create an environment in which criminal law enforcement would be barred as the primary purpose regardless of the presence of a foreign intelligence nexus. The FISC held that the March 2002 guidelines were not reasonably designed to satisfy the statutory minimization requirements, and thus, the FISC ordered detailed procedures to maintain "the wall" between foreign intelligence and criminal investigations.[211]

The FISCR Reversal

The FISCR reversed the FISC decision on appeal in *In re Sealed Case*. The Department of Justice raised three issues in that case. First, the government claimed that the pre-Patriot Act restrictions imposed upon the government via the primary purpose test found no support in either the FISA statute or its legislative history that requires foreign intelligence to be the primary purpose of FISA surveillance.[212] Alternatively, the

---

[209] *FISC Decision*, 619.

[210] Ibid. at 623.

[211] Ibid. at 625.

[212] *In re Sealed Case,* 722. ("…the supposed pre-Patriot Act limitation in FISA that restricts the government's intention to use foreign intelligence information in criminal prosecutions is an illusion; it finds no support in either the language of FISA or its legislative history."). The government did concede

government contended that the Patriot Act eliminated the primary purpose test even if the primary purpose test is construed as a legitimate construction of FISA.[213] Third, the government claimed that the primary purpose test is not required under the 4th amendment.[214]

According to the FISCR, the distinction between foreign intelligence surveillance and criminal surveillance created a false dichotomy under FISA.[215] The court rejected the FISC view that Congress contemplated some form of "the wall" when it enacted FISA in 1978.[216] Addressing the significant purpose language, the FISCR stated that the government need only show "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes" in applying for and interpreting from surveillance.[217] The court noted that the significant purpose test will be satisfied if the government realistically plans on dealing with an agent for additional purposes apart from criminal prosecution.[218] However, the court cautioned that an application should be denied "if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct – even foreign intelligence crimes – to punish the agent rather than halt ongoing espionage or terrorist activity."[219] The FISCR upheld the March

---

that several lower courts applied the primary purposes test, but the government argued that such findings rested upon faulty analysis and result in erroneous statements if not erroneous holdings.

[213] *In re Sealed Case*, 722.

[214] Ibid. at 722.

[215] Ibid. at 725-735.

[216] Ibid. at 735.

[217] Ibid.

[218] Ibid.

[219] Ibid.

2002 guidelines against both statutory and constitutional challenges.[220] The decision stands today.

FISA and Domestic Intelligence Surveillance

The contentious nature and the complexity of the FISA statute illustrate the necessity for creating a distinct and easily recognizable surveillance statute for domestic intelligence purposes. Detecting homegrown terrorists is an important, if not the most important national security concern. Congress must find a solution that, unlike FISA, is not based on borders and foreign powers. FISA cannot and has never facilitated detection of terrorists, but FISA can be fashioned to work in tandem with a domestic intelligence statute. For instance, if the purpose of initiating domestic intelligence serves to identify a potential homegrown terrorist, such identification can assist in establishing the probable cause necessary to warrant further surveillance follow-up via Title III or FISA requirements. A domestic intelligence surveillance statute is reasonable especially when the history of FISA demonstrates that surveillance statues, which implicate Fourth Amendment privacy concerns, necessarily are dynamic and adaptable. Congress can and should create a domestic intelligence surveillance statute that is similar to FISA in its monitoring function, but first allows for identifying potential terrorists based on reasonable suspicion.

Two FISA provisions suggest how Congress might create a reasonable domestic intelligence statute. The first provision involves the distinction between Title III and FISA surveillances. Justifying the distinction between Title III and FISA shows why

[220] *In re Sealed Case*, 719-20. ("…we conclude that FISA, as amended by the Patriot Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution.").

Congress should treat homegrown terrorists and the attendant intelligence needs as distinct from either Title III or FISA. A typical counterintelligence strategy illustrates the issue. In addressing national security concerns, governments typically collect information about foreign embassy employees to determine whether such employees also act as agents of a foreign power. Whether such employees are also engaged in crime or acts in preparation thereof generally is unknown prior to the initiation of surveillance. Courts in these cases would have no basis to authorize a Title III wiretap because no probable cause exists that the employee committed or is about to commit a crime. Yet, the U.S. government has a legitimate interest in procuring the information to protect national security. The FISA statute applies to such circumstances as Congress tailored the statute to authorize surveillance despite failing to meet all of the traditional Fourth Amendment warrant requirements. Similarly, Congress must develop a statute that addresses the relationship of surveillance to the homegrown terrorism threat, which does not squarely fit within the parameters of either Title III or FISA requirements that satisfy the Fourth Amendment.

The Lone Wolf Amendment also is illustrative. Congress redressed the legal gap created by the nonresident loophole whereby nonresident terrorists, such as Zacarias Moussaoui, could freely operate in the United States without legal constraint because such nonresidents could not be tied to a foreign power. Similarly, Congress must address the dangerous gap caused by the lack of standards to monitor those homegrown actors who operate freely without legal constraint by hiding behind their U.S. citizenship or permanent resident status.

CHAPTER 4

The Homegrown Terrorism Threat

Congress enacted FISA with the intent that the FISA statute would be the exclusive means by which the U.S. Government could conduct foreign and domestic intelligence surveillance within the United States. Congress did not, however contemplate the severity or unique challenged presented by the homegrown terrorism threat. The United States has experienced homeland attacks from non-Islamist, self-radicalized domestic entities, such as Timothy McVeigh and the Unabomber. In addition, Islamist radicalization in the United States now poses a similar, if not more dangerous, threat because of the transnationalization of radicalized Islamist terrorism. This chapter demonstrates how citizenship and legal residency in the United States can serve as a sanctuary for radicalized individuals because legal roadblocks prevent intelligence and law enforcement agencies from detecting them. Even without a formalized methodology, Islamist radicalization occurs as a social movement that continues to grow in the United States. Social radicalization in the United States, inspired by Al-Qa'ida (AQ), may pose more danger to the United States than does the AQ organization itself.[221] U.S. citizens who embrace the AQ social movement and who seek to act upon their beliefs are a serious threat to national security. Thus, this chapter illustrates why domestic intelligence reform is necessary to identify U.S. citizens and legal residents who wish to harm the United States. A domestic intelligence targeting tool is necessary to prevent attacks on the homeland from identified nodes of radicalization. The two most important of these nodes are identified and explained in this

[221] Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008), 13-29.

chapter. They are the U.S. correctional system and the Internet. Left unmonitored, these two nodes create an advantageous environment in which influential, radicalized rhetoric festers, thereby exposing the United States to a potentially devastating attack.

The Homegrown Islamist Phenomenon

Islamist radicalization is no longer confined to overseas training camps. Rather, after the terrorist attacks on September 11, 2001, Islamist radicalization has evolved into an expansive threat within the United States that is largely undetectable by traditional means. Radicalization in this sense involves several factors that start with religiously-inspired indoctrination and move toward violent extremism.[222] Drivers of radicalization, such as perceived discrimination, marginalization, and frustrated expectations, may heighten the susceptibility of some individuals to extremist influences.[223] Islamist-Salafi ideology is one such driver that motivates young individuals in Western countries to independently commit terrorist acts against their host countries. According to Silber & Bhatt, the ideology "guides movements, identifies the issues, drives recruitment, and is the basis for action."[224] This philosophy also creates an obligation to attack those uncommitted to the Islamist worldview. Extremists represent a fringe element within the

---

[222] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs, 2009. *Violent Islamist Extremism: Al-Shabaab Recruitment in America.* Andrew Liepman, Deputy Director of Intelligence, National Counterterrorism Center (NCTC). 111th Cong., 1st sess., 2009. http://74.125.95.132/search?q=cache:P-Xiw0OqJsgJ:hsgac.senate.gov/public/_files/031109Liepman.pdf+cause+of+radicalization&cd=16&hl=en&ct=clnk&gl=us&client=firefox-a (accessed July 4, 2009).

[223] Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism: Al-Shabaab Recruitment in America.*

[224] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2007. *The Role of Local Law Enforcement in Countering Violent Extremism.* Major Thomas Dailey, Kansas City, Missouri Police Department, Homeland Security Division, 22. 110th Cong., 1st sess., Oct. 30.

U.S. Muslim community, and thus, one should not suspect the Muslim community overall. Radicalized U.S. citizens, however, can and do commit to an extremist Islamist worldview and pose a predictable threat to national security. Thus, the U.S. Government needs tools to identify the fringe element.

The transnationalization of Islamist radicalization requires the United States to apply the lessons learned from its allies. The bombings in Madrid on March 11, 2004 and London on July 7, 2005 signaled the realization of an additional, violent Islamist threat: Islamist homegrown terrorism, not directly linked to a foreign organization. Al-Qa'ida claimed responsibility for these plans and attacks, but the terrorist actors were not under the command and control of the centralized al-Qa'ida organization.[225] Rather, local residents and citizens used al-Qa'ida as their ideological inspiration to wreak devastation in their land of residence.

Islamist radicalization fuels the homegrown terrorism threat. Radical Islam can vary by ideology, location, and socio-economic condition. In the West, radicalization occurs due to an individual's need to find a purpose, to redefine themselves in an identity that is often nurtured by radical Islam.[226] The radicalized individuals mobilize into a violent, Islamist social movement that is primarily cultivated by friendship and kinship.[227]

---

[225] U.S. Congress. Senate. *Testimony of Mitchell Silber, Senior Intelligence Analyst, New York City Police Department, before the Senate Committee on Homeland Security and Governmental Affairs.* "The Role of Local Law Enforcement in Countering Violent Islamist Extremism," Washington DC: October 30, 2007.

[226] Committee on Homeland Security and Governmental Affairs, *The Role of Local Law Enforcement in Countering Violent Extremism.*

[227] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2007. *Radicalization of Global Islamist Terrorists.* Marc Sageman, 1. 110th Cong., 1st sess., Oct. 30.

According to Marc Sageman, Senior Fellow at the Center on Terrorism, Counter-Terrorism, and Homeland Security at the Foreign Policy Research Institute, the radicalization process consists of four inter-related and recurrent prongs: 1) a sense of moral outrage; 2) a specific interpretation of the world; 3) resonance with personal experience; and 4) mobilization through networks.[228] A sense of moral outrage emerges from wide-ranging global and local triggers, such as the war in Iraq or the perception from the Muslim community that local law enforcement targets Muslims.[229] That sense of moral outage can evolve into an interpretive worldview that reflects how one feels, rather than how one thinks. Such interpretations typically occur within a cultural tradition, such as the belief that the West engages in a war on Islam. The degree to which one incorporates a cultural interpretation will be a factor in how that interpretation applies to one's personal experiences. For instance, in Europe many Muslims strongly believe that Europe discriminates on the basis of Muslim identity.[230] That worldview may be reinforced by the high unemployment rates of European Muslim males, the high percentage of Muslims counted in the unskilled labor pool, and the lack of a Muslim political presence.[231] The combination of the previous prongs may influence some young Muslims to become angry and seek like-minded individuals who share their frustrations, thereby initially establishing informal networks that can grow into something more amorphous.

---

[228] Marc Sageman, "Terrorism: What the Next President Will Face; Special Editor: Richard A. Clarke: Section Four; Overall U.S. Strategy: A Strategy for Fighting International Islamist Terrorists," *The Annals of The American Academy of Political and Social Science* 618 (July, 2008): 224-26.

[229] Sageman, "Terrorism: What the Next President Will Face," 225.

[230] Ibid. at 226.

[231] Ibid.

Homegrown Islamist Terrorism in the United States

. The 2007 National Intelligence Estimate on the Terrorist Threat to the Homeland assessed that "the United States will face a persistent and evolving threat over the next three years" and that a growing number of radical, self-generating terrorist cells that plotted attacks in Western countries signifies that a violent segment of the Western population is expanding.[232] Recent homegrown terrorism planning in the United States may be an indicator that domestic Islamist radicalization is taking hold in the United States.[233] Recent U.S. experience with homegrown incidents illustrates the diverse and pervasive nature of the threat:

- December 2006: U.S. citizen and Islamic convert Derrick Shareef (aka Talib Abu Salam Ibn Shareef) planned to bomb the Cherry Vale shopping mall in Rockford, Illinois during Christmas 2006. Shareef was not part of a centralized Al-Qa'ida plot. Rather, through the use of the Internet and e-mail, he communicated with a fellow jihadist and eventually engaged with a person Shareef thought to be a fellow believer. Fortunately, that individual was an informant who reported to federal authorities, which resulted in the eventual conviction of Shareef in 2008.[234]

- March 2007: Shareef's former roommate, U.S. citizen and former Signalman Second Class in the US Navy, Paul Hall (aka Hassan Abujihaad), intentionally compromised national security via the Internet. He exchanged e-mails with Babar Ahmad, a website administrator for Azzam Publications, which carried jihadist propaganda and which allegedly provided material support for terrorist activities. Hall provided Ahmad with classified military briefings and drawings of Navy battle groups. Hall was convicted in March 2008 of

[232] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2007. *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11.* Senator Joe Lieberman, 4. 110th Cong., 1st sess., Sept. 10.

