NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MAKING U.S. SECURITY AND PRIVACY RIGHTS COMPATIBLE

by

David A. Clarke Jr.

September 2013

Thesis Advisor: Robert Simeral
Second Reader: Christopher Bellavita

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE MAKING U.S. SECURITY AND PRIVACY RIGHTS COMPATIBLE		**5. FUNDING NUMBERS**	
6. AUTHOR(S) David A. Clarke Jr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The terror attacks against the United States on September 11, 2001, necessitated changes in the way domestic intelligence agencies and services conducted information-collection activities to protect against further attacks. Congress acted quickly to prevent the next attack by expanding government authority under the USA PATRIOT Act and the Federal Intelligence Surveillance Court. This gave domestic intelligence services the tools needed due to advances in technology that allowed terror organizations and suspects to travel, communicate, raise money and recruit using the Internet. Safeguards were written into the enhanced authority to protect against privacy abuses by government.

Ten years after 9/11, civil-liberties advocates called for more transparency, more privacy protections and better oversight because of past abuses by government officials operating in the name of national security. Leaks about government spying on U.S. citizens have heightened the balance debate between security and privacy. Privacy or security is not a zero-sum game. A policy that incorporates an adversarial process in the FISC and a streamlined oversight mechanism in Congress for more effective oversight, and the release of redacted classified documents to educate the public about surveillance techniques, would instill more balance and greater public trust.

14. SUBJECT TERMS USA PATRIOT Act, Federal Intelligence Surveillance Court, Domestic Intelligence Services, Oversight, Adversarial Process, Surveillance Techniques, Privacy, Information Collection			**15. NUMBER OF PAGES** 117
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MAKING U.S. SECURITY AND PRIVACY RIGHTS COMPATIBLE

David A. Clarke Jr.
Sheriff, Milwaukee, WI
B.A., Concordia University Wisconsin 1999

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND DEFENSE AND SECURITY)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2013**

Author: David A. Clarke Jr.

Approved by: Robert Simeral
Thesis Co-Advisor

Christopher Bellavita
Thesis Co-Advisor

Dr. Mohammed M. Hafez, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The terror attacks against the United States on September 11, 2001, necessitated changes in the way domestic intelligence agencies and services conducted information collection activities to protect against further attacks. Congress acted quickly to prevent the next attack by expanding government authority under the USA PATRIOT ACT and the Federal Intelligence Surveillance Court. This gave domestic intelligence services the tools needed due to advances in technology that allowed terror organizations and suspects to travel, communicate, raise money and recruit using the Internet. Safeguards were written into the enhanced authority to protect against privacy abuses by government.

Ten years after 9/11, civil liberties advocates called for more transparency, more privacy protections and better oversight because of past abuses by government officials operating in the name of national security. Leaks about government spying on U.S. citizens have heightened the balance debate between security and privacy. Privacy or security is not a zero sum game. A policy that incorporates an adversarial process in the FISC and a streamlined oversight mechanism in Congress for more effective oversight, and the release of redacted classified documents to educate the public about surveillance techniques, would instill more balance and greater public trust.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
ATM	Automated Teller Machine
CIA	Central Intelligence Agency
CONTEST	United Kingdom intelligence strategy
CT	Counterterrorism
CTC	Counterterrorism Center
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
EIT	Enhanced Interrogation Technique
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
FC	Fusion Centers
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GCHQ	Government Communications Headquarters
GWOT	Global War on Terror
I&A	Intelligence & Analysis
IC	Intelligence Community
ICE	Immigration & Customs Enforcement
IO	Intelligence Officer
IRTPA	Intelligence Reform and Terrorism Protection Act 2004
JTTF	Joint Terrorism Task Force
LIBERT-E	Limiting Internet and Blanket Electronic Review of Telecommunications and E-mail Act
MI5	United Kingdom Intelligence Service
NCT	National Commission on Terrorism
NPS	Naval Postgraduate School
NSA	National Security Agency

OSS	Office of Strategic Services
PRISM	Planning Tool for Resource Integration Synchronization and Management
SB	Special Branch
TIA	Total Information Awareness
TSA	Transportation Security Administration
U.S.	United States
UK	United Kingdom
USAPATRIOT	Patriot Act

EXECUTIVE SUMMARY

The debate on how to maintain a balance between security and privacy in the aftermath of the 9/11 attacks rages on after revelations that intelligence services and agencies amassed a vast collection of data on Americans not suspected of terror or criminal involvement. Expanded interpretations of the new laws governing data collection under the USA PATRIOT Act by domestic intelligence officials have led to calls by privacy advocates for more transparency, more protections and more effective congressional oversight. A lack of candid testimony by intelligence officials about methods used by government agencies has lessened pubic trust about these techniques.

Congress has responded by conducting hearings into government data collection on Americans not suspected of terror or other criminal activity. Members from both sides of the aisle are threatening changes that would hamper domestic intelligence efforts. Courts are weighing in as well. The concern is that if some changes are not made and accepted by the executive branch to better balance privacy and security then change will be forced on them. This would put intelligence efforts at a disadvantage in preventing, deterring, disrupting and identifying terror plans and identifying suspects. Momentum is on the side of greater privacy protections. The argument of conducting vast data collection by domestic intelligence officials in the name of national security is being lost.

This thesis offers a better way forward in light of the controversy surrounding domestic intelligence data collection methods, and incorporates the needs of three identified stakeholder groups: Privacy Advocates, Domestic Intelligence Officials, and Congress/Courts.

Three policy options are examined and a policy alternative presented that will better balance security and privacy and restore public confidence:

- Maintaining the status quo of data collection by domestic intelligence agencies.
- Creating a single integrated domestic intelligence service to replace the disparate approach currently used.

- A streamlined congressional oversight process with one House and one Senate committee responsible for oversight that replaces the estimated 88 committees and sub-committees currently overseeing these entities, and inserting an adversarial process into the FISC for warrant and wiretap applications.

The policy recommended contains a blend of the three options presented. It maintains enhanced surveillance methods, and for balance needed to protect privacy, includes more transparency and trust with an adversarial process in the warrant and wiretap application process. The policy option includes more effective oversight by a more frequent release of classified documents that have been redacted to protect secrets when officials brief streamlined congressional oversight committees.

ACKNOWLEDGMENTS

At one time in this great country, it was against the law to educate "*Negroes*" as they called them. Any attempt to educate slaves had to occur underground. Many of the early abolitionists, like Frederick Douglas, were self taught. It was frowned upon to teach slaves to read and write. The prevailing orthodoxy at the time was that education would open the eyes of slaves and that it would incite rebellion toward their oppressors, and eventually they would demand their freedom. The following language actually appeared in the State of Virginia statutes (Revised Code of 1819).

> *That all meetings or assemblages of slaves, or free negroes or mulattoes mixing and associating with such slaves at any meeting-house or houses, &c., in the night; or at any SCHOOL OR SCHOOLS for teaching them READING OR WRITING, either in the day or night, under whatsoever pretext, shall be deemed and considered an UNLAWFUL ASSEMBLY; and any justice of a county, &c., wherein such assemblage shall be, either from his own knowledge or the information of others, of such unlawful assemblage, &c., may issue his warrant, directed to any sworn officer or officers, authorizing him or them to enter the house or houses where such unlawful assemblages, &c., may be, for the purpose of apprehending or dispersing such slaves, and to inflict corporal punishment on the offender or offenders, at the discretion of any justice of the peace, not exceeding twenty lashes.*

Education opens minds. It teaches people to think for themselves, it connects people to the past and prepares them for the future. Education has always been the vehicle to upward mobility in the United States. With this in mind I want to thank the following people.