[233] Examples of recently disrupted terrorist attack plans as well as one attack are noted below.

[234] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat.*, 2. 110th Cong., 2d sess., 2008.

providing material support to terrorists and disclosing classified national defense information.[235]

- May 2007: Six men, three of whom are legal U.S. residents, planned to attack the Fort Dix military base in New Jersey.[236] The Fort Dix probe only came to the attention of the authorities in January 2006 when an electronics store clerk gave police a copy of a customer's videotape that showed the men firing rifles and shouting Islamic battle cries. The evidence indicated that the men regularly watched and discussed Al Qaeda videos extolling violent jihad and depicting deadly attacks against U.S. forces. Five of the six were convicted on terrorism-related charges in December 2008.[237]

- May 2009: Federal authorities arrested three U.S. citizens and one Haitian for a plot to bomb two synagogues in the Bronx and to shoot down military planes at an Air National Guard base in Newburgh, New York. The arrestees are James Cromitie, David Williams, Onta Williams and Laguerre Payen. All four are Muslim converts. The men intended to fire Stinger missiles at military aircraft at the base, which is located at Stewart International Airport. They planned to leave bombs in the cars in front of the two synagogues and to subsequently retrieve cell phone-detonating devices. They then planned to attack the air base, thereby simultaneously shooting down aircraft while remotely setting off the devices in the cars.[238]

- June 2009: Carlos Bledsoe, aka Abdulhakin Muhammed, is charged with killing Pvt. William Long and injuring Pvt. Quinton Ezeagwula in a bloody rampage outside of an Arkansas military recruiting station. Raised in Memphis, Tennessee, Bledsoe converted to the Islamic faith, changed his name, and traveled to Yemen in 2007. He claimed that he conducted the

---

[235] Department of Justice, "Former Member of U.S. Navy Sentenced to 10 Years in Federal Prison for Disclosing Classified Information," www.usdoj.gov, http://www.usdoj.gov/opa/pr/2009/April/09-nsd-306.html (accessed July 3, 2009).

[236] John P. Martin, "Fort Dix Five Guilty of Conspiracy to Kill Soldiers," *New Jersey Star-Ledger*, December 22, 2008. http://www.nj.com/news/index.ssf/2008/12/shell_fort_dix.html (accessed March 20, 2009).

[237] Martin, "Fort Dix Five Guilty of Conspiracy to Kill Soldiers," December 22, 2008.

[238] Al Baker and Javier C. Hernandez, "4 Accused of Bombing Plot at Bronx Synagogues," *New York Times*, May 20, 2009. http://www.nytimes.com/2009/05/21/nyregion/21arrests.html?_r=1&scp=3&sq=terrorism%20arrests&st=cse (accessed May 25, 2009).

> attacks as an "act for the sake of God, for the sake of Allah, the Lord of all the world, and also retaliation on U.S. military."[239]

These recent examples demonstrate that homegrown terrorism within the United States is on the rise. Although, the United States has yet to experience a homegrown attack of the magnitude of Madrid or London, the United States must address the homegrown Islamist terrorism issue as a long-term threat. While the immediate threat the United States faces may be less than that of its European counterparts, U.S. policymakers should be concerned about the expansion of radicalization over the long term. Some experts claim that the radicalization process in the United States is less insidious than in Europe due to the rapid assimilation and cultural absorption possible in the United States.[240] The United States is not, however, immune.

The United States Government cannot ignore the threat of homegrown terrorism, but instead must act to implement every available tool to combat both the root causes and consequences of Islamist radicalization.

In addition, according to Robert S. Mueller, the Director of the Federal Bureau of Investigation, three trends converge to suggest that a radical and violent segment of Western Muslim population is growing: 1) the spread of radical Salafist Internet sites that proselytize religious justification for Western attacks; 2) the frequency of both violent anti-Western rhetoric and actions by local groups; and 3) the growing number of

---

[239] Associated Press, "Recruiter attack sparks homegrown terrorism fears: American convert to Islam, who was raised in Memphis, charged in shooting," *MSNBC*, June 15, 2009. http://www.msnbc.msn.com/id/31365302/ns/us_news-security (accessed June 21, 2009).

[240] Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 4.

radicalized, self-generating cells in Western countries that identify with and adhere to violent Salafi objectives.[241]

These trends tend to be influential in the radicalization process, most notably via identified nodes of radicalization. According to Charles Allen, "nodes are the conduits facilitating or supporting a person or group through the radicalization process. They may be physical institutions, virtual communities, charismatic individuals, written or recorded material, or even shared experiences."[242] Within the United States, two nodes in particular deserve special attention: 1) the U.S. correctional system; and 2) the Internet. The Intelligence Community must have the tools to target these nodes to not only identify those engaged in potential terrorist activity, but also to diminish the root causes of Islamist radicalization.

The Threat of Islamist Radicalization in U.S. Prisons

Targeted domestic intelligence surveillance could temper the expanding reach of radicalization by facilitating the identification of and targeting the operating environment of homegrown terrorists. Nowhere is the need for domestic surveillance more prevalent than within the U.S. correctional system. In radical Islam disenfranchised prisoners find a purpose. Prison radicalization is a pervasive and often incontrollable problem that could influence select prisoners to act against the U.S. government.

---

[241] U.S. Congress. Senate. *Testimony of Robert S. Mueller III, Director, Federal Bureau of Investigation before the U.S. Senate, Select Committee on Intelligence hearing on* "Current and Projected National Security Threats." (Washington DC: February 5, 2008).

[242] U.S. Congress. Senate. *Written testimony of Charles E. Allen, Assistant Secretary for Intelligence and Analysis, Chief Intelligence Officer, Department of Homeland Security, before the Senate Committee on Homeland Security and Governmental Affairs* "Threat of Islamic Radicalization to the Homeland." Charles E. Allen, 4. 110th Cong., 1st sess., March 14.

Radicalized members of the U.S. prison population will pose additional security risks unless Islamist radicalization can be sanitized or contained. The U.S. correctional population -- those in jail, prison, on probation or on parole -- totaled 7.3 million or 1 in every 31 adults in 2007.[243] Roughly 30,000 inmates convert to Islam each year in the United States.[244] These numbers combined with the fact that prisons house a violent population make the U.S. correctional system an ideal recruitment node for violent extremism. Neither Islam nor conversion is a homeland security issue by itself; but, both become a threat when driven by radical ideology. Similarly, radicalization by itself is not an issue; rather, radicalization becomes an issue when it influences others to act upon their beliefs by engaging in violence against the United States and its citizens. Only a small number of prisoners exposed to extremist influence adopt a radicalized worldview, and fewer still may emerge from the prison system with the intent to conduct terrorist activity.[245] Yet, that small percentage poses the most significant danger: a low-probability of occurrence, but a high impact in devastation. Congress must equip the U.S. Government with the necessary legal tools to identify that small percentage of homegrown terrorists.

---

[243] CNN, "Study: 7.3 million in U.S. prison system in '07," www.cnn.com, http://www.cnn.com/2009/CRIME/03/02/record.prison.population/ (accessed July 4, 2009).

[244] Jane's Islamic Affairs Analyst, "Muslim Radicals Enlisting U.S. Inmates," *Jane's Intelligence Review* (27 November 2006),
(b) (3)

[245] Greg Hannah, Lindsay Clutterbuck and Jennifer Rubin, *Radicalization or Rehabilitation: Understanding the Challenge of Extremist and Radicalized Prisoners* (Santa Monica: RAND Corporation, 2008), 15.

Identifying Targets for Domestic Surveillance in the Prison Environment

The United States will continue to produce prison-bred homegrown terrorists unless the U.S. Government adopts preventative-based surveillance programs, such as DISA, that focus on those radicalized prisoners who are likely to act upon their worldview. The government can exploit domestic surveillance in this context in two ways. First, the government should target potential Islamist extremists released from prison. Second, the government should surveil potential extremists, such as suspicious visitors or radical imams, connected to prisoners. Both of these methods require extensive cooperation and information-sharing between correctional intelligence units and external agencies tasked with conducting domestic surveillance. The reason for such coordination is due to the fact that DISA could not be used as a targeting mechanism in these instances, because of First and Fourth Amendment concerns (see Chapter 1). The government instead would only apply DISA surveillance against a predetermined target after prison intelligence units identified the target. Such a limitation would require external law enforcement and intelligence agencies to heavily rely upon the correctional system to develop leads. Thus, agencies must ensure that they educate prison intelligence units about indicators and warnings in order to identify ideal surveillance targets.

Prison intelligence units should incorporate extremist recruitment methodology into their own practices to detect and deter violent extremism. For instance, radicalization within prisons occurs when prisoners are encouraged to study extremist media or hear anti-U.S. sermons, which may be delivered by militant imams or influential prisoners.[246] Imprisoned extremists worldwide use prison for recruitment and they guide

[246] Jane's Islamic Affairs Analyst, "Muslim Radicals Enlisting U.S. Inmates."

followers through anti-Western rhetoric. Over time, the extremists distinguish between "true believers" and mere followers. Extremists encourage true believers to act upon their radicalized beliefs. Like extremist recruiters, U.S. prisons must distinguish between extremists and mere followers if officials are to identify appropriate targets for surveillance. Identifying radicalized individuals requires robust intelligence collection efforts while the prisoner is incarcerated, so that law enforcement and intelligence agencies can conduct focused and preventive surveillance.

Prison intelligence units should identify those prisoners who are susceptible to extremist recruitment as well as to isolate radical prison imams. Congress, as well as the correctional system, must allocate resources to deter radicalized extremists from using prisoners and the prison atmosphere as recruiting tools. Imams or prisoners who already are members of radicalized, violent organizations historically become influential conduits for the information and propaganda campaigns that are run by parent organizations.[247] Like good intelligence officers, extremist imams can spot and assess individuals who respond to their messages and they can guide those prisoners into extremist circles.

Prison personnel must strive to identify charismatic leaders, to monitor their interactions with other prisoners, and to share the results of such observations with the correctional system. Although such functions traditionally are reserved to law enforcement or intelligence agencies function, these external agencies simply do not have sufficient normative knowledge of or value-added access to the prison system to be effective. Prison personnel are the optimal choice as they have the appropriate access to spot and assess influential leaders within the prison.

---

[247] Hannah, Clutterbuck and Rubin, *Radicalization or Rehabilitation*, 41.

Leaders can be either fellow inmates or those who visit the prison under the guise of providing legitimate religious instruction. Charismatic leaders seek out new recruits in the prison environment where the disenfranchised find a purpose in the radical Islamist movement. Imprisoned extremists worldwide use prison for recruitment and they guide followers through anti-Western rhetoric. The correctional system must ensure that adequate screening of religious leaders coming into the prisons in order to ensure that such leaders are not actually operating in the prison to promote a brand of indoctrination that creates an unnecessary risk.[248] Such screening processes already take place in certain state systems, such as the Michigan Department of Corrections, the Florida Department of Corrections, and the California Department of Corrections and Rehabilitation.[249]

Compounding the problem is the clandestine nature of violent extremists who seek to remain hidden within the prison environment, rather than overtly declare allegiance to extremist groups. Of significant concern are resource limitations.

---

[248] Such monitoring likely does not pose a First Amendment challenge because convicted prisoners possess limited constitutional rights and the screening for imams falls within the purview or maintaining order. Criminal conviction and lawful imprisonment deprive citizens of their freedom and other constitutional rights but prisoners retain constitutional rights compatible with the objectives of incarceration. Federal courts are reluctant to interfere with the internal administration of prisons and the judiciary accords wide-ranging deference to the "expert judgment" of prison officials. Prison officials must afford prisoners opportunities to exercise their religious freedom. Prison regulations interfering with an inmate's free exercise of religion are subject only to the requirement that they be "reasonably related to legitimate penological interests." Impediments to a prisoner's right of free exercise may be constitutional if: (1) the regulation is rationally related to legitimate concerns of rehabilitation, institutional order, and security; (2) no ready alternatives to the regulation exist; (3) prisoners retain some freedom of religious expression in alternative ways; and (4) accommodation of prisoners' practices would require extra supervision, threaten prison security, and create perceptions of favoritism. A prisoner asserting his or her right of religious liberty must establish that his or her beliefs are sincere2764 and religious in nature. *See* Stephen S. Sypherd, Gary M. Ronan, Rahul Patel and Ann N. Sagerson, "Prisoner's Rights," *Georgetown Law Journal* (May 2001): page nr., http://findarticles.com/p/articles/mi_qa3805/is_200105/ai_n8934901/pg_6/?tag=content;col1 (accessed July 4, 2009).

[249] Mark S. Hamm. "Terrorist Recruitment in American Correctional Institutions: An Exploratory Study of Non-Traditional Faith Groups." December 2007. http://www.ncjrs.gov/pdffiles1/nij/grants/220957.pdf (accessed March 29, 2008).