First, I want to thank my parents who understood the value of an education and poured what little money they had into providing me with a solid educational base. They knew that, in a sometimes unfair and unjust world that I would have to be doubly-prepared to overcome obstacles.

This Master's Program from the renowned Center for Homeland Defense and Security at the Naval Postgraduate School fulfills the promise I made to my parents to see

education as a life-long learning endeavor, even at this stage in my life, and having already reached the top level of my local law enforcement career. This achievement is more about the future.

Nobody accomplishes anything of value without tremendous love, patience, understanding, and support of the people around them. I want to thank the staff at the Center for Homeland Defense and Security. The staff does the logistics that many think just happen. Things like travel arrangements, reimbursements, and class materials take on added importance when traveling across the country, which for two-week segments is no easy task. I want to thank the teaching staff and will not try to name every one for fear of leaving someone out, but a hardy thank you, nonetheless.

I do want to point out my thesis advisors, however, for special thanks. Captain Robert Simeral and Dr. Chris Bellavita stuck with me. I know I made this challenging to them and left them shaking their heads on more than one occasion. They held my hand throughout the process, and I will be forever indebted for their patience.

To cohort 1201 and 1202, I want to say that your support and friendship during the last 18 months made the long weeks away from home less stressful. We were all experiencing the same situations while away from family. I hope to continue these relationships in the future. Good luck, and God Bless you as your life's journey proceeds.

A special thank you goes out to my Executive Assistant Dawn Colla. A proof reader extraordinaire, she looked over every paper that I submitted and always found corrections that I could not have, even after re-reading it three times over. She should have been an English teacher.

Last but not least I want to thank my wife Julie. You have been a steadying force during this program. Your patience, love, and encouragement allowed me to grind it out! You epitomize the saying that 'beside every man who accomplishes great things in life stands a woman who deserves sainthood!' I can only hope to return to you in your endeavors what you have done in mine. I look forward to the transition of student back to that of husband.

I. INTRODUCTION

This thesis will examine domestic intelligence operations and other government activities that address the issue of maintaining the rule of law, while at the same time strengthening government's duty to prevent, deter, and disrupt terror plots, and identify terror cells and suspects post 9/11.[1] The USA PATRIOT Act that expanded government authority in the area of communication surveillance for a new kind of threat, is being debated in Congress in terms of how far domestic intelligence agencies are intruding into the lives of not only international citizens, but American citizens as well.[2]

There are issues about government overreach and encroachment into the privacy and civil liberties of American citizens. Congress expressed concerns over privacy and civil liberty implications by conducting hearings and passing laws. For example, Public Law 108-7 stopped all funding for the proposed Total Information Awareness (TIA) program, a sophisticated information technology program that collects, stores, and analyzes information, until the Pentagon could prove that the program does not violate privacy rights.[3] Congress has also criticized the Transportation Security Agency's Computer Assisted Passenger Prescreening System II that produces realistic full-body images because it potentially impacts the public's right to privacy and civil liberties.[4] Critics have labeled the program *virtual strip searches.*[5]

1Philip Bobbitt, Terror and Consent: The Wars for the Twenty-First Century, (New York: First Anchor Books, 2009), 290.

2Donald F. Kettl, System Under Stress: Homeland Security and American Politics, (Washington D.C.: CQ Press, 2007), 104.

3United States Department of Defense, Office of the Inspector General, 2003: DoD addressing concerns of Senators Grassley, Nelson and Hagel on safeguards against governmental abuse of power in developing technology programs, United States Department of Defense, http://www.hsdl.org/?view&did=443324.

4 Ibid., 5.

5 CNN report that criticizes body scanners as too revealing, http://fox6now.com,tsa-removes-body-scanners-criticized-as-too-revealing, 1.

Totally reshaping intelligence on the basis of what happened on September 11, 2001, and what was learned in the days following, is not good public policy.[6] It doesn't allow for considering the ramification of these changes and what new problems will arise as a consequence to wholesale changes.

The focus of this thesis will be to determine, through policy analysis, what policy options might better accomplish a balance between security and civil liberty in domestic intelligence operations that seem to be tipping the scales toward security and away from privacy, a decade after 9/11.

Authors, academics, and former intelligence veterans have written papers, books, essays, and journals on the danger of government intrusion into constitutionally protected areas, and how to balance that with providing law enforcement needed tools to protect against terror.[7] Former Secretary of State Colin Powell said,

> Terrorists are dangerous criminals and we must deal with them, but the only thing that can really destroy us is us. It is time for Congress to make the secrecy problem an issue of the highest priority and enact a sweeping overhaul of the national security establishment to re-impose democratic controls.[8]

Privacy and protecting the United States from terror are not polar opposites.[9] Many agree that the balance will change as the terror threat evolves, but that Congress must exert its power to monitor and regulate national security initiatives with more effective oversight.[10] Some have suggested the creation of a single intelligence-integrated community modeled after MI5 in the UK.[11] Concerns about domestic spying

---

6 Jennifer E. Sims, and Gerber Berton, Transforming U.S. Intelligence, (Washington, D.C.: Georgetown University Press, 2005), 18.

7 Bobbitt, Terror and Consent: The Wars for The Twenty-First Century. 289.

8 Michael German, and Stanley Jay, Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Secret Security Establishment, American Civil Liberties Union, (September 2011), http://aclu.org/files/assets/secrecyreport_20110727.pdf.

9 Samuel H.Clovis, Jr., Letter to the Editor: Twelve Questions Answered, Clovis answers questions from Chris Bellavita regarding Homeland Security, (May 2010), Naval Postgraduate School (U.S.). Center for Homeland Defense and Security, https://www.hsdl.org/?view&did=34925.

10 German and Stanley, Drastic Measures Required, 3.

11 Richard A. Best, Intelligence Reform After Five Years: The Role of the Director of National Intelligence.

have long been debated. In the 1990s, Senator Daniel Patrick Moynihan called for the outright abolition of the CIA on the grounds that it had demonstrated it uselessness for failing to forecast the fall of the Soviet Union.[12] There was an anti-intelligence sentiment growing in the public domain and Congress after the Cold War ended.[13]

That pushback is manifesting itself again with the recent disclosure by Edward Snowden, a government contract employee, that government may be stretching the meaning and interpretation of the rule of law.[14] On September 11, 2001, America was forced to face a new threat requiring new rules, after terrorists attacked the United States homeland.

Civil liberty advocates believe that domestic intelligence agencies working in so much secrecy are untrustworthy, and that it is an abandonment of a core American principle that a government working for the people and by the people must be transparent to the people.[15] A lack of transparency is problematic according to stakeholders representing civil liberty advocates, because in a democracy legitimacy of government action emerges from a process that is deliberate and largely open to the public.[16] Like the intelligence process at the national level, the domestic intelligence process used at the local level is soaked in secrecy. Withholding information allows the executive branch

12 Loch K. Johnson, The Aspin-Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission, Center for the Study of Intelligence, https://www.cia.gov/center-for-the-study-of-intelligence, 2.

13 L. Britt Snider, A Different Angle on the Aspin-Brown Commission, Center for the Study of Intelligence.

14Threats Test Obama's Balancing Act on Surveillance, New York Times, News story details President Obama's attempt to get control of the debate of balance and security after NSA contract employee Edward Snowden leaked classified documents about domestic intelligence surveillance activities. http://www.nytimes.com/2013/08/10/us/threats-test-obamas-balancing-act-on-surveillance.html?pagewanted=all&_r=0.

15 American Civil Liberties Union, Insatiable Appetite: The Government's Demand for New and Unnecessary Powers after September 11, (October 2002), https://aclu.org/FilesPDFs/insatiable appetite final.pdf, 1.

16 Ibid., 14.

which enforces the law, to insulate itself from public criticism, congressional and judicial oversight, which increases the likelihood of improper, unwise and illegal activity.[17]

17Elizabeth Goitein, and David M. Shapiro, Reducing Overclassification Through Accountability, Brennan Center for Justice, (2011), https://www.hsdl.org/?view&did=689494, 10.

II. BACKGROUND AND HISTORY

"He who would sacrifice liberty for security deserves neither liberty nor security."
Benjamin Franklin

A. GOVERNMENT SURVEILLANCE ACTIVITIES, TRANSPARENCY, PRIVACY ISSUES

This chapter will describe major issues surrounding public policy enactments following the terror attacks of September 11, 2001, including providing domestic intelligence agencies new tools for surveillance, and identifying what safeguards are needed as a check on expanded government authority, and the impact that resulted in the balance between security and liberty. The issues are:

- Privacy surrounding government surveillance authority in the digital age, classifying government activity in a veil of secrecy, and
- Calls for more transparency, an adversarial court mechanism and congressional oversight that will re-establish trust in government. The cost concerning these methods will also be analyzed.

The terror attacks against the United States on 9/11 and the Commission Report that followed caused major changes in the way the government goes about protecting Americans and the nation from further attack, and called for government to increase its presence in our lives.[18] A major finding by the Commission was that there were barriers to effective information sharing between federal, state and local law enforcement agencies called stovepipes, and these may have contributed to intelligence failure of 9/11. A quick reorganization was set up to bridge information sharing between law enforcement and domestic intelligence agencies instead of a methodical approach to

18 National Commission on Terrorist Attacks on the United States, (2004), http://www.911commission.gov/about/index.htm.

obtain clarity about the deficiencies that existed.[19] The Commission Report indicated the need for expanded government authority into areas that are constitutionally protected, in order to prevent future terror attacks.[20]

United States domestic intelligence operations and activities have an important role in protecting the American people from foreign and domestic threats that can affect the economic, physical and psychological well being of the country. This same domestic intelligence enterprise has a history of abusing, overreaching and infringing on civil liberty protections guaranteed by the U.S. Constitution, with unlawful wiretaps and surveillance as was discovered when the FBI spied on a wide range of political figures and organizations between 1956 and 1971.[21]

B. COMPETING INTERESTS OF PRIVACY AND SECURITY

The problem to be addressed is how a system can guard itself against terror events both man-made and natural, and which are intrusive, rare, unpredictable, and very costly.[22] The basis for this thesis is to make the argument on a policy recommendation for what can be called a *wicked* problem of simultaneously allowing agencies that have domestic intelligence responsibility the latitude they need to prevent, deter and preempt terror attacks, and ensuring that our privacy and civil liberties are kept intact, so that the foundation of limited government on which this country was established remains protected.[23]

The natural reaction for government (presidents) in a time of war is to seize power for itself, sometimes overreaching, citing national security interests as the reason. For example, Abraham Lincoln suspended Habeas Corpus during the Civil War, and

---

19 Ronald R. Stimeare, Is it Really Possible to Prevent Interagency Information-Sharing from Becoming an Oxymoron? Army War College, (March 2005), https://www.hsdl.org/?view&did=459181, iii.

20 Raphael Perl, National Commission on Terrorism Report: Background and Issues for Congress, (Library of Congress, Congressional Research Service, RS20598, February 2001), https://www.hsdl.org/?view&did=144.

21The 9/11 Commission Report, Location 312 of 2567, Chapter 3.

22Kettl, System Under Stress, 84.

23 Wicked problems are those that are difficult to solve because the information is often incomplete, contradictory and constantly changing. http://www.ac4d.com/home/philosophy/understanding-wicked-problems/.

President Franklin Roosevelt issued a detainment order in WW II of Japanese citizens.[24] Between 1960 and 1974, the FBI under J. Edgar Hoover, conducted surveillance and kept files on millions of Americans, including Dr. Martin Luther King Jr., (who was viewed as a potential threat), and other "subversives," all without a court conviction or court authority.[25]

The 9/11 terror attack on the United States was one of those situations where government officials felt a need to seize more power and engage in activities that appear to encroach on civil liberty and privacy in the name of national security interests. Today we call it homeland security.[26]

Foreign terror suspects were able to organize, plan and carry out the hijacking of four U.S. commercial airliners and fly them into the World Trade Center towers in New York City, and into the Pentagon. They killed nearly 3,000 people, shutting down the entire commercial airline industry for several days, and severely damaging the United States economy with damage estimates placed around $90 billion.[27] They were able to accomplish this using American travel, banking and communications systems.[28] There existed no coordinated way of tying this information together that could either track the suspects or identify a terror plot.

C. CONGRESS RESPONDS TO 9/11

The 9/11 Commission (The Commission) studied the pre-events of September 11, 2001, and it assessed the conditions, the agencies, the environment and the series of events that may have led to the attacks.[29] One of the findings from the commission was

---

24George W. Bush, Decisions Points, (New York: Crown Publishers, 2010), Kindle loc 3053. President Bush discusses wartime powers under Article II of the U.S. Constitution.

25 American Civil Liberties Union, History Repeated: The Dangers of Domestic Spying by Federal Law Enforcement, (2007), http://www,aclu.org/images/assets_upload_file893_29902.pdf, 2.

26 Shawn Reese, Defining Homeland Security: Analysis and Congressional Considerations, Congressional Research Service Report for Congress, (January 8, 2010), https://www.hsdl.org/?view&did=728387.