California officials, for example, reported that radical group investigations produce numerous leads, but agencies do not have enough investigators to follow each lead.[250] Thus, an information-sharing environment between prisons as well as law enforcement and intelligence agencies is necessary to target those prisoners who likely experienced violent jihadist influence and who should be monitored further upon release. The U.S. Bureau of Prisons (BOP) commenced this strategic change at the federal level, but the state and local levels lack such mechanisms and the majority of inmates are incarcerated in those prisons.[251]

The United States has already experienced terrorism as the result of prisoner recruitment, radicalization, and release, which confirms the need for an effective monitoring mechanism. For example, U.S. authorities disrupted an indigenous jihadist cell in 2005.[252] The cell's leader and self-styled imam, U.S. citizen Kevin James, developed a terror plot while serving a sentence in a California state prison. Also known as Shaykh Shahaab Murshid, James founded *Jam'iyyat Ul-Islam Is-Shaheeh* (JIS), an organization structured to promote James' radical interpretation of Islam. James actively recruited members while in prison and told followers that they had a duty to attack infidel targets.[253]

James recruited Levar Washington in November 2004. Shortly before Washington's parole release that same month, James instructed him to recruit five

---

[250] Frank Cilluffo and Gregory Saathoff, "Out of the Shadows: Getting Ahead of Prison Radicalization," *The George Washington University Homeland Security Policy Institute and The University of Virginia Critical Incident Analysis Group* (2006): 8.

[251] Cilluffo and Saathoff, "Out of the Shadows: Getting Ahead of Prison Radicalization," 8-9.

[252] Hannah, Clutterbuck and Rubin, *Radicalization or Rehabilitation*, 35.

[253] Hannah, Clutterbuck and Rubin, *Radicalization or Rehabilitation*, 35.

individuals without felony convictions and to train them in covert operations.[254] The cell planned to attack military recruiting stations, the Israeli Consulate in Los Angeles, and the Los Angeles International Airport (LAX). James coordinated these plans from prison. Authorities discovered the plot through traditional law enforcement techniques only after Washington and his accomplices committed several gas station robberies to finance their terror plot.[255] In fact, detectives identified Washington after he mistakenly left his cell phone at one of the robbery scenes.[256] But for Washington's criminal blunders, the JIS terrorism plot likely would have materialized. James and his followers had selected targets.[257] They had chosen attack dates.[258] They had obtained weapons.[259] They had written down plans.[260] Domestic intelligence surveillance might have revealed this plot and allowed for controlled and proactive intelligence-gathering. Instead, evidence involved in a crime triggered a reactive investigation.

---

[254] Josh Lefkowitz, "Terrorists Behind Bars," *NEFA Foundation*, May 5, 2008, 19-21.

[255] U.S. Congress. Senate. *Statement of Donald Van Duyn, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation before the Senate Committee on Homeland Security and Governmental Affairs.* "Prison Radicalization: The Environment, The Threat, and The Response," Donald Van Duyn (Washington DC: September 19, 2006), 13.

[256] Mark S. Hamm, "Prisoner Radicalization: Assessing the Threat in U.S. Correctional Institutions," *National Institute of Justice Journal* 261 (October 2008): under "261,", http://www.ojp.usdoj.gov/nij/journals/261/prisoner-radicalization.htm (accessed July 1, 2009).

[257] Lefkowitz, "Terrorists Behind Bars," 20.

[258] Ibid. at 20.

[259] Ibid.

[260] Ibid.

Radicalization Literature in Prison

Identifying targets for surveillance also requires scrutinizing the literature that is regularly distributed to the prisons and learning how to identify incendiary content. Such inspection is warranted by the fact that perverted versions of the Qur'an heavily influence prisoner radicalization. Until federal authorities banned it after the September 11th attacks, the Wahhabi/Salafi version of the Qur'an (the Noble Qur'an) was widely distributed throughout the U.S. prison system. The English translation contains numerous radical excerpts that are absent in the original Arabic. The excerpts seem to be designed to explain the Arabic verses. However, these particular excerpts openly endorse violent jihad as a method by which to propagate Islam among non-Muslims.[261] The now-defunct Al-Haramain Foundation (AHF) also regularly distributed *The Call to Jihad*, a 22-page appendix advocating that Muslims are religiously obligated to oppose non-Muslims.[262]

The U.S. intelligence and law enforcement communities must strive to create a moderate environment within the U.S. prison system and participate in persuasive discourse that lessens the appeal of radical Islam. The strategic distribution of radical literature bolsters the proposition that U.S. prisoners are attractive targets for terrorist

[261] The Noble Qur'an is not the only literature that advances the jihadist agenda. Several publications promote violent extremist rhetoric that influences America's prisons. Examples include: 1) *Sawt al-Jihad* (Voice of Jihad), a magazine that regularly publishes articles that urge jihadists to stand their ground, if arrested; 2) *al-Jamma'ah,* a magazine that promotes the plight of Muslim prisoners and urges the Muslim population to act in furtherance of their release whether by money or other means; and 3) *The Declaration of Jihad Against the Country's Tyrants (aka The Manchester Manual)*, a publication which was discovered in a raid in Manchester in 2000 and which provides guidance for how jihadists should behave when taken prisoner. *The Manchester Manual* directs jihadists to create Islamic programs within the prison system as well as to master the art of hiding messages.

[262] The appendix was written by former Saudi Arabian chief justice Abdullah bin Muhammad bin Humaid. In it, bin Humaid argues that Muslims are obligated to wage war against non-Muslims who refused to submit to Islamic rule. The Al-Haramain Foundation was controversial for its role in radicalizing Muslim populations worldwide. U.S. federal authorities banned the foundation in 2004.

recruitment. The construct of prison *da'wa* (Islamic evangelism) programs reveal the recruitment potential that radical Islamic literature supports. Former AHF employee and author of *My Year Inside Radical Islam*, Daveed Gartenstein-Ross, claimed that the cornerstone of AHF's *da'wa* program was the radical literature distributed to the inmates. Al-Haramain stamped its contact information in its introductory literature, which prompted a response from inmates who subsequently requested additional literature from AHF. AHF then forwarded additional extremist literature, which included Muhammad bin Jamail Zino's *Islamic Guidelines for Individual and Social Reform*, which advocates that children should be indoctrinated in the glories of jihad from an early age.[263] Another distributed text illustrates the dangers of radical literature. In *The Fundamentals of Tawheed (Islamic Monotheism)*, Abu Ameenah Bilal Philips claimed that acquiescing to non-Islamic rule constitutes an act of idolatry, and thus, true believers do not accept non-Islamic rule in place of Shar'ia law.[264] Not only did AHF flood the prisons with such influential text, but also sent the inmates a loaded questionnaire. Gartenstein-Ross explained that the questionnaire contained inquiries that would elicit data about an inmate's background as well as assess an inmate's level of Islamic knowledge.[265] Employees of AHF later graded the responses to determine the extent to which an inmate was truly Muslim. The names were then entered into a database that eventually contained over 15,000 entries. According to Gartenstein-Ross, AHF missed its

[263] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2006. *Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?* Daveed Gartenstein-Ross. 109th Cong., 2nd sess., Sept. 19.

[264] Committee on Homeland Security and Governmental Affairs, *Prison Radicalization*.

[265] Ibid.

opportunity to recruit potential terrorists because the names were not exploited.[266] Yet, the AHF's *da'wa* program illustrates how terrorist organizations could exploit such systems for recruitment and other programs may have already done so.

Targeting Released Inmates

The correctional system's inability to effectively monitor prisoners while incarcerated only exacerbates the security risk when extremists or their recruits are released from prison. The post-imprisonment period poses the most significant challenge for those who seek to counter radicalization or to identify potentially activated homegrown terrorist cells. Radicalized, but released prisoners can plan future attacks beyond the confines of prison, presenting a monumental security risk. Adding to that risk are the resource deficiencies in the prison system. For example, the BOP reported in 2006 that it does not read all mail of high-risk terrorist inmates because the BOP does not have sufficient personnel to translate mail written in foreign languages or to detect suspicious content due to insufficient training in intelligence techniques. Similar deficiencies apply to verbal communications, such as telephone calls, family visits, and cellblock conversations.[267]

An inability to track inmates upon release combined with practically nonexistent social programs expose the United States to heightened security risks. Not only do inmates face recruitment while in prison, but must also contend with radical groups that

[266] Committee on Homeland Security and Governmental Affairs, *Prison Radicalization.*

[267] Lefkowitz, "Terrorists Behind Bars," 26.

pose as post-release reintegration organizations.[268] Such radical groups are more interested in promoting their extremist agenda than reintegrating former prisoners.

Moreover, no database exists to track inmates upon release or to identify inmates associated with radical groups.[269] Similarly, no centralized database exists to track radical religious service providers who are contracted through various, unaligned prison systems and who are known to incite inmates with radical rhetoric.[270] Such a centralized database would streamline intelligence efforts and would maximize the information available to not only the U.S. correctional system, but also intelligence and law enforcement agencies. Consequently, the database would facilitate identification and focused surveillance collection of targets.

Extremist Propaganda and the Internet.

The danger of Islamist radicalization and extremist propaganda within the United States is not limited to the U.S. correctional system. Radical Islamist literature also finds its way into American homes. Terrorist groups regularly have distributed and sold printed materials, operational videos, and recordings of fiery sermons for decades.[271] Moreover, some of those radicalized by traditional jihadist literature furthered their education and become more entrenched in operational extremism by attending terrorist

---

[268] Cilluffo and Saathoff, "Out of the Shadows: Getting Ahead of Prison Radicalization," 7.

[269] U.S. Congress. House of Representatives. *Statement of Frank Cilluffo, Director, Homeland Security Policy Institute, The George Washington University before the House Committee on Homeland Security, Subcommittee on Intelligence Information Sharing, and Terrorism Risk Assessment.* "The Homeland Security Implications of Radicalization," Frank Cilluffo, (Washington DC: September 20, 2006), 32.

[270] House of Representatives, "The Homeland Security Implications of Radicalization," 32.

[271] Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 5.

training camps and connecting to the centralized Al-Qa'ida organization prior to the September 11th attacks.[272] Circumstance and technology exacerbated the proliferation of jihadist propaganda to render such information an even more ubiquitous threat today. Inspired by extremist ideology, today's would-be extremists may be physically isolated from the Al-Qa'ida organization in the post-9/11 world, but they connect with like-minded peers through the Internet.

Not only does violent and influential propaganda find an audience through traditional books and pamphlets, but also through the Internet, which provides a virtual sanctuary for radicalization, recruitment, and training through the written word and video. The Internet provides the most accessible source of both passive and interactive information.[273] The passive researcher can be influenced by a plethora of material on static web pages, whereas others can be inclined to act after engaging in private chat rooms and discussion forums dedicated to extremist causes. The Internet has essentially globalized jihadist rhetoric, which poses a threat to national security, especially when such provocative communication is unmonitored and easily transmittable. Importantly, disenfranchised and disengaged U.S. citizens are increasingly exposed to and recruited by such rhetoric. For example, the Internet played a role in radicalizing Derrick Shareef, who planned to bomb a mall in Rockford, Illinois. Shareef became radicalized due to his friendship and Internet relationship with Hassan Abu-Jihad, who was convicted of

---

[272] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2007. *Radicalization of Global Islamist Terrorists.* Marc Sageman, 1. 110th Cong., 1st sess., Oct. 30.

[273] Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 5.

sending Navy secrets to the website of Azzam Publications, a media website devoted to promoting and fundraising for Usama bin Laden.[274]

The reach of Islamist radicalization has become even more pervasive with the advent of jihadist websites, chat rooms, and social networking sites. Terrorist groups, such as AQ, have transformed perception through the Internet. That terrorist groups are adaptable is exhibited in their swift adoption of one of the Internet's benefits: dissemination of information. For example, in 1998, less than half of the 30 groups that the U.S. State Department designated as "Foreign Terrorist Organizations" (FTOs) had websites; yet, nearly all of those groups had their own website by the end of 1999.[275] The growing use of the Internet to identify with and globally connect to radical networks facilitates access to expertise that previously could only be experienced in overseas training camps.[276] Al-Qa'ida's transformation provides an example of this phenomenon. Once a close-knit and insular militant group, AQ now uses the Internet to disseminate radical text and expects sympathizers to act on the information independently, thereby expanding AQ's role as an ideological social movement.[277] Moreover, Saudi researchers

---

[274] Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 13.

[275] Gabriel Weinmann, *Terror on the Internet: The New Arena, The New Challenges* (Washington, DC: U.S. Institute of Peace, 2006), p. 15.

[276] Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 14-15.

[277] MITRE Corporation. "Al-Qaeda-Linked Web Sites Number 5,000 and Growing," *Terrorism Open Source Intelligence Report (TOSIR) No. 310*, 20 December 2007, http://www.mitre.osis.gov/isi/tosir/TOSIR310.doc (accessed January 26, 2009).

recently estimated that approximately 5,600 websites worldwide currently espouse AQ ideology.[278] In addition, new sites also appear at a rate of approximately 900 a year.[279]

The fact that the Internet serves as a virtual terrorist campaign delivers challenges that appear insurmountable to defeat the reach of Islamist radicalization.[280] Massive amounts of operational information and extremist propaganda is available online. Terrorist groups regularly leverage social situations and world events to develop perceptions of victimization and their message is persuasive. The proliferation of websites and extremist forums support this proposition.[281]

The Internet is both a driver and enabler of preliminary radicalization as face-to-face radicalization is increasingly replaced by online radicalization. Network mobilization further drives a very small percentage to become terrorists. Such networks operated on a face-to-face basis before the propagation of the Internet. Members encountered radicalization together as they shared their grievances and engaged in radical discourse as they bonded in dynamic settings whether through student associations or study groups at radical mosques.[282] The interconnectivity between groups and individuals changes beliefs, a systemic occurrence which is driven by Islamist extremist

---

[278] MITRE Corporation. "Al-Qaeda-Linked Web Sites Number 5,000 and Growing," 20 December 2007.

[279] MITRE Corporation. "Al-Qaeda-Linked Web Sites Number 5,000 and Growing," 20 December 2007.

[280] Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 14-15.

[281] Ibid. at 14-15.

[282] Sageman, "Terrorism: What the Next President Will Face," 227-28.

forums on the Internet.[283] Traditional offline peer groups are now established online in virtual Islamist forums. These forums become the invisible conduit through which terrorist groups organize. They also provide a conduit that entices individuals to join a politicized social cause absent an affiliation with a formalized terrorist organization. Rather than an influential imam or firebrand sheikh, the true leader of this violent social movement is the collective discourse flowing through extremist forums.[284] Such pervasive reach explains why the law enforcement and intelligence communities expect the homegrown terrorism threat to rapidly increase over the next several years due to the Internet.[285] The assessment is reasonable given that the Internet continues to propagandize terrorist ideological messages, to enlist followers to act upon ideological messages, and to provide methodologies that serve destructive terrorist objectives.

Extremists exploit the common roots they share with their potential followers, thereby maximizing the extremist appeal. Radicalized U.S. individuals, for instance, can find an American kindred spirit in propaganda videos sponsored by AQ and distributed through the Internet. A skilled propagandist, Adam Gadhan is an AQ media adviser and spokesman who is also the first American charged with treason since 1952.[286] Since 2004, he has appeared in six videos where Gadhan espouses anti-American messages

---

[283] U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2007. *Radicalization of Global Islamist Terrorists.* Marc Sageman, 4. 110th Cong., 1st sess., Oct. 30.

[284] Committee on Homeland Security and Governmental Affairs, *Radicalization of Global Islamist Terrorists,* 4.

[285] Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 16.

[286] Fox News, "American Al Qaeda Member to Be Indicted for Treason," www.foxnews.com, http://www.foxnews.com/story/0,2933,219861,00.html (accessed July 3, 2009).

laced with threats while persuading viewers to convert to Islam.[287] In one such video, "An Invitation to Islam," Gadhan urged the people of the United States to discard their religious beliefs, to adopt an uncompromising form of Islam, and to "join the winning side."[288] In 2005, with his head wrapped in a black turban and his face covered with a black veil, he warned, "We love nothing better than the heat of battle, the echo of explosions, and slitting the throats of the infidels."[289] Gadhan also incorporates suggestive and actionable messages into his rhetoric. For instance, in 2006, he said, "It's hard to imagine that any compassionate person could see pictures, just pictures, of what the Crusaders did to those children, and not want to go on a shooting spree at the Marines' housing facilities at Camp Pendleton."[290] So pervasive is Gadhan's presence that he is prominently featured as one of FBI's Most Wanted Terrorists with a one million dollar reward for information that leads to his capture.[291] In the meantime, Gadhan influences potential U.S. extremists in the privacy of their own homes.

The Internet will breed a new level of homegrown terrorist sophistication that will make radicalized cells almost impossible to detect unless the United States Government assumes an aggressive and proactive domestic surveillance posture. Although authorities

---

[287] Craig Whitlock, "Converts To Islam Move Up In Cells: Arrests in Europe Illuminate Shift," *Washington Post*, September 15, 2007, under "Page A10," http://www.washingtonpost.com/wp-dyn/content/article/2007/09/14/AR2007091402265.html (accessed July 3, 2009).

[288] Raffi Khatchadourian, "Azzam the American: The Making of an Al Qaeda Homegrown," *The New Yorker*, January 22, 2007, page nr. http://www.newyorker.com/reporting/2007/01/22/070122fa_fact_khatchadourian?currentPage=all (accessed July 4, 2009).

[289] Khatchadourian, "Azzam the American: The Making of an Al Qaeda Homegrown," January 22, 2007.

[290] Ibid.

[291] Federal Bureau of Investigation, "Most Wanted Terrorists," www.fbi.gov, http://www.fbi.gov/wanted/terrorists/gadahn_a.htm (accessed July 3, 2009).

have detected radicalized cells in the United States, this success should not become an excuse for complacency with the status quo. Previously disrupted cells have lacked sophistication, experience, and access to resources overseas, and thus, were done in by poor operational tradecraft.[292] The Internet changes the scenario as it accords potential extremists the ability to identify and connect to jihadist networks throughout the world, which in turn, provides opportunities to build relationships and to gain operational sophistication and expertise previously only available in overseas training camps.[293] The U.S. government must identify those who would use the Internet for such knowledge to prevent a homeland attack from within. The lack of traceable formal ties to groups overseas combined with increasing Internet usage necessarily renders a U.S.-based extremist hard to detect. Consequently, Congress must enact legislation that allows for a legal, practical, and expedient Internet surveillance tool that serves as a preventive intelligence collection platform even if the collection does not involve direct foreign connections. The rapidity by which jihadists groups propagandize their objectives via the Internet warrants such an expansive proposition.

Just as the Internet serves as an extremist recruitment and training camp environment, the U.S. Government can use the Internet to gather information and monitor the activities of emerging threats, such as homegrown terrorism. Congress must develop new legal tools to identify those susceptible to recruitment and to combat the allure of jihadist rhetoric targeted for potential homegrown terrorists. As applied to the Internet, for example, current law allows that in limited circumstances adversarial websites can be

---

[292] Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 3.

[293] Ibid. at 3.

shut down for inciting violence or providing material support to identified terrorist organizations.[294] These cases cross the line from constitutionally protected speech into illegal activity. However, this legal mechanism fails to resolve the root cause of the homegrown dilemma: how can the United States identify those citizens who are becoming radicalized through the Internet and try to prevent radicalization from taking hold? Violent Islamist extremists radicalized online are a challenge because under current law such domestic lone wolves evade the attention of law enforcement.[295]

DISA: An Answer to the Homegrown Threat

The absence of a legal framework for domestic surveillance intelligence collection exposes the United States to unnecessary risk in light of an nascent yet escalating homegrown terrorism threat. Although AQ continues to be a centralized organization, its influence materialized into a social movement of people who grew up in and became radicalized in the United States. These homegrown extremists now pose a serious threat in that they remain largely undetected and are sheltered by the umbrella of U.S. citizenship. The Foreign Intelligence Surveillance Act (FISA) authorizes domestic surveillance collection against only foreign nationals or entities located within the United States as well as U.S. citizens tied to foreign nationals or foreign organizations. FISA surveillance cannot and has never been used to detect terrorists; rather, FISA is a monitoring mechanism for previously identified subjects. Congress must equip both the

[294] Homeland Security Policy Institute and Critical Incident Analysis Group, "NETworked Radicalization: A Counter-Strategy," *George Washington University* (2008): 14-16 http://www.gwumc.edu/hspi/news/index.cfm?d=4098 (accessed January 26, 2009).

[295] Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*., 14.

intelligence and law enforcement communities with updated legal tools to detect radicalized homegrown terrorists. Creating a Domestic Intelligence Surveillance Act (DISA) that authorizes surveillance of U.S. citizens would provide the intelligence community (IC) with a valuable domestic collection capability that would be of particular use in taking advantage of prison information and targeting nodes that are now beyond the reach of the law.

CHAPTER 5

FISA Is Inadequate for Domestic Intelligence Surveillance

The nascent homegrown terrorism threat poses a threat to national security due to the absence of a legal framework that facilitates terrorist identification and surveillance. This chapter argues that amending FISA is an inadequate remedy because it is a monitoring mechanism, rather than a robust intelligence collection tool. Recent attempts to synchronize domestic and foreign intelligence investigations also have fallen short of what the government needs to protect national security. Congress must equip the U.S. government with a robust yet balanced law to conduct domestic intelligence surveillance. Such a law should codify the Fourth Amendment's reasonableness touchstone and predicate surveillances on the reasonable suspicion standard, which requires the government to articulate specific facts prior to initiating surveillance. The chapter concludes by illustrating how Congress can balance the legitimate national security interests of the U.S. Government while protecting American civil liberties. In essence, Congress should and must enact the proposed Domestic Intelligence Surveillance Act (DISA) for the benefit of the U.S. Government and for the people that the government exists to protect.

FISA's Provisions are Outdated

The FISA statute retains value as a method to monitor communications of known terrorists with foreign connections based on a probable cause standard. However, FISA cannot and has never facilitated the detection of terrorists, which has become a top

priority for the U.S. Government.[296] Carving out an exception to the FISA statute to encompass surveillance of U.S. citizens would not be an adequate solution to combat the homegrown terrorism threat. Such an expansive exception would swallow the rule and would nullify an important principle of FISA, that targets of intelligence collection must be tied to agents of a foreign power. Foreign entities are not subject to the same constitutional protections enjoyed by U.S. persons, and thus, regulatory parameters must necessarily be distinct. One could argue that domestic intelligence surveillance should be incorporated into the FISA framework as an exception given that the statute addresses warrantless surveillance as applied to U.S. citizens. Such an argument is untenable, however, for the following reasons.

First, with the FISA statute Congress did not contemplate the transnational, globalized nature of current threats that endanger national security. Borders-based rules are now too antiquated to fight against borderless terrorist threats. Radicalized Islamist terrorism is festering within our borders, influenced by Islamist groups outside U.S. borders. The key word "influenced" demonstrates another point. Homegrown U.S.-based groups do not have to be directed by or even tied to foreign entities in order to act upon the tenets of Al-Qa'ida-inspired ideology. These groups also do not fit squarely within the Lone Wolf exception to FISA because they are American citizen lone wolf actors with no ties to any agents of a foreign power.

Second, when it passed FISA, Congress did not anticipate the explosion of global communications networks and advanced technical methods that would neutralize traditional intelligence-gathering within the context of FISA. As previously discussed

[296] Richard A. Posner, "A New Surveillance Act," *Wall Street Journal*, February 15, 2006. http://online.wsj.com/article/SB113996743590074183-search.html (accessed July 4, 2009).

in Chapter 3, FISA requires a court order to conduct electronic surveillance to gather foreign intelligence information when the surveillance either targets U.S. persons or is conducted within the United States.[297] Congress did not intend the FISA statute to extend to wholly foreign communications of non-U.S. persons. Congress also did not intend FISA to be triggered by incidental interceptions of U.S. person communications during legitimate foreign interceptions of those not subject to FISA.[298] Yet, due to the warrant requirement for any electronic surveillance conducted physically within the United States, FISA constrains surveillance of wholly foreign communications when applied to transit intercepts, those cases when the interception could occur in the United States while the communication is in transit between two overseas countries.[299] For example, FISA requires a warrant when a non-U.S. terrorist logistics supplier located in Jordan places a phone call to a Saudi sheikh in Riyadh despite the fact that the only nexus to the United States is a U.S.-based telecommunications switch that facilitated the international phone call.

---

[297] "Electronic surveillance" means –

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States…;

50 U.S.C. § 1801(f) (2000).

[298] Kim A. Taipale, "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance," *Yale Journal of Law and Technology* 9 (2007): 133-34.

[299] Kim A. Taipale, "Rethinking Foreign Intelligence," *World Policy Journal* 13, no. 4 (Winter 2006-2007): 77-79.

FISA is Unnecessarily Inefficient

The antiquated quality of the FISA statute is further aggravated by FISA's inefficiency. Three subject areas demonstrate this point: 1) collateral intercepts of U.S. citizens; 2) nonexistence of automated analysis; and 3) existence of procedural hurdles. The issue of collateral intercepts reveals the cumbersome nature of the FISA statute. The U.S. government must produce an individualized and particularized application to the Foreign Intelligence Surveillance Court (FISC) when the government seeks authorization to target a specific U.S. person or location.[300] Prior to any authorization of electronic surveillance, the application must show probable cause that the target is involved in nefarious foreign intelligence pursuits, such as being a terrorist or engaging in terrorist activity.[301] This standard appears reasonable on its face for the purpose of monitoring a suspected terrorist, yet does nothing to focus targeting methods. What remains unreasonable is the probable cause standard in circumstances where the government collects collateral U.S. intercepts incidental to an authorized foreign intelligence target that is not subject to FISA's reach. Such collateral intercepts arguably could implicate the lower reasonable suspicion threshold, which in turn, would require follow-up surveillance to determine whether probable cause even exists in assessing the extent to which the subject of the collateral intercept is involved in nefarious foreign intelligence activity. Yet, the FISA statute precludes the government from further pursuing surveillance for the purpose of determining whether probable cause exists.[302] Instead, the

[300] Taipale, "Rethinking Foreign Intelligence," 77-79.