27 Bobbitt, Terror And Consent, 292.

28 Bush, Kindle, loc 3172.

29The 9/11 Commission Report, xvi.

that a reorganization of the intelligence community was needed.[30] This would not be the first attempt of this kind. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) followed, and this law finally achieved what many reform efforts had attempted since the passing of the National Security Act of 1947.[31]

New relationships were fused between agencies that previously could not or did not share information, referred to by some as *the wall.*[32] The problem was that no formal mechanism existed to share information. Information shortcomings referred to as stove piping--where information within an agency travels up and down in an organization with little sharing horizontally between organizations--prevented the reporting out of counter terror information.[33] It is hard to break down stovepipes when there are so many stoves that are legally and politically entitled to have cast iron pipes of their own.[34] The objective by the Commission was to replace a "*need to know"* culture with a "*need to share"* culture.[35]

An entire new federal agency, the Department of Homeland Security (DHS) was created to be the lead agency for problems that featured so prominently in the 9/11 attacks, such as border protection, securing transportation, immigration, Customs Service, critical infrastructure and organizing assistance to critical incidents.[36] The idea was to unify homeland security efforts from the current patchwork approach.[37] Fusions Centers and Joint Terrorism Task Forces (JTTF) were created at the state and local level to improve collection, analysis, reporting and sharing of information between local law

30 Ibid., 408.

31 Michael J. Warner, and Kenneth McDonald, U.S. Intelligence Community Reform Studies Since 1947, (Washington D.C.: Center for the Study of Intelligence, 2005), 38.

32 Bush, Kindle, loc 3172.

33Medhat A. Abuhantash, and Matthew V. Sholtz, From Stove-pipe to Network Centric Leveraging Technology to Present a Unified View, Command and Control Research Program (U.S.), (2004), https://www,hsdl.org/?view&did=455174, 1.

34The 9/11 Commission Report, 403.

35 Ibid., 417.

36 The 9/11 Commission Report, 395.

37 Bush, Kindle, loc, 3066.

enforcement agencies, the FBI and the DHS. This relationship coordinated by DHS would make state and local law enforcement a new player in counterterrorism investigations.[38]

Prior to 9/11, no executive department had as its first priority, the job of defending America from domestic attack.[39] The FBI was designated as the lead agency responsible for domestic intelligence.[40] Some have questioned whether the FBI is the appropriate agency for intelligence investigations because its culture and design are to gather evidence for arrest and prosecution, not on-going intelligence production.[41] This sensitivity to conducting investigations in compliance with the law has built in safeguards for privacy and civil liberty protection because the FBI has a cultural tendency to err on the side of *doing everything by the book*, evidenced by the Mohammed Atta investigation prior to 9/11.[42]

The Boston Marathon bombing, Fort Hood terror incident involving Nidal Hassan and the FBI's role in 9/11 with the Phoenix memo and known terrorist Zacharias Moussoui, demonstrate what can happen when a *downstream* agency like the FBI, that reviews past events as a basis for prosecution, instead of an upstream agency like MI5 that looks at information that may inform about future events, is designated with intelligence responsibility.[43] Intelligence services had information about the actors in these events before they were carried out.[44]

D. HOW MUCH IS TOO MUCH ENCROACHMENT AND WHAT OVERSIGHT IS NECESSARY?

A central question surrounding domestic intelligence post 9/11 is how much encroachment into the affairs of private citizens will Congress, courts, and the public

38The 9/11 Commission Report, 427.

39 Ibid., 395.

40 Ibid., 494.

41 Bobbitt, Terror And Consent: The Wars of the Twenty-First Century. 301–302.

42 Ibid.

43 Bobbitt, Terror And Consent: The Wars For The Twenty-First Century, 302.

44Kettl, System Under Stress: Homeland Security And American Politics, 23.

allow in conducting sensitive investigations, while not impeding the ability of domestic intelligence agencies to disrupt terror plans and identify suspects.[45] Whether Congress, the courts or public opinion should make those decisions has not been resolved, as 56% of Americans in a poll taken in July 2013, say that the federal courts fail to provide adequate limits on data collection and that mirrors the sentiment in Congress.[46]

Several pieces of legislation are being proposed that would curtail the seizing of metadata on Americans not suspected of terror involvement or any other crime. Metadata is the envelope of a phone call or Internet communication.[47] For a phone call it could include the duration of a call, the phone numbers involved, and when it happened. For an email it would include the sender and recipient, time, but not the subject or content, and in both cases it could include location information. Republican Congressman Justin Amash and Democrat Congressman John Conyers have introduced The LIBERT-E Act that would require the NSA to have a specific target if it is seeking phone records.[48]

The National Security Agency's (NSA) PRISM program has civil liberty advocates and members of Congress also asking whether these operations have gone too far.[49] The Commission Report initially pointed out the need to balance the interest of protecting the homeland and ensuring civil liberty protection when they said that the choice between liberty and security is a false one.[50] After the leak of the NSA secrets detailing the spying on American citizens who have not been accused of terror involvement, President Barack Obama in an interview stated that we cannot have 100%

45 Sims, *Transforming U.S. Intelligence*, 12.

46 Pew Research Poll, http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

47 Glen Greenwald, NSA collecting phone records of millions of Verizon customers daily, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

48 Ginger Gibson, Amash, Conyers introduce NSA bill, June 18, 2013, http://dyn.politico.com/printstory.ctm?uuid=2FABE059-3182-4411.

49 Spencer Ackerman, and Paul Lewis, U.S. senators rail against intelligence disclosures over NSA practices, http://www.theguardian.com/world/2013/jul/31/us-senate-intelligence-officials-nsa.

50The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. 1st ed. (New York: Norton, 2004), 395.

security and 100% privacy with zero inconvenience. These contradictory statements exemplify the competing opinions surrounding the balance of liberty and freedom.[51]

E. REORGANIZING U.S. INTELLIGENCE RAISES PRIVACY ISSUES

The only agency at the time of 9/11 with an intelligence role or authorization inside the United States was the FBI, and it was mainly in the area of counterintelligence.[52] Previous spying operations on U.S. citizens and groups led to congressional investigations that resulted in reform measures that prohibited the FBI from engaging in these operations, as well as prohibiting the Central Intelligence Agency (CIA) from collaborating with the FBI or engaging in operations within the United States. This raises the question about whether an integrated intelligence service would provide a better unity of effort, or through a model such as the Goldwater-Nichols Act, a paradigm for resolving large-scale bureaucratic problems.[53]

After the 9/11 attacks, federal law enforcement agencies, security services and the White House sought more authority and tools in order to be more effective in countering the emerging threat of terror being used as a tactic against the United States.[54] The World Trade Center bombing in 1993 was the first attack from this emerging adversary, but at the time the capability and intentions of the organization, identified as al Qaeda, was not yet clearly understood by the national intelligence community.[55]

F. EXECUTIVE AUTHORITY AS COMMANDER IN CHIEF AND CONGRESSIONAL OVERSIGHT

President George W. Bush declared a Global War on Terror (GWOT) soon after September 11, 2001. In framing it that way it gave the President, as Commander in

---

51 President Obama in a public address in Northern California fielding a question about the NSA spying program, June 7, 2013, http://rt.com/usa/obama-surveillance-nsa-monitoring-385/.

52 Loch J. Johnson, and James J. Wirtz, *Intelligence: The Secret World of Spies (*New York: Oxford University Press, 2008), 72.

53John Bansemer, Intelligence Reform: A Question of Balance, (U.S.: Air University Press, 2006-08), https://www.hsdl.org/?view&did=47037, 9.

54 Bush, Kindle, loc 3172.

55 The 9/11 Commission Report, 72.

Chief, authority under the War Powers Act to take action almost unilaterally to protect the homeland without authorization or pre-notification to Congress. For example, the use of Predator Drones to kill foreign terrorists abroad, a tactic used by President George W. Bush, has been expanded by President Barack Obama to include killing American citizens abroad without due process.[56] Might that eventually go on to include the use of Enhanced Interrogation Techniques (EIT) with Americans detained and suspected of terror involvement? The use of EIT such as sleep deprivation, hunger, water-boarding, long periods of standing harsh lights and excessive noise, to obtain vital information that might save thousands of American lives, has caused controversy and debate in Congress and the public about human rights violations.[57] There are legal and moral arguments for and against the use of torture as a tactic in obtaining vital information from enemy combatants.[58] As writer Mark Bowden put it, "The most effective way to gather intelligence and thwart terrorism can also be a direct route into morally repugnant terrain."[59]

The pattern has been that each succeeding U.S. president uses the policies that have been established before them, and then expands them to meet their own objectives or their own interpretations.[60] There ends up being an expansion of government authority and very little contraction where rights are restored to pre-crisis event status, especially with a *War On Terrorism* that likely has no end.[61] Various presidents get different interpretations of Article II of the US Constitution from White House lawyers.[62] Lincoln wiretapped telegraph machines during the Civil War, Woodrow Wilson ordered the interception of nearly every telephone and telegraph message into or out of the United

56 Kevin Johnson, and David Jackson, "Holder says four U.S. citizens killed in drone strikes," USA Today, http://www.usatoday.com/story/news/politics/2013/05/22/holder-citizens-killed-in-drone-strikes.

57 Bush, Kindle, loc. 3387.

58 Bruce A. Hoffman, "A Nasty Business," *The Atlantic Magazine*, 2002-01, http://www.theatlantic.com/magazine/print/2002/01/a-nasty-business, 1–6.

59 Mark Bowden, "The Dark Art of Interrogation," *The Atlantic Magazine*, http://www.theatlantic.com/magazine/archive/2003/10/the-dark-art-of-interrogation/302791/.

60 Bush, Kindle, loc. 3224.

61 Paul Shemella, Fighting Back: What Governments Can Do About Terrorism, (Stanford, California: Stanford University Press, 2011), 143.

62 Bush, Kindle, loc 3224.

States during WW I, and Franklin Roosevelt allowed the military to read and censor communications during WW II.[63] The NSA collecting metadata on American citizens not suspected of terror has a similar theme.

Terror organizations like Al Qaeda, unlike nation states that the U.S. intelligence community had become accustomed to facing, are for the most part, stealth and sophisticated operations and tend to operate in a decentralized structure.[64] Being decentralized means that they have spiritual and cultural leaders but no formal ones, and members do not necessarily take orders on when and how to attack adversaries.[65] These characteristics make terror organizations hard to track or identify, or to know when and where the next attack might be.[66] A terror group's network includes leadership roles, fundraisers, document forgers, bomb makers and recruiters.[67] Taking out or weakening one of these elements can disrupt a terror organization at least temporarily.[68] Because terrorists operate from a senseless state, information about them is difficult to identify because it ebbs and flows among ordinary people.[69]

In order for the agencies responsible for detecting, deterring, disrupting and preventing terror plots to identify those involved in the plan, law enforcement agencies need a more flexible process to deal with the emergence of the digital age in communications.[70] With advances in technology and the rights approvals, government can capture a person's digital exhaust, which is revealing data a human being leaves behind through activities like credit card purchases, cell phone use, Internet use and information on flying and driving from state to state.[71] Innovation means a more

63 Ibid., Kindle, loc 3238.

64 Ibid.

65 Ori Brafman, and Rod A.Beckstrom, The Starfish and The Spider: The Unstoppable Power Of Leaderless Organizations, (New York: Penguin Books, 2006), 20.

66 Ibid., 41–48.

67 Shemella, Fighting Back: What Governments Can Do About Terrorism, 39.

68 Ibid., 18.

69 Bobbitt, Terror and Consent: The Wars For The Twenty-First Century, 314.

70 Ibid., 310.

71 Dana Priest, and William M. Arkin, Top Secret America, (New York: Little, Brown and Company, 2011), 135.

streamlined process for securing the authority to obtain authorization for wiretaps and warrants so that time and resources can be efficiently managed.[72] These efficiencies however create privacy and civil liberty concerns because they short-circuit the traditional deliberate court approval process in place before 9/11.

G. CONGRESS PROVIDES FOR ENHANCED SURVEILLANCE AUTHORITY

The Patriot Act became the tool, the authority and the process to carry out necessary law enforcement activities and was intended to provide the judicial oversight needed to ensure privacy and civil liberty protection.[73] That satisfied the security issues but created a new dilemma. The Commission knew that abuses of civil liberties could create a backlash that would impair the collection of needed information.[74] These activities require that government engage in surveillance into constitutionally protected areas that then result in collection and recordkeeping on American citizens. Former DHS Secretary Michael Chertoff admits that by its very nature, domestic and homeland security intelligence work is intrusive.[75]

The USA PATRIOT Act has received much attention from civil liberty groups about government overreach in the area of privacy and civil liberty in the name of national security.[76] This law was put together without much debate, discussion or deliberation and voted into law nearly unanimously.[77] It has been described by psychologists studying the impact of terror on policy decisions made post 9/11 as fear-

72 Bobbitt. Terror And Consent: The Wars For The Twenty-First Century, 311.

73 Howard A. Johnson, Patriot Act and Civil Liberties; A Closer Look, March 15, 2006, https://?www.hsdl.org/?view&did=469628. 2–3 .

74 The 9/11 Commission Report, 424.

75Civil Liberties Impact Assessment for the State, Local and Regional Fusion Center, United States Dept. of Homeland Security, https:www.hsdl.org/?view&did=35177.

76 Julian Sanchez, Leashing the Surveillance State: How to Reform Patriot Act Surveillance Authorities, (Cato Institute, May 16, 2011), https://www.hsdl.org/?view&did=5259, 2–3.

77 Ibid., 2.

driven public policy.[78] This fear forces people to do things that they might not otherwise do except for the feeling of having to make a hurried decision.

A problem in getting coherent thinking on the risk of terrorism is that politicians find extreme and alarmist possibilities so much more appealing than discussions of broader context, much less of statistical reality. Hysteria and alarmism rarely make much sense but politicians and the media are drawn to them.[79] Psychology shows that when people feel vulnerable they are more likely to be trusting of government and give away rights without question. This psychology points out that aspects of fear can strongly influence the public's trust in and support of certain government policy that may not be in their best interest.[80]

Some of the complaints centered around the secrecy of not only the investigations and activities, but the actions approved by the Foreign Intelligence Surveillance Courts (FISC) under the Foreign Intelligence Surveillance Act (FISA).[81] The action of these courts are not adversarial, the wiretaps and warrants have been nearly unanimously approved, are not able to be appealed, and are sealed indefinitely to protect national security interests.[82]

This lack of transparency causes mistrust and can be a barrier to effective oversight by congressional committees tasked with this responsibility. This area of intelligence operations needs more discussion and debate according to civil liberty groups and members of Congress.[83] Congress and the public do not argue about the need to

78 James Breckenridge, and Philip G. Zimbardo, Psychology of Terrorism, (New York: Oxford University Press, 2007) The Strategy of Terrorism and the Psychology of Mass-mediated Fear, (New York Oxford University Press, 14).