[301] Ibid. at 77-79.

[302] Ibid.

government first must now establish probable cause and submit a FISA application. Inefficiency is at its maximum when FISA creates such a circuitous method for hybrid communications between a non-FISA based foreign intelligence target and a U.S. citizen. Not only is this system simply unworkable when applied to domestic intelligence surveillance collection, but it also is prohibited. Even if a FISA exception could be fashioned to include domestic surveillance collection, the probable cause standard frustrates the purpose of conducting domestic surveillance when the government is trying to identify its U.S.-based terrorists.

The FISA statute is inefficient in its processes as well. The statute fails to provide any mechanism for pre-authorization of technical methods, such as pattern analysis or filtering, to uncover any connections to foreign terrorist activities or a terrorist organization.[303] Such an impediment to foreign intelligence collection necessarily renders pre-authorized pattern analysis impossible as applied to domestic intelligence. Yet, restrictions are unnecessary for either foreign or domestic surveillance collection if the government implements the automated screening process as a targeting mechanism. Pre-authorized automated pattern screening could monitor data flows, which may reveal suspicious terrorist connections or communications without any initial human involvement necessary.[304] The automated screening process would serve as a warning system that alerts the government to the potential for further investigative follow-up. Such pre-authorized technical methods would not implicate data-mining concerns because the government is not seeking pre-authorized access to filter the content of

[303] Taipale, "Rethinking Foreign Intelligence," 78-79.

[304] Ibid. at 79.

collected information; rather, the government is trying to identify and isolate patterns of suspicious communications activity. In turn, the identified patterns would trigger the legal controls already in place for further investigating the content of communications. The automated screening process is merely a targeting tool that would legally facilitate identification of potential terrorists whether at home or abroad.

Moreover, creating additional FISA exceptions based on U.S. citizenship is impracticable given the labyrinth of existing exceptions and procedural hurdles that already exist as to non-citizens or those U.S. citizens tied to an agent of a foreign power. For instance, the government stated that even the most experienced lawyers need a week to prepare the necessary paperwork for the FISA court and noted that the documents are "like mortgage applications in their complexity."[305] Another procedural hurdle involves the emergency FISA exception. The FISA statute authorizes electronic surveillance without a court order in certain emergency circumstances. Such surveillance is authorized when the Attorney General (AG) reasonably determines that an emergency situation exists before an order authorizing the surveillance can be obtained with due diligence and that a factual basis for the surveillance exists.[306] The Attorney General must notify a judge from the Foreign Intelligence Surveillance Court (FISC) at the time of authorization and must file a regular FISA application no more than 72 hours after the

[305] Ronald J. Sievert, "Patriot 2005-2007: Truth, Controversy, and Consequences," *Texas Review of Law and Politics* 11 (Spring 2007): 327. (citing Richard Lacayo, "Has Bush Gone Too Far?: The President's Secret Directive to Let the NSA Snoop Without Warrants Sets Off a Furor," *Time* Jan. 9, 2006: 28.).

[306] Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A §1805 (f) (West 2003 & Supp. 2005).

Attorney General authorizes the surveillance.[307] The surveillance may be permitted to last up to a year provided the surveillance is directed solely at communications between foreign powers or focused on their property, when there is "no substantial likelihood" that a communication involving a U.S. person will be acquired.[308] Although the emergency FISA exception may appear to provide the government with unbridled authority, the exception procedures actually diminish its potential effectiveness as a situational awareness tool. For instance, the exception requires that probable cause must exist prior to authorization of the surveillance. Such a requirement defeats the purpose of expediency when emergency surveillance only can be applied to identified or suspected targets involved in imminent threat streams.

The Attorney General's Guidelines for Domestic FBI Operations Fall Short

Good-faith attempts to synchronize domestic national security and foreign intelligence investigations presently have thus far proven ineffective. The recently enacted Attorney General's (AG) Guidelines for Domestic FBI Operations prove this point. The purpose of the new AG Guidelines is to establish consistent policy regarding FBI investigative matters that serve to protect the United States from national security threats, to shield citizens from federal crime, and to further U.S. foreign intelligence

[307] The FISA Amendments Act of 2008 expanded the 72-hour timing provision to one week, a provision which is scheduled to sunset in 2012. The Attorney General and the Director of National Intelligence must submit authorized targeting procedures within seven days and the FISC will make a final determination within 30 days. During this period, minimization procedures, the probable cause requirement, and reverse targeting guidelines will apply. U.S. Congress. H.R. 6304--110th Congress (2008): FISA Amendments Act of 2008, *GovTrack.us* http://www.govtrack.us/congress/bill.xpd?bill=h110-6304 (accessed June 1, 2009).

[308] Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A §1802 (West 2003 & Supp. 2005).

objectives while balancing the privacy concerns and civil liberties of U.S, citizens.[309] The AG Guidelines also underscore the necessity of expanding FBI capabilities to become better integrated if the FBI is to effectively lead domestic national security and foreign intelligence investigations:

> "Continuing coordination…is necessary to optimize the FBI's performance in both national security and criminal investigations….[The] new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very different FBI from the one we had on September 10, 2001."[310]

In addition, the Guidelines authorize the FBI to conduct investigations to detect, obtain information about, or protect against crimes or threats to national security. The FBI derives such authority from a variety of sources, such as the Executive Order 12,333, the AG's powers to delegate, and statutory law.[311]

Recognizing that the FBI is an intelligence agency as well as a law enforcement agency in the context of both criminal and national security investigations, the AG Guidelines charge the FBI with proactively drawing upon available sources of information to identify terrorist threats and activities.[312] The FBI must be vigilant in

---

[309] U.S. Department of Justice, "The Attorney General's Guidelines for Domestic FBI Operations," *U.S. Department of Justice*, October 2008, 5. http://www.usdoj.gov/ag/readingroom/guidelines.pdf (accessed June 6, 2009).

[310] U.S. Department of Justice, "The Attorney General's Guidelines for Domestic FBI Operations," 5-6.

[311] See respectively, "U.S. Intelligence Activities," Executive Order, No. 12,333; "National Security Act of 1947," 50 U.S.C. § 401, et seq.; "Foreign Intelligence Surveillance Act," 50 U.S.C. § 1801, et seq.

[312] U.S. Department of Justice, "The Attorney General's Guidelines for Domestic FBI Operations," 17.

detecting terrorist threats with strategies that encompass early intervention and prevention of terrorist attacks before they occur, and the Guidelines stress that the FBI cannot wait for investigative leads from others. The Guidelines also contemplate that the FBI proactively will exercise its protective functions by showing initiative to both disrupt terrorist threats and secure those entities that represent attractive targets for terrorism or espionage.[313] The Guidelines thus authorize the FBI to develop analyses of threats and vulnerabilities of the United States that include domestic and international criminal threats and activities as well as those domestic and international matters affecting national security.[314] In assessing and investigating respective threats within the United States, the FBI:

> "…shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism."[315]

The AG Guidelines also caution against infringing upon the civil liberties of U.S. persons. Therefore, the AG Guidelines do not authorize investigating, collecting, or maintaining information on U.S. person solely for monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution and laws of the United States.[316] The FBI may use all lawful investigative methods as

---

[313] U.S. Department of Justice, "The Attorney General's Guidelines for Domestic FBI Operations," 17.

[314] Ibid. at 17.

[315] Ibid.

[316] U.S. Department of Justice, "The Attorney General's Guidelines for Domestic FBI Operations," 29.

authorized by the AG Guidelines. One such authorized method allows for electronic surveillance under 18 U.S.C. §§ 2510-2522 (Chapter 119 – "Wire and Electronic Communications Interception and Interception of Oral Communications.") or 50 U.S.C. §§ 1841-1846 ("The Foreign Intelligence Surveillance Act.").

The AG Guidelines simply do not reach far enough to close the domestic intelligence gaps that the homegrown terrorism threat creates. Granted, the AG Guidelines are progressive in that they attempt to expand FBI powers to integrate its law enforcement and intelligence roles. However, as applied to the homegrown terrorism threat, the AG Guidelines merely reinforce the dichotomy between criminal investigations and foreign intelligence without addressing the domestic powers necessary for identifying homegrown terrorists. For example, the only authorized surveillance methods of electronic surveillance must conform to either the criminal code or the FISA statute. In his statement before the Senate Committee on Homeland Security and Governmental Affairs in 2007, FBI Director Robert S. Mueller III articulated the need for legal tools that allow for the interceptions of U.S.-based communications of potential homegrown terrorists:

> "One of the areas that we're concerned about and have been for some time is, first of all the lone wolf actor who is not tied with any particular groups overseas, and we addressed that in legislation a year or so ago. But as you have self-radicalization growing, and regularization in the United States, where it does not have any foreign components, we are still, we operate under Title III, on the criminal side of the house. And over a period of time as technology has improved, and the statutes focus on facilities, particularly facilities as opposed to the target. We'd like the possibility of making modifications to make it easier with appropriate safeguards to do interceptions of those individuals who might be self-radicalized and intent on undertaking terrorist attacks as opposed to other criminal activities within the United States, without any foreign nexus."[317]

[317] U.S. Congress. Senate. *Testimony of Robert S. Mueller IIII, Director of the Federal Bureau of Investigation, before the Senate Committee on Homeland Security and Governmental Affairs,* 2007.

Not only would the proposed DISA statute satisfy the investigative and intelligence needs that the FBI Director identified, but also would provide the FBI and attendant agencies with the legal tool necessary to satisfy the intent of the AG Guidelines. The AG Guidelines emphasize the requirement that the FBI and other agencies must improve its domestic intelligence gathering capabilities within the United States. However, only Congress can provide the FBI with the requisite tools for AG Guideline compliance to identify and counter potential acts of terrorism planned and conducted by U.S.-based citizens.

A Proposed Domestic Intelligence Surveillance Act (DISA)

Congress has created a large intelligence gap by failing to provide a legally sufficient identification mechanism to address the significant homegrown terrorism threat. Simply monitoring terrorists is not enough, especially when the law enforcement and intelligence communities do not know who the potential extremists are. Law enforcement and intelligence agencies cannot monitor a person who has not been identified. Because Islamist radicalization and other types of homegrown terrorism are on the rise in the United States, Congress must equip the U.S. law enforcement and intelligence communities with a mechanism by which they can identify potential homegrown extremists. Only with such a tool can the government detect those radicalized individuals who choose to operationalize their beliefs. The Domestic Intelligence Surveillance Act (DISA) is the appropriate targeting and intelligence

---

"Confronting the Terrorist Threat to the Homeland: Six Years After 9/11." Robert S. Mueller III, 28. 110th Cong., 1st sess., Sept. 10.

collection method that would facilitate the identification of homegrown terrorists, thereby closing the widening intelligence gap.

The enactment of the DISA statute will require debate about how best to apply a proactive domestic targeting mechanism that also does not infringe upon privacy rights and civil liberties. Consequently, Congress must frame difficult DISA issues around a preemptive discourse, rather than a reactive solution. The debate should not be centered on whether a proactive domestic approach toward defeating homegrown terrorism is necessary. Even the staunchest of civil libertarians agree that preemption is preferred.[318] Rather, preemption will be at issue when congressional members debate and define the applicable methodologies that the DISA statute should employ. Not only can the DISA statute become a domestic intelligence collection breakthrough, but also can be fashioned to respect the civil liberties so dearly held by American citizens. For instance, in implementing DISA, Congress can create oversight committees, incorporate procedural safeguards, and define governing rules to ensure that the United States is well-armed in fighting against the homegrown terrorism threat while honoring the rights of its citizens. Citizens should demand no less from Congress in the interest of national security.

The Mechanics of DISA

The proposed DISA statute is a necessary and reasonable solution for closing the domestic intelligence gaps underscored by the homegrown terrorism issue. Congress can incorporate legal principles expounded in Fourth Amendment jurisprudence (see Chapters 1-2) into DISA and develop oversight procedures to ensure that domestic

[318] Taipale, "The Ear of Dionysus," 138.

intelligence legislation balances national security needs against privacy rights. Transparency is the key component necessary for the successful passage, enactment, and implementation of the Domestic Intelligence Surveillance Act.

Changing the Fourth Amendment Paradigm

Passing DISA would require a shift in traditional Fourth Amendment paradigms. Congress can incorporate Fourth Amendment principles into a domestic surveillance statute that is reasonable in scope. Such an approach also may result in the Supreme Court modifying or outright reversing its *Keith* ruling, which requires warrants for domestic electronic surveillance even in the national security context. Congress can create procedural requirements that adequately address civil liberties without imposing the warrant process upon domestic intelligence. If properly created and implemented, DISA can fit squarely within the Court's Fourth Amendment jurisprudence as an extension of one of several Fourth Amendment standards and exceptions.

Reasonable Suspicion Threshold Vice Probable Cause

Three areas of Fourth Amendment jurisprudence provide Congress with legal standards to consider.[319] The Supreme Court outlined the reasonable suspicion standard in *Terry v. Ohio.*[320] In *Terry*, the Court held that police officers may conduct a quick

[319] The following legal principles are not exhaustive. They also may appear unconventional at first glance as applied to domestic intelligence. Domestic intelligence surveillance is an activity that often carries negative connotations, yet does not have to be negative in scope if implemented in a responsible and transparent manner. Thus, the ideas cited and analyzed here are intended to raise awareness, generate creative legal solutions, and provide Congress with potential frameworks for fashioning a comprehensive, workable, and balanced DISA.

[320] *Terry v. Ohio*, 392 U.S. 1 (1968).

warrantless surface search of an individual or detain individuals in vehicles (known as a *Terry* stop) if those officers do not have full probable cause, but merely a "reasonable suspicion" that an individual is armed. The Court added that reasonable suspicion requires that the officer base the stop on specific and articulable facts, rather than an officer's hunch. Moreover, unlike the probable cause standard that requires officers to establish a crime's occurrence, the reasonable suspicion standard allows a search when a police officer has reason to believe a crime is about to occur. The underlying issue in the *Terry* case actually involved whether the exclusionary rule of criminal procedure served as a sufficient deterrent to police misconduct, rather than whether the traffic stop was appropriate.[321] In determining whether a traffic stop is unreasonable and subject to the exclusionary rule, the Court analyzed the validity under the totality of circumstances test.[322] The test requires courts to determine whether justification for a stop existed in the form of reasonable suspicion and whether the degree of intrusion into the suspect's liberty was reasonably related in scope to the situation. Although the *Terry* ruling focused upon assessing reasonable suspicion as applied to the evidentiary exclusionary rule, the totality of circumstances test and resultant reasonable suspicion standard in *Terry* applies to domestic intelligence surveillance and the passage of DISA.

---

[321] "Proper adjudication of cases in which the exclusionary rule is invoked demands a constant awareness of these limitations. The wholesale harassment by certain elements of the police community, of which minority groups, particularly Negroes, frequently complain, will not be stopped by the exclusion of any evidence from any criminal trial. Yet a rigid and unthinking application of the exclusionary rule, in futile protest against practices which it can never be effectively used to control, may exact a high toll in human injury and frustration of efforts to prevent crime." *Terry v. Ohio*, 392 U.S. 1, 14-15.

[322] The exclusionary rule is designed to exclude evidence obtained in violation of a criminal defendant's Fourth Amendment rights. The rule provides that evidence obtained through a violation of the Fourth Amendment is generally not admissible by the prosecution during the defendant's criminal trial. If the search of a criminal suspect is unreasonable, the evidence obtained in the search will be excluded from trial. A criminal defendant's claim of unreasonable search and seizure is usually heard in a suppression hearing before the presiding judge. This hearing is conducted before trial to determine what evidence will be suppressed, or excluded from trial.

A domestically-focused surveillance statute based on reasonable suspicion, rather than probable cause, is necessary for efficient targeting of potential homegrown terrorists. Congress can apply the Supreme Court's *Terry* stop reasoning to create a responsible DISA framework. Rather than limiting an investigative method from the onset, the reasonable suspicion standard creates a valuable intelligence collection tool. For instance, compliance with a totality of circumstances test would require the U.S. government to provide Congress with specific and articulable facts to initiate surveillance on a likely U.S. person or facility for a specified and limited amount of time. Such facts also should demonstrate why surveillance is reasonable for either targeting individuals or addressing threat streams and why traditional criminal methods are unavailable. The results will provide context and situational awareness to determine whether additional investigation under a probable cause standard is even necessary. The surveillance must cease when the time limit expires or when the U.S. Government discovers that a targeting purpose is no longer relevant. Otherwise, surveillance will continue to identify individuals related to potential threat streams. The DISA statute initially would serve to identify potentially operational extremists based on reasonable suspicion, thereby facilitating a focused and intelligence-driven investigation once the government establishes information sufficient to meet the probable cause standard. Such a reasonable suspicion framework allows the government to identify someone whom the government reasonably believes may be tied to terrorist plots or activities. The requirement of specified, articulable facts would prevent generic approvals predicated on vagueness and the congressional reporting requirement would prevent overreach by the Executive Branch.

As a preliminary targeting and determination tool, surveillance under the reasonable suspicion standard is preferable and rational given the confining burdens of the probable cause standard as evidenced by FISA. The probable cause standard imposes excessive costs on domestic intelligence. As previously noted, the probable cause standard of FISA hamstrings the statute from becoming a targeting mechanism and Congress should not similarly restrict the DISA statute. First, the probable cause standard presumes that a subject or target already is conducting nefarious activity as applied to foreign intelligence. The purpose of DISA is to provide a targeting mechanism regarding highly suspicious domestic-based terrorist activity, and thus, for cases where the government cannot assert with certainty that a potential target is involved in nefarious activity. In the context of preventing terrorist attacks, the U.S. Government simply will not have evidence sufficient to satisfy the probable cause standard as required in the criminal context because intelligence officers do not have a concrete idea of what they seek when the goal is to detect and prevent terrorist threats.[323] Second, in the context of procuring warrants, the Fourth Amendment expressly bans a search based on any standard less than probable cause.[324] This standard places a significant burden on counterterrorism efforts in the domestic intelligence realm when the U.S. Government does not know the identities of potential terrorists in advance of the surveillance. The DISA statute will provide a preliminary mechanism by which the U.S. Government can either further pursue investigative activity or disqualify individuals as terrorists. Such situational awareness is necessary to produce focused and intelligence-driven

[323] Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York: Oxford University Press, 2006), 100-101.

[324] U.S. Const. amend. IV

investigations. The probable cause standard unduly frustrates this purpose. Thus, Congress should lower the probable cause standard to reasonable suspicion in DISA to justify a surveillance that comports with DISA's purpose.

Furthermore, incidental collection that identifies relevant, additional U.S. targets should be added to any existing DISA surveillance order. The term "relevant" is important here for the purpose of protecting civil liberties. Merely connecting with or talking to a U.S. target is insufficient to trigger the reasonable person standard to sustain an addition to the DISA order; otherwise, the U.S. government risks a First Amendment violation. The U.S. Government must articulate facts that give rise to reasonable suspicion in order to add those U.S. persons identified through incidental collection. For instance, the surveillance may have incidentally identified a person once tied to a closed terrorism investigation. The U.S. government would have a legitimate interest in determining whether it closed the investigation prematurely, whether new facts justify re-opening the investigation, or whether the actual target of surveillance is also involved. Once the reasonable standard is satisfied, incidental collection would facilitate an individualized preliminary inquiry to determine whether probable cause exists for a criminal investigation or whether reasonable suspicion remains sufficient to continue the surveillance intelligence operation. Such an inquiry must be limited in duration to protect civil liberties within a reasonable timeframe to be determined by Congress.

The Reasonableness Requirement Vice the Warrant Clause

An additional consideration that complements the reasonable suspicion standard is the Reasonableness Requirement of the Fourth Amendment itself. Congress as well as

the Supreme Court should shift away from the Warrant Clause and rely upon the Reasonableness Requirement as applied to domestic intelligence gathering. The Warrant Clause combined with its attendant probable cause standard imposes too high of a cost in the domestic intelligence realm as they are legal tools standards too restrictive for identifying homegrown terrorists and homegrown threat streams. The warrant requirement for domestic intelligence is unnecessary and obstructs government access to information necessary for thwarting homegrown terrorist attacks. Congress should relax the warrant requirement for domestic intelligence surveillance, especially when the Fourth Amendment does not require the government to apply for a warrant prior to conducting any search:

> 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 or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[325]

The Framers of the Constitution intended to limit the use of warrants as noted by several members of the Rehnquist Court.[326] Had the Framers intended the Fourth Amendment to execute a warrant requirement, the Framers could have drafted the Amendment to command the use of warrants. Instead, the Framers developed permissive language that limits warrants to those circumstances that satisfy the probable cause standard. Moreover, the Supreme Court has stated that the true "touchstone of the Fourth Amendment is reasonableness," to the extent that the Fourth Amendment only

[325] U.S. Const. amend. IV.

[326] Tracey Maclin, "The Central Meaning of the Fourth Amendment," *William and Mary Law Review* 35 (1993): 199-201.

"sometimes…require[s] warrants."[327] Although the government is not required to obtain a warrant in all situations, any warrant that does issue is deemed per se unreasonable unless supported by probable cause.[328] Absent an unnecessary warrant requirement, Congress and the Supreme Court can apply the Reasonableness Requirement to assess the appropriateness of domestic intelligence surveillance.

Unlike the confining parameters of the Warrant Clause, the Reasonableness Requirement inherently requires a more flexible balancing test predicated on a sliding-scale analysis. This framework facilitates a case-specific methodology for defining reasonableness and takes the timing of fact development into account. For instance, Congress and the Supreme Court may determine that the intrusive nature of warrantless surveillance is reasonable and becomes less intrusive when applied to preventing a terrorist act. Conversely, the legislative and judicial branches may conclude that a similar surveillance is unreasonable when initiated for the purpose of investigating a crime that already occurred. The Warrant Clause also allows government officials to hide behind court authority should problems with surveillance later arise, whereas the Reasonableness Requirement promotes accountability in that government officials must justify their actions or face remedial consequences.

Another salient reason for relaxing the warrant requirement involves the difference between ex post and ex ante constitutional judicial review. Working in tandem with the Reasonableness Requirement is the concept of ex post constitutional review

---

[327] Harvard Law Review, "Shifting the FISA Paradigm: Protecting Civil Liberties by Eliminating Ex Ante Judicial Approval," *Harvard Law Review* 121, no. 8 (June 2008): 2220-21. (citing *United States v. Knights*, 534 U.S. 112, 118 (2001) and *Illinois v. McArthur*, 531 U.S. 326, 330 (2001).

[328] Akhil Reed Amar, "Fourth Amendment First Principles," *Harvard Law Review* 107 (2002): 761-63.

(after-the-fact review), which encourages a comprehensive assessment of whether domestic surveillance meets constitutional safeguards. Congress should not require a warrant requirement in the DISA statute because ex ante judicial approval (before-the-fact review) is overly restrictive due to the highly unpredictable nature of employing domestic intelligence surveillance as an identification tool.

The FISA statute is archetypal in that Congress created a system that heavily relies upon ex ante judicial approval through the issuance of warrants, thereby limiting FISA's effectiveness in the national security realm.[329] Although requiring the government to articulate specific facts regarding the circumstances of domestic surveillance is reasonable, ex ante restrictions imposed on DISA due to a warrant requirement would be unreasonable if such restrictions required the government to wholly identify targets of surveillance. Perhaps one can best understand the ineffectiveness of ex ante review by its implications. For instance, prior to committing an act, one does not seek the opinion of a judge to determine the legal sufficiency of that act. Instead, one acts and later addresses any resulting legal issues that may arise from the act. The legal sufficiency of the act is then determined through a comprehensive ex post analysis. The remedial operation of ex post review best exemplifies several of its benefits for DISA. First, ex post review will deter unconstitutional searches if Congress includes sanctions, such as monetary damages or criminal prosecution, in the DISA framework. Second, ex post review requires the consideration of all information related to the constitutionality of domestic surveillance. Not only does this review allow a complainant to challenge the constitutionality of the DISA statute on its face and its

[329] Harvard Law Review, "Shifting the FISA Paradigm," 2201.

purpose, but also its effects. Any resulting issues will promote early detection of unintended consequences with the DISA statute and will increase the quality of DISA to achieve a responsible and transparent domestic intelligence collection goal. Third, ex post review facilitates transparency due to its adversarial nature. For instance, a judge conducts ex ante review of warrants ex parte, which results in presumptive legal sufficiency for the warrants issued prior to the initiation of any search or surveillance. Ex post review, on the other hand, would promote debate about the reasonableness of a search or surveillance and would reveal unconstitutional searches in application. Such ex post reviews of warrantless surveillance provide better safeguards against Fourth Amendment violation than do the restrictive ex ante reviews related to the warrant application process.

Special Needs Exception

Alternatively, even if Congress determines that warrants are necessary for providing judicial checks upon the Executive Branch, Congress and the Supreme Court each have the power to create a domestic intelligence collection exception to any warrant requirement in the DISA statute. The Supreme Court has recognized the futility of requiring warrants in certain circumstances as the Court has carved out exceptions to the warrant requirement. Examples include the exigent circumstances exception, the border search exception, and the special needs exception.[330] Congress also should recognize the

[330] Exigent circumstances arise when law enforcement reasonably believes that there is an immediate need to protect their lives, the lives of others, their property, or that of others. Thus, a search is reasonable because it is not motivated by intent to arrest and seize evidence, and there is reason to associate an emergency with the area or place to be searched. Searches conducted at the United States border or the equivalent of the border (such as a port authority or an international airport) may be conducted without a warrant or probable cause. However, reasonable suspicion is required for border searches when a search potentially can intrude on one's personal dignity, such as cavity searches. Courts apply the "special needs"

merits of excluding warrantless domestic intelligence surveillance from the warrant requirement. Relaxing the requirement in a domestic intelligence realm actually facilitates targeted, focused, and responsible surveillance based on an analysis of reasonableness. For example, knowing that surveillance results may be subject to congressional and judicial review, intelligence and law enforcement personnel have an interest in ensuring that the surveillance is reasonable and sufficient for favorable review.