79 John A. Mueller, A False Sense of Insecurity, Regulation, Vol. 27, No. 3, 42-46, Fall 2004. Available at SSRN: http://ssrn.com/abstract=604063.

80 Breckenridge and Zimbardo, The Strategy of Terrorism and the Psychology of Mass-mediated Fear, 118.

81 Eric London, Secret FISA Court Redefines Law to Justify Illegal Spying Operations, Global Research, (2013-07-09), http://www.global research.ca/secret-fisa-court-redefines-law-to-justify-illegal-spying-operations/5342183.

82 James G. Carr, "A Better Secret Court," New York Times, former FISC judge on how to improve FISA to create more balance and transparency and privacy protection without sacrificing security, http://nytimes.com/2013/07/23/opinion/a-better-secret-court.html?

83 The 9/11 Commission Report, 420.

protect people and to keep most activities confidential, but a policy needs to be put in place as a check on government overreach. Just trusting the government to do the right thing and to let the American people and Congress know when mistakes are made, sounds good, but it is not good public policy in terms of transparency or privacy and civil liberty protections.[84]

H. STATE AND LOCAL FUSION CENTERS AND JOINT TERRORISM TASK FORCES

Another area of concern by civil liberty advocates about the domestic counterintelligence apparatus, is privacy, and the activities of state and local fusion centers. After 9/11, pressure grew for a larger state role in counterterrorism.[85] The growth in the number of fusion centers after 9/11 added another layer of disparate local agencies that were collecting potentially valuable counter-terror information. Oversight, unity of effort, and a standard way of doing things to ensure privacy protections needed to be addressed. Local law enforcement plays a significant role in the homeland security enterprise. According to the DHS, there are 78 fusion centers with 70 Intelligence Officers (IO) assigned.[86] DHS officials indicate that state and local fusion centers are vital to protecting the homeland and produce intelligence products that are shared across this enterprise. They are at the front line in the collection and analysis phase; they are the eyes and ears in the field.

Civil liberties advocates questioned whether oversight of this added player in the domestic intelligence apparatus was adequate. They contended that the creation of new institutions like state and local fusion centers must be planned in a public, open manner with carefully thought-out and debated implications for privacy and other key values

84 Priest and Arkin, Top Secret America, 14.

85 Jay Stanley, and Michael German, What's Wrong with Fusion Centers?, American Civil Liberties Union (2007–2012), http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf.

86 Information Sharing Environment Annual Report to The Congress, (June 30, 2011).

important in a democracy.[87] This thesis will examine the consequences of unbridled authority by domestic intelligence agencies.

Intelligence fusion centers grew in popularity at the local level as officers tried to establish a role in defending the homeland by developing their own intelligence capabilities.[88] This expansion took place outside any legal framework for regulation, leading to a disparate collection of centers, defining their own mission and tailored to meet local or regional needs[89] This allows fusion centers to operate in what has been described as no man's land with little public oversight or standardized training, rules, or policies.[90] The missions, objectives, standards of operation and policies are all different, leading to the potential for privacy and civil liberty abuses.

DHS and the FBI are the primary sources of information between state and local law enforcement and are responsible for coordinating such a vast pool of disparate local and private agencies.[91] In a recent Congressional hearing however, one DHS official described the fusion center as the "wild west," where officials are free to use a variety of technologies before politics catches up and limits the options.[92] For example, the use of tracking devices by local law enforcement without a search warrant brought privacy rights into question. Federal authorities are happy to reap the benefits of working with fusion centers without officially taking ownership.[93]

In October 2012, a congressional study by the Homeland Security and Government Affairs Committee had some members of Congress raising questions about

87 Stanley and German, What's Wrong with Fusion Centers?.

88 Ibid.

89 Ibid.

90 Stanley and German, What's Wrong with Fusion Centers?

91Mark A. Randol, Congressional Research Service, The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress, March 19, 2010, www.crs.gov, R40602.

92 Stanley and German, What's Wrong with Fusion Centers?

93 Ibid.

the effectiveness of fusion centers in the area of counterintelligence capability.[94] Originally designed with the intention of improving counterintelligence collection and analysis, their mission has morphed into an all-crimes drive focus with little produced in the way of counterterrorism intelligence.[95]

The National Association of Fusion Centers authored a letter countering the senate subcommittee study, and in it denied many of the findings and reaffirmed their value to their local communities, but offered only rhetorical claims of substantial value in the area of counterintelligence or counterterrorism.[96] An article that appeared in *Police Chief* magazine on the role of fusion centers in counterterrorism operations sounded a conflicting message when it indicated that detailed analysis of counterterrorism intelligence is not the role of fusion centers.[97] This serves as another example for examining the benefits of a single, integrated domestic intelligence agency for unity of effort.

The focus of the questions being asked by the senate permanent subcommittee on investigations was whether fusion centers need more standardization of policies and procedures, about training of officers for proficiency and competency in the area of privacy and civil liberty protections, and about the poor quality of the reports that are submitted for sharing purposes.[98]

Gaps in information sharing continue to plague domestic intelligence and counterterrorism operations. The 9/11 Commission talked about the need for unity of effort and unity of command in intelligence and counterterrorism operations overseas and

---

94Federal Support for Involvement in State and Local Fusion Centers, Majority and Minority Staff Report, Permanent Subcommittee on Investigations, United States Senate, United States Congress. Senate Committee on Homeland Security and Government Affairs., (October 3, 2012), https://www.hsdl.org/?view&did=723145, 93.

95 Ibid.

96 IACP, MCC,MCSA, NFCA, ASCIA, NSA, NGAHSAC. Response To The Senate PSI Report Joint Statement, https://nfcausa.org/default.aspx?menuitemid=167&menugroup=Home+New.

97The Police Chief, February 2013, http://www.policechiefmagazine.org, 26.

98Federal Support for Involvement in State and Local Fusion Centers, Majority and Minority Staff Report, Permanent Subcommittee on Investigations, United States Senate, United States Congress.

at home.[99] Whether the domestic intelligence approach using fragmented federal, state and local law enforcement agencies can bridge the divide for a better flow of information up, down and across the enterprise will be examined in the policy options section of this thesis. An analysis of whether the United Kingdom approach to an integrated intelligence agency (MI5) would work in the U.S. will be proposed in Chapter IV. The Goldwater-Nichols reform legislation of 1986, that brought joint capability to the then fragmented military, has been proposed as a way forward to achieve integration among agencies with similar objectives, like law enforcement.[100]

Congress was contemplating pulling back on *all* state and local fusion center funding after it learned that very little valuable counterterrorism intelligence was emanating from fusion centers.[101] Losing funding could cripple local law enforcement efforts in counterterror intelligence due to state budget cuts for police agencies. Fusion centers were intended to advance a federal objective relating to anti-terror initiatives, not local objectives like crime.[102]

State and local fusion center privacy restriction is codified under federal regulation 28 C.F.R. Part 23. The law prohibits state law enforcement agencies that receive federal funding from collecting or maintaining personal information about individuals in criminal intelligence databases unless, *there is reasonable suspicion that the individual is involved in criminal conduct and the information is relevant to that criminal conduct.*[103] Several observations arise here. First is that in counterterrorism intelligence investigations oftentimes you don't know specifically who or what the target is at the onset of the investigation. Second is that the Privacy Act and some other federal laws do not apply to the states conducting information gathering. Third is that 28 C.F.R

99 The 9/11 Commission Report, 399–410.

100 The 9/11 Commission Report, 403.

101Senate Permanent Subcommittee on Investigations, http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

102 Ibid., 4.

10328 C.F.R. Part 23.20(a).

Part 23 says that fusion centers that *receive federal funding* must comply. What about fusion centers which do not receive federal funds? Can they operate under less restrictive guidelines?

Questions remain as to a system of sufficient checks and balances to prevent abuse and who would provide oversight of their activities, records and reports.[104] With few minimum standard operating procedures or policies between these disparate law enforcement agencies, it sets up a system by which authorities can manipulate differences in federal, state and local laws and policy shop to maximize their information-gathering potential.[105]

An additional concern is that if the information gathered by police is illegally obtained or done in error and then used in a vast sharing domain, the entire system becomes contaminated with the unlawfully obtained information. Worse yet is that arrests and prosecutions can end up being based on illegally obtained information in violation of someone's civil liberty or privacy.[106]

I. COST OF MAINTAINING GOVERNMENT SECRETS

Are the gains in security worth the funds expended?[107] The cost associated with homeland security domestic intelligence operations such as infrastructure protection, government surveillance, secrecy, and classification of documents and information has come into question. In the years immediately following the terror attacks of 9/11, it was understandable to initiate new public policy and to spend whatever was needed to protect the homeland.[108] The problem however is that policymakers and Congress have not properly assessed the return on investment.

104Todd Massee, and John Rollins, Summary of Fusion Centers; Core Issues and Options for Congress, CRS Report for Congress, (July 19, 2007), https://www.hsdl.org/?view&did=479037, 5.

105Stanley and German, What's Wrong With Fusion Centers? (December 2007), www.aclu.org.

106 New York Times story by Susan Jo Keller that details the arrest by the FBI of a lawyer from Oregon who was mistakenly linked to the Madrid train bombings in March 2004, http://www.nytimes.com/2007/09/27/washington/27patriot.html?n=Top/Reference/Times%20Topics/People/M/Mayfield,%20Brandon&_r=0&pagewanted=print.

107 John Mueller, and Mark G. Stewart, Terror, Security And Money: Balancing Risks, Benefits, and Costs of Homeland Security, (New York: Oxford University Press, 2011), 1.

108 Ibid.

A source of harm is identified and then money is spent to do something about it without ever justifying the cost.[109] Infrastructure protection such as the commercial airline industry was secured by the formation of the Transportation Security Administration (TSA) that has an annual budget of $8.2 billion dollars.[110] Enhancing resiliency by fortifying cockpit doors at a cost of $30-50,000 each, for a total of about $40 billion from a cost benefit analysis made more sense economically and with less inconvenience to airline passengers. This may also have negated the need to intrude into the privacy of airline passengers with screening, and may have saved airline corporations the cost associated with flight delays.

After the 9/11 attacks, Osama Bin Laden's stated goal was to bankrupt the United States on security spending.[111] Over the last decade, spending on homeland security activities has increased by $360 billion and the total exceeds $1 trillion.[112] More homeland security spending, means less money available for education, healthcare, economic development, housing, infrastructure improvements, and national defense.

Some of the cost is associated with overlap and duplication by having so many different agencies involved in homeland security activities each with their own mission, their own culture and their own reporting systems.[113] This struggle in developing a *true fusion process* to fill gaps in information sharing, a proactive collection of information and value added analysis still remains.[114] Might this be accomplished by having a single integrated domestic intelligence agency? This policy option will be examined further in chapter three.

Determining the appropriate level of homeland security spending requires thoughtful and rational debate and discussion outside the realm of hyperbole, hysteria and

109 Mueller and Stewart, Terror, Security, And Money: Balancing the Risks, Benefits, and Costs of Homeland Security, 6.

110 Ibid., 137.

111 Ibid., 3.

112 Ibid., 1,3.

113 Masse and Rollins, Summary of Fusion Centers: Core Issues and Options for Congress, CSR Report for Congress, 7.

114 Ibid., 12.

fear that often dominates the discourse.[115] If we do not have this dialogue now, more than ten years removed from the fog of 9/11, and ask ourselves if the policies we are enacting to defend the homeland are lawful and reasonable, we might lose on both fronts.

Balancing security and liberty, the main thrust of this thesis, is important in our approach to domestic intelligence activities in the United States. After ten plus years, the debates in Congress, the media and the public, are increasing to the point of blowback.[116] This may result in the domestic intelligence enterprise returning to operating at a distinct disadvantage as it was forced to do prior to the 9/11 attacks under laws governed by the Privacy Act. Prior to the passage of the USA PATRIOT Act, a higher government threshold for obtaining court orders to search suspect activity was the standard for government surveillance.

J. METHODOLOGY

Using policy options analysis, I will examine three homeland security policies. After an analysis of the impact of those policies on the three key stakeholder groups, I will develop a policy recommendation that satisfies privacy protections of civil liberty advocates, security needs for domestic intelligence agencies and that will be found to be politically acceptable to members of Congress and the American public.

I will conduct this policy analysis using six steps:

- Analyze the problem (see Chapter II)
- Identify criterion that will mitigate the problem
- Analyze alternative policy choices as solutions
- Compare the alternatives against the criteria to determine the advantages and disadvantages of each policy
- Recommend a preferred policy
- Suggest a way to implement the policy

115 John A. Mueller, Risk analyst David Banks commenting on realistic reactions versus hyperbolic overreaction to improbable contingencies, A False Sense of Insecurity. Regulation, Vol. 27, No. 3, 42-46, Fall 2004. Available at SSRN: http://ssrn.com/abstract=604063.

116 Madhani and Jackson, USA Today, news story on whether keeping surveillance programs cloaked on secrecy is vital to effectiveness, with NSA controversy, debate over secrecy is revived, http://www.usatoday.com/story/news/politics/2013/06/12.

Policy alternatives that will be examined are the following:

- Examining the status quo allowing government agencies expanded intrusion into areas previously constitutionally protected.
- Dismantling the fragmented approach to U.S domestic intelligence and replacing it with an integrated security agency and the consequences that would result. An examination of MI5.
- Strengthening trusted oversight mechanisms currently in place and determining an adequate oversight metric to audit progress and reporting and making adjustments when necessary to sustain the appropriate balance of privacy and security.

A recommendation will be made from those alternatives as a way forward until future problems arise. This balance between security and liberty will always need to be revisited as new technologies emerge and the means with which government can exploit conducting intelligence operations changes quickly.

This chapter has covered the extensive background of U.S. domestic intelligence, identified key issues, provided a problem statement and posed the research question to be answered in this thesis. Areas of controversy are:

- Expanded government surveillance authority
- Effective congressional and judicial oversight of domestic intelligence activities to prevent privacy abuses
- The disparate nature of U.S. domestic intelligence and whether a single domestic intelligence service like MI5 would instill more accountability.

Chapter III will be a review of the literature on the issue of domestic intelligence activity and the impact it is having on privacy and civil liberty in the years following 9/11.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

A. INTRODUCTION

In the aftermath of the September 11, 2001, terror attacks on the United States, a new concept made its way into the American lexicon. We call it homeland security. America was made to face the reality that our security and the way of life we had taken for granted would have to change. Our national government scrambled to give Americans peace of mind about their safety in the days and years that followed the attacks in New York, Pennsylvania and Washington D.C. On the other side of the discussion are civil libertarians, who fear giving government a blank check to determine the cost of this expanded encroachment on privacy and civil liberties.

This literature review will examine government reports, research and writings by noted authors, speeches by government officials, and essays and journals, and lay out what is generally agreed on in the areas of civil liberty and homeland security. Additionally, literature review will be on issues and concerns that have arisen in the decade following 9/11, which saw expanded government authority granted to domestic intelligence agencies. Questions have arisen as to whether a red line exists for advocates of civil liberties where they begin to push back in the direction of more liberty at the expense of security.

B. WHERE IS THERE AGREEMENT?

The themes that emerged from the literature review focused on balancing the need for further government intrusion to protect the homeland; stricter oversight of domestic intelligence agencies that include the Federal Bureau of Investigation, Joint Terrorism Task Forces and state and local fusion centers; and a lack of public trust of government operating in secrecy. There is almost universal agreement through the literature reviewed of the need to balance security with maintaining liberty, and that the choice between liberty and security is a false choice.[117] The 9/11 Commission Report to Congress

[117] The 9/11 Commission Report: *Final Report of the National Commission on Terrorist Attacks Upon the United States. 1st ed.* (New York: Norton, 2004), 395.

pointed out that in wartime, government calls for greater power, and then for those powers to recede after the war ends.[118] The Global War on Terror (GWOT) is in its eleventh year with no end in sight. The public tends to be willing to forego individual freedoms in the early stages following a terror attack, but as they move further from the event, the infringements on their liberty spark intense debate. Protecting civil liberties, while effectively combating terror, continues to be debated in Congress.

The literature points out that the push for more government security at the expense of civil liberty is not coming from the public, but rather from government domestic intelligence agencies and officials. In August 2002, the National Commission on Terrorism (NCT) argued for a more aggressive strategy in combating terrorism.[119] Critics of this approach argue that those conclusions and recommendations ignore U.S. privacy interests that might lead to curbing individual rights and liberties.[120]

Another report for Congress raises questions in responding to anti-terror efforts, stemming from the conflict between individual privacy interests and the intelligence needs of law enforcement and national security.[121] Instead of looking for balance, the NCT report previously cited advances that push for more government intrusion by calling for *all* government agencies to use *every* available means to thwart terrorism.[122] With the roles that technology and the Internet play in the GWOT, critics fear that the potential for abuse and harm by government officials with an increased capacity to assemble information, will result in increased and unchecked government power.[123]

Review of a journal article on the question of sacrificing liberty in the name of increased terrorism protection points out the good news/bad news result. The author

---

[118] Ibid., 394.

119 National Commission on Terrorism. Countering the Changing Threat of International Terrorism, Report of the NCT, 105th Congress, https://www.hsdl.org/?view&did=992.

120 CRS Repot for Congress RS21915, Privacy: Key Recommendations of the 9/11 Commission, (August 2004), https://www.hsdl.org/?view&did=727019, 2.

121 Gina Marie Stevens, and Harold C. Relyea, Key Recommendations of the 9/11 Commission, CRS Report for Congress.

122 National Commission on Terrorism, Countering the Changing Threat of International Terrorism, Report of the NCT, 105th Congress, https://www.hsdl.org/?view&did=992 Executive summary.

123 Stevens and Relyea, Key Recommendations of the 9/11 Commission, 2.

writes that the domestic intelligence system appears to have been successful in increasing security within the U.S., but that the gains are coming at the cost of ever-increasing domestic surveillance and at the risk of civil liberties.[124] The public is not asking to have their freedom from unnecessary government intrusion scaled back. It is becoming a situation of mandatory compliance. Critics argue that the balance between security and liberty has shifted firmly toward security, leading to greater government power. [125] Oversight by the same branch of government that is executing domestic intelligence raises issues of credibility in the watch system.

A 2007 American Civil Liberties Union report about state and local fusion centers, raises serious privacy issues at a time when government power and zeal in the GWOT are threatening privacy at an unprecedented level.[126] In the report they express that fusion center planning and design for the most part occurred without public planning or debate. Little training of personnel has taken place on civil liberty protection and the potential for abuse is great.

Public trust is a common theme in the literature due to the sensitive nature of what the government is doing in spying on U.S. citizens. In a Pew Research Center study on American trust in government, a poll showed that a majority of Americans (53%) think that the federal government threatens their rights and freedoms.[127] In a system of government that derives its authority by the consent of the governed public, trust is at the foundation of the policies of homeland security. The report goes on to indicate that for the first time, a majority of the public says that the federal government threatens their personal rights and freedoms.[128]

---

124 Eric J. Dahl, Domestic Intelligence Today: More Security but Less Liberty? Homeland Security Affairs Journal, (September 2011), https://hsdl.org/?view&did=691059.

125 Ibid., 5.

126 American Civil Liberties Union, What's Wrong With Fusion Centers? (December 2007), www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf, Executive summary.

127 The Pew Research Center, For The People & Press, (January 31, 2013), www.people-press.org, 4.

128 Pew Research Center Report, 1.

Another review of literature concerning government threatening personal rights and freedoms points out that this lack of trust transcends political party affiliation and political ideology. Whether political partisanship plays a role in privacy protections, one author argues that both political parties have sought to maximize government's control over its citizenry.[129] Author James Bovard cites instances showing that erosion of personal rights have occurred in the Clinton, Bush and Obama administrations, with increases in wiretapping and searches of electronic communications due to emerging technology.[130]

Government use of emerging technologies to spy on people in public spaces has raised concerns from civil liberty advocates. In a review of literature from the General Accounting Office on the use by law enforcement of closed circuit television to monitor public areas to combat terrorism, civil liberty advocates stress the need for controls to ensure individual privacy that establish supervision, training requirements, public notification and periodic audits.[131] Written policies, standard operating procedures, along with credible training and oversight through periodic audits, are a common theme in much of the literature. The ACLU and the Electronic Privacy Information Center (EPIC) and the American Bar Association (ABA) are a few of the watchdogs of government's expanding authority post 9/11. The ACLU and EPIC have argued that the use of surveillance systems to monitor public spaces may, nevertheless, infringe upon freedom of expression under the First Amendment, believing that it might "chill" protestors from demonstrating in public spaces.[132]

In a review of literature on fusion center recommendations, a group of policy experts and legal practitioners write that although fusion centers have the potential to strengthen the nation's counterterrorism efforts, without effective limits on data

---

129James Bovard, Are Democrats Better on Privacy and Surveillance? The Future Of Freedom Foundation, (December 2012), https://www.hsdl.org/?view&did=231875.

130 Ibid.

131 United States General Accounting Office, Report to the Chairman, Committee on Government Reform, House of Representatives Video Surveillance: Information on Law Enforcement