Congress should not be deterred from enacting DISA due to prior Supreme Court rulings that fail to extend Fourth Amendment exceptions to domestic intelligence surveillance. No articulated warrant exception exists as to domestic intelligence surveillance and the Court's 1972 decision in *United States v. U.S. Dist. Court (Keith)* is the controlling authority. The *Keith* Court determined that the ultimate issues in that case rested upon the reasonableness of the search and the way that such reasonableness derives meaning through reference to the Warrant Clause.[331] Writing for the Court, Justice Powell declined to extend a warrant exception for domestic intelligence due to the "inherent vagueness of the domestic security concept" and the expansive scope of domestic intelligence collection.[332] Thus, the Court held that warrantless domestic intelligence surveillance is unconstitutional, which also meant that issues regarding wholly domestic terrorist threats are subject to the warrant requirement.[333]

---

exception to uphold certain suspicionless searches and seizures as an exception to the general rule that a search must be based on individualized suspicion of wrongdoing. The caveat is that the exception applies only when the justification for the search is divorced from criminal law enforcement and that law enforcement does not use the search for collecting evidence for criminal law enforcement purposes.

[331] *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 309-310 (1972).

[332] *Keith*, 320.

[333] Ibid. at 297.

The *Keith* ruling is untenable and no longer relevant today for three reasons. First, the *Keith* decision may be controlling, but the Court also acknowledged that the warrant requirement is not finite. Recognizing that targets are more difficult to identify in the domestic intelligence realm, the *Keith* Court noted that Congress could create legislation with procedural controls that would distinguish domestic intelligence collection from criminal investigations.[334] Second, the *Keith* Court recognized that, under Title III, warrantless national security wiretaps authorized by the President may be necessary in grave circumstances even when such wiretaps involved domestic organizations unrelated to foreign powers.[335] Third, the *Keith* decision occurred in 1972, an era of non-existent regulation over intelligence abuses that occurred within a world demarcated by national boundaries. Since 1972, transnational and homegrown terrorism emerged and the U.S. government established a history of compliance with requisite intelligence legislation, such as FISA. The world of 1972 no longer exists. Existing law

---

[334] *Keith*, 322.

[335] The case of domestic intelligence as applied to the homegrown terrorism threat appears to go beyond even what the Court initially contemplated. *See United States v. United States District Court (Keith)*, 407 U.S. 297, 309, 322 (1972). (*see FN 8:* "Section 2511(3) (of Title III) refers to 'the constitutional power of the President' in two types of situations: (i) where necessary to protect against attack, other hostile acts or intelligence activities of a 'foreign power'; or (ii) where necessary to protect against the overthrow of the Government or other clear and present danger to the structure or existence of the Government. Although both of the specified situations are sometimes referred to as 'national security' threats, the term 'national security' is used only in the first sentence of s 2511(3) with respect to the activities of foreign powers. This case involves only the second sentence of s 2511(3), with the threat emanating-according to the Attorney General's affidavit-from 'domestic organizations.' Although we attempt no precise definition, we use the term 'domestic organization' in this opinion to mean a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies. No doubt there are cases where it will be difficult to distinguish between 'domestic' and 'foreign' unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case." *See also FN 20*: "For the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved, see *United States v. Smith,* 321 F.Supp. 424, 425-426 (CDCal.1971); and American Bar Association Project on Standards for Criminal Justice, Electronic Surveillance 120, 121 (Approved Draft 1971 and Feb. 1971 Supp. 11). See also *United States v. Clay*, 430 F.2d 165 (CA5 1970).")

can and must adapt to the times, rather than adhere to an outdated analysis that no longer works. The special needs exception to the Fourth Amendment thus merits attention.

Although the DISA statute should be premised on the Reasonableness Requirement, the DISA framework also fits comfortably within the Fourth Amendment's special needs exception should Congress or the Supreme Court refuse to dispense with the Warrant Clause when assessing domestic intelligence surveillance. Under traditional judicial analysis, a showing of special government non-law enforcement need triggers the exception, whereby a court determines the constitutional validity of a search or surveillance based on reasonableness. Courts reach their determination by balancing the intrusion on a person's Fourth Amendment rights against the legitimate governmental interest in conducting the search or surveillance.[336] The special needs exception authorizes the President to conduct warrantless surveillance in order to respond to specific threats from foreign powers.[337] However, the special needs exception need not limit warrantless domestic intelligence surveillance.

The special needs exception applies to warrantless domestic intelligence surveillance because the government has a legitimate interest in detecting homegrown terrorism, which is a threat that extends beyond criminal law enforcement. The Supreme Court alluded to the threat of terrorism as sufficient grounds for applying the special needs exception to suspicionless searches in *City of Indianapolis v. Edmond*.[338] In that case, the *Edmond* Court analyzed suspicionless searches in the context of a traditional

---

[336] *Delaware v. Prouse*, 440 U.S. 648, 654-55 (1979).

[337] *In re Sealed Case*, 310 F.3d 717, 745 (FISA Ct. Rev. 2002).

[338] *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).

criminal case. The Court invalidated a suspicionless search derived from a highway checkpoint erected to detect a drug transportation route.[339] The Court stated that suspicionless searches require a purpose beyond criminal prosecution to protect citizens against special hazards.[340] An imminent terrorist plot would justify a suspicionless search, according to the Court.[341]

Similarly, the threat of homegrown terrorist plots justifies warrantless domestic intelligence surveillance, thereby triggering the special needs exception to the warrant requirement of the Fourth Amendment. In a foreign intelligence realm, the Court decided in *In Re Sealed Case* that the proper method of applying the exception requires analyzing the programmatic purpose of FISA-related activity, rather than the purpose for which the government conducts each search.[342] The methodology also applies in the domestic intelligence realm because, as the Court noted, it is "the nature of the 'emergency,' which is simply another word for threat that takes the matter out of the realm of ordinary crime control."[343] Although the Court has yet to apply the special needs exception to warrantless domestic surveillance, DISA appears to fit squarely within the special needs exception because the government has a legitimate interest in preventing homegrown terrorist acts, which implicate threats that extend beyond ordinary crime control and that require robust intelligence mechanisms.

---

[339] *Edmond*, 48.

[340] Ibid. at 32-41.

[341] Ibid. at 44.

[342] *In Re Sealed Case*, 745.

[343] *In Re Sealed Case*, 746.

Congressional Oversight and Political Checks Preserve Civil Liberties

National security will reach its maximum potential when all three branches of government participate in domestic intelligence processes that address constitutional concerns. The Judicial branch regularly enforces and redefines Fourth Amendment jurisprudence as applied to domestic intelligence matters. The Executive Branch regularly develops policies tailored to address and redefine polices as homeland threats emerge. Congress must exert its legislative authority now to proactively, rather than reactively, create workable solutions for closing domestic intelligence gaps. Congress exercised such authority in the foreign intelligence realm when it enacted FISA and its subsequent amendments. Congress now must do the same to facilitate domestic intelligence surveillance collection, especially since Congress knows more about national security issues than does the Supreme Court, and thus, may be a more effective political check on the Executive Branch.[344] The national security apparatus in the United States will become a formidable environment in which terrorists choose to operate if Congress incorporates congressional oversight and imposes political checks upon domestic intelligence legislation. No longer can Congress let judicial rulings shape domestic intelligence policy.

Congress can enhance privacy protection and maximize the utility of DISA by reevaluating a systemic failure of FISA. Surveillance law "has become paradoxically overprotective and underproductive at the same time."[345] The FISA statute overly restricts the acquisition of data, particularly acquiring real-time data, yet does little to

[344] Posner, *Not a Suicide Pact,* 150.

[345] Benjamin Wittes, *Law and the Long War: The Future of Justice in the Age of Terror* (New York: The Penguin Press, 2008), 233.

regulate what the U.S. Government does with the data.[346] The FISA statute impedes the collection of data and makes the content of communications difficult to acquire.[347] Yet, the real privacy interest lies in the use of data, rather than its acquisition. Adding to the acquisition issue is the fact that FISA becomes more outdated as technology grows, so regulating the acquisition of data is inefficient as the law realistically cannot adapt quickly enough.[348] Yet, regulating the application and use of data is more static as the basic principle of safeguarding civil liberties does not change. Thus, Congress should develop a DISA that contains a relaxed standard for acquisition of surveillance data and imposes severe penalties for violating predetermined applications of that data.

Privacy groups likely would protest as the idea is unconventional and demarcates from the carefully deliberated standards articulated in FISA. The idea of trusting the U.S. government is unsettling. However, Congress can easily create an accountability structure that incorporates redundancy into its checks and balances system. Such a system would include inspector general audits, internal checks, and reporting requirements to the courts and Congress.[349] Congress can also mandate reporting requirements from every level of the bureaucratic sphere to ensure consistency regarding the validity of each surveillance operation. Moreover, Congress must assure the public that such a mandate is not finite. For instance, Congress can institute regularly scheduled unclassified and classified forums to reevaluate whether the new surveillance strategy works and whether it adversely impacts civil liberties.

---

[346] Wittes, *Law and the Long War,* 238-39.

[347] Ibid. at 238-239.

[348] Ibid. at 222-224.

[349] Ibid. at 253.

Transparency in government is the underlying principle of DISA's construction. Congress has the power to and should create congressional committees that focus on Executive branch decisions to pursue warrantless domestic intelligence surveillance. The committees will serve as a centralized oversight and reporting system that requires the Executive Branch to report all occurrences of warrantless domestic surveillance and that provides a method by which intelligence and law enforcement officials can report illegal surveillances that demand further congressional investigation. The notice requirement to the committees is essential because it serves as an appropriate check and balance on specific uses of surveillance. For instance, should the committees find that surveillance is unreasonable, the surveillance activity will cease and minimization procedures similar to those found in FISA will transpire to prevent retention or dissemination of communications information related to U.S. persons. However, surveillance deemed reasonable merely will require measurable progress reports to the congressional committees until such time the Executive Branch determines the intelligence reveals information sufficient for probable cause, information that calls for a disruption and dismantlement operation, or information that renders the surveillance moot. The materials presented to the committees may be classified, thereby creating an aura of secrecy from a public perspective. As representatives of the American public, however, committee members are politically accountable for infringing upon any rights of the citizens they represent. Their duty to the public provides members with an incentive to ensure that the government upholds Fourth Amendment principles in light of warrantless domestic intelligence surveillance. The representatives will be responsible to their

constituents for any individualized adverse consequences as they will be complicit in approving the surveillance measures.

Congress should require political accountability regarding domestic intelligence surveillance from executive officials. Such a requirement institutes a procedural safeguard regarding warrantless surveillance. For instance, under FISA, the AG must be the approving authority who initiates any warrantless surveillance in the United States.[350] Congress should impose a similar requirement on the AG as applied to domestic intelligence because the requirement identifies a person who must answer to Congress if facts reveal that the government conducted a search for any improper purpose. Compatible with creating political accountability is Congress' ability to punish those officials who abuse their authority and violate the Fourth Amendment. The potential for punitive outcomes will deter officials from abusing their authority, thereby facilitating a good-faith, well-reasoned decisionmaking process.

Those adversely affected by warrantless domestic intelligence surveillance ideally will have legal remedies available to them. Congress could develop a civil tort remedy whereby injured individuals could seek redress in court via monetary damages. The logistics and degree to which such redress is viable is outside the scope of this thesis, but the idea of a remedial option demonstrates that Congress should incorporate civil remedies into DISA in order to instill public confidence in the government's ability to conduct responsible domestic surveillance. Additionally, Congress could garner more public support if it created an independent review board that would streamline the often costly and time-consuming characteristics of civil lawsuits.

[350] "Foreign Intelligence Surveillance," 50 U.S.C. § 1804 (2006).

BIBLIOGRAPHY

911 Commission. "911 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." (2004).

Amar, Akhil Reed. "Fourth Amendment First Principles." *Harvard Law Review* 107 (2002): 761-63.

Benge, Jr., G. Jack. "Partners in Crime: Federal Crime Control Policy and the States, 1894-1938." Ph.D. diss., Bowling Green State University, December 2006.

Chemerinsky, Erwin. *Constitutional Law: Principles and Policies*. 2nd ed. New York: Aspen Law & Business, 2002.

Cilluffo, Frank, and Gregory Saathoff. "Out of the Shadows: Getting Ahead of Prison Radicalization." *The George Washington University Homeland Security Policy Institute and The University of Virginia Critical Incident Analysis Group* (2006).

City of Boerne v. Flores, 521 U.S. 507 (1997).

City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

CNN. "Study: 7.3 million in U.S. prison system in '07." www.cnn.com. http://www.cnn.com/2009/CRIME/03/02/record.prison.population/ (accessed July 4, 2009).

Coolidge v. New Hampshire, 403 U.S. 443 (1971).

Department of Justice. "Former Member of U.S. Navy Sentenced to 10 Years in Federal Prison for Disclosing Classified Information." www.usdoj.gov. http://www.usdoj.gov/opa/pr/2009/April/09-nsd-306.html (accessed July 3, 2009).

_____. "National Security Division Launches New Office of Intelligence," *Department of Justice*, April 30, 2008. http://www.fas.org/irp/news/2008/04/doj043008.html (accessed June 6, 2009).

Delaware v. Prouse, 440 U.S. 648 (1979).

Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

Dycus, Stephen, Arthur L. Berney, William C. Banks, and Peter Raven-Hansen. *National Security Law*, 4th ed. New York: Aspen Publishers, 2007.

Federal Bureau of Investigation. "Most Wanted Terrorists." www.fbi.gov. http://www.fbi.gov/wanted/terrorists/gadahn_a.htm (accessed July 3, 2009).

Federal Communications Act, 47 U.S.C. § 151 (1934).

Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A. §§ 1801-1862 (West 2003 & Supp. 2005).

Fox News. "American Al Qaeda Member to Be Indicted for Treason." www.foxnews.com. http://www.foxnews.com/story/0,2933,219861,00.html (accessed July 3, 2009).

Gonzalez, Jason A. "Article, Essay and Note: Constitutional Aspects of Foreign Affairs: How the War on Terror Has Changed the Intelligence Gathering Paradigm." *Naval Law Review* 51 (2005).

Hamm, Mark S. "Prisoner Radicalization: Assessing the Threat in U.S. Correctional Institutions." *National Institute of Justice Journal* 261 (October 2008): under "261." http://www.ojp.usdoj.gov/nij/journals/261/prisoner-radicalization.htm (accessed July 1, 2009).

_____. "Terrorist Recruitment in American Correctional Institutions: An Exploratory Study of Non-Traditional Faith Groups." December 2007. http://www.ncjrs.gov/pdffiles1/nij/grants/220957.pdf (accessed March 29, 2008).

Hannah, Greg, Lindsay Clutterbuck, and Jennifer Rubin. *Radicalization or Rehabilitation: Understanding the Challenge of Extremist and Radicalized Prisoners*. Santa Monica: RAND Corporation, 2008.

Harvard Law Review. "Shifting the FISA Paradigm: Protecting Civil Liberties by Eliminating Ex Ante Judicial Approval." *Harvard Law Review* 121, no. 8 (June 2008): 2220-21.

Homeland Security Policy Institute, and Critical Incident Analysis Group. "NETworked Radicalization: A Counter-Strategy." *George Washington University* (2008). http://www.gwumc.edu/hspi/news/index.cfm?d=4098 (accessed January 26, 2009).

In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002).

In Re Sealed Case (FISCR Decision), 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002)

Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, §601(2), 112 Stat. 2396, 2405-10 (1998).

Intelligence Reform and Terrorism Prevention Act of 2004. 108th Cong., 2d sess., 2004. H. Rept. 108-796. Pub. L. 108-458. 118 Stat. 3638.

Irvine v. California, 347 U.S. 128 (1954).

Jane's Islamic Affairs Analyst. "Muslim Radicals Enlisting U.S. Inmates." *Jane's Intelligence Review,* 2006. http://www.intelink.ic.gov/Reference/janes/display.html?type=S&nav=C_7&sn=jiaa&ed=jiaa2001122006. (accessed 01 January 2009).

Khatchadourian, Raffi. "Azzam the American: The Making of an Al Qaeda Homegrown." *The New Yorker*, January 22, 2007. http://www.newyorker.com/reporting/2007/01/22/070122fa_fact_khatchadourian?currentPage=all (accessed July 4, 2009).

Lefkowitz, Josh. "Terrorists Behind Bars." *NEFA Foundation*, May 5, 2008.

Maclin, Tracey. "The Central Meaning of the Fourth Amendment." *William and Mary Law Review* 35 (1993): 199-201.

Masse, Todd, and William Krouse. "The FBI: Past, Present, and Future." *Congressional Research Service* (October 2, 2003). http://www.fas.org/irp/crs/RL32095.pdf (accessed March 20, 2008).

MITRE Corporation. "Al-Qaeda-Linked Web Sites Number 5,000 and Growing." *Terrorism Open Source Intelligence Report (TOSIR)* 310 (20 December 2007). http://www.mitre.osis.gov/isi/tosir/TOSIR310.doc (accessed January 26, 2009).

Nardone v. United States, 308 U.S. 338 (1939).

National Security Act of 1947, ch. 343, Title I, § 103 (1947) (currently codified as 50 U.S.C. § 403-3(d)(1)(2004)).

O'Harrow, Robert. *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society*. New York: Free Press, 2005.

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

Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20.

Posner, Richard A. *Countering Terrorism: Blurred Focus, Halting Steps*. Lanham, Maryland: Rowman & Littlefield Publishers, Inc., 2007.

_____. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York: Oxford University Press, 2006.

Richards, Ashley Nicole. "Note: So You Think A Woman Can't Carry Out a Suicide Bombing? Terrorism, Homeland Security, and Gender Profiling: Legal Discrimination for National Security." *William and Mary Journal of Women and the Law* 13 (Winter 2007).

Reno, Janet. "Memorandum from Janet Reno, Attorney General, to Assistant Attorney General Criminal Division, FBI Director, Counsel for Intelligence Policy, and

United States Attorneys." (July 19, 1995) http://www.fas.org/irp/agency/doj/fisa/1995procs.html (accessed June 25, 2009).

Rogers, William P. "The Case for Wire Tapping." *Yale Law Journal* 63 (April 1954).

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

_____. "Terrorism: What the Next President Will Face: Section Four: U.S. Strategy; A Strategy for Fighting International Islamist Terrorists." *The Annals of The American Academy of Political and Social Science* 618 (July 2008).

Seamon, Richard Henry. "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits." *Hastings Constitutional Law Quarterly* 35 (Spring 2008).

Seamon, Richard Henry, and Willaim Dylan Gardner. "The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement." *Harvard Journal of Law and Public Policy* 28 (2005): 333-34.

Sievert, Ronald J. "Patriot 2005-2007: Truth, Controversy, and Consequences." *Texas Review of Law and Politics* 11 (Spring 2007).

Socialist Workers Party v. United States, 642 F. Supp. 1357 (S.D.N.Y. 1986).

Swire, Peter P. "The Future of Internet Surveillance Law Symposium: A Symposium to Discuss Internet Surveillance, Privacy, and the USA Patriot Act; Surveillance Law: Reshaping the Framework." *George Washington Law Review* 72 (August 2004): 1306-71.

Sypherd, Stephen S., Gary M. Ronan, Rahul Patel, and Ann N. Sagerson. "Prisoner's Rights." *Georgetown Law Journal* (May 2001): page nr. http://findarticles.com/p/articles/mi_qa3805/is_200105/ai_n8934901/pg_6/?tag=content;col1 (accessed July 4, 2009).

Taipale, Kim A. "Rethinking Foreign Intelligence." *World Policy Journal* 13, no. 4 (Winter 2006-2007): 77-79.

_____. "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance." *Yale Journal of Law and Technology* 9 (2007): 133-34.

Terry v. Ohio, 392 U.S. 1 (1968).

United States v. Katz, 389 U.S. 347 (1967).

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

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

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.

U.S. Congress. House of Representatives. *Statement of Frank Cilluffo, Director, Homeland Security Policy Institute, The George Washington University before the House Committee on Homeland Security, Subcommittee on Intelligence Information Sharing, and Terrorism Risk Assessment.* "The Homeland Security Implications of Radicalization." (Washington DC: September 20, 2006) 109th Cong., 2nd sess., 2006.

U.S. Congress. H.R. 6304. FISA Amendments Act of 2008, *GovTrack.us.* (Washington DC: July 10, 2008) 110th Cong., 2d sess. 2008. http://www.govtrack.us/congress/bill.xpd?bill=h110-6304 (accessed June 1, 2009).

U.S. Congress. Senate. Committee on Homeland Security and Governmental Affairs. 2007. *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11.* Senator Joe Lieberman. (Washington DC: September 10, 2007) 110th Cong., 1st sess., 2007.

_____. Committee on Homeland Security and Governmental Affairs. 2006. *Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?* Daveed Gartenstein-Ross. (Washington DC: September 19, 2006) 109th Cong., 2nd sess., 2006.

_____. Committee on Homeland Security and Governmental Affairs. 2007. *Radicalization of Global Islamist Terrorists.* Marc Sageman. (Washington DC: June 27, 2007) 110th Cong., 1st sess., 2007.

_____. Committee on Homeland Security and Governmental Affairs. *Statement of Donald Van Duyn, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation before the Senate Committee on Homeland Security and Governmental Affairs.* "Prison Radicalization: The Environment, the Threat, and the Response." (Washington DC: September 19, 2006.) 109th Cong., 2d sess., 2006.

_____. Committee on Homeland Security and Governmental Affairs. *Testimony of Mitchell Silber, Senior Intelligence Analyst, New York City Police Department, before the Senate Committee on Homeland Security and Governmental Affairs.* "The Role of Local Law Enforcement in Countering Violent Islamist Extremism." (Washington DC: October 30, 2007) 110th Cong., 1st sess., 2007.

_____. Committee on Homeland Security and Governmental Affairs. *Testimony of Robert S. Mueller III, Director, Federal Bureau of Investigation before the U.S. Senate Committee on Homeland Security and Governmental Affairs hearing on* "Confronting the Terrorist Threat to the Homeland: Six Years After 9/11." (Washington DC: September 10, 2007) 110th Cong., 2d sess., 2007.

_____. Committee on Homeland Security and Governmental Affairs. 2007. *The Role of Local Law Enforcement in Countering Violent Extremism.* Major Thomas Dailey, Kansas City, Missouri Police Department, Homeland Security Division. (Washington DC: October 30, 2007) 110th Cong., 1st sess., 2007.

_____. Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism: Al-Shabaab Recruitment in America.* Andrew Liepman, Deputy Director of Intelligence, National Counterterrorism Center (NCTC). (Washington D.C.: March 11, 2009) 111th Cong., 1st sess., 2009. http://74.125.95.132/search?q=cache:P-Xiw0OqJsgJ:hsgac.senate.gov/public/_files/031109Liepman.pdf+cause+of+radicalization&cd=16&hl=en&ct=clnk&gl=us&client=firefox-a (accessed July 4, 2009).

_____. Committee on Homeland Security and Governmental Affairs. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorism Threat*. 110th Cong., 2d sess., 2008.

_____. *Statement of Jean-Louis Brugiere before the Senate Committee on Homeland Security and Governmental Affairs,* 2007. "Violent Islamist Extremism: The European Experience." (Washington DC: June 27, 2007) 110th Cong., 1st sess., 2007.

_____. Select Committee on Intelligence. *Testimony of Robert S. Mueller III, Director, Federal Bureau of Investigation before the U.S. Senate, Select Committee on Intelligence hearing on* "Current and Projected National Security Threats." (Washington DC: February 5, 2008) 110th Cong., 2d sess., 2008.

_____. Select Committee to Study Governmental Operations. 1976. *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Book III, Warrantless FBI Electronic Surveillance*. 94th Cong. 2nd sess., April 23. http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book3.htm. (accessed March 1, 2009).

_____. *Testimony of Mike McConnell, Director of National Intelligence, before the Senate Committee on Homeland Security and Governmental Affairs,* 2007. "Confronting the Terrorist Threat to the Homeland: Six Years After 9/11." (Washington, DC: September 10, 2007) 110th Cong., 1st sess., 2007.

_____. *Written testimony of Charles E. Allen, Assistant Secretary for Intelligence and Analysis, Chief Intelligence Officer, Department of Homeland Security, before the Senate Committee on Homeland Security and Governmental Affairs,* 2007. "Threat of Islamic Radicalization to the Homeland." (Washington DC: March 14, 2007) 110th Cong., 1st sess., 2007.

U.S. Constitution. Amendment I.

U.S. Constitution. Amendment IV.

U.S. Constitution. Article I.

U.S. Constitution. Article I, §8, cl. 18.

U.S. Constitution. Article II.

U.S. Constitution. Article III.

U.S. Department of Justice. "The Attorney General's Guidelines for Domestic FBI Operations." *U.S. Department of Justice*, October 2008. http://www.usdoj.gov/ag/readingroom/guidelines.pdf (accessed June 6, 2009).

U.S. President. Executive Order No. 12,333. "United States Intelligence Activities." 4 December 1981.

United States. *Report to the President of the United States.* Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Washington, D.C.: 2005.

Weinmann, Gabriel. *Terror on the Internet: The New Arena, The New Challenges*. Washington, DC: U.S. Institute of Peace, 2006.

Wire and Electronic Communications Interception and Interception of Oral Communications, "Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited," 18 U.S.C. § 2511-2518 (2000).

Wittes, Benjamin. *Law and the Long War: The Future of Justice in the Age of Terror*. New York: The Penguin Press, 2008.

Youngstown Sheet and Tube Co. v. Sawyer (Steel Seizure Case), 343 U.S. 579 (1952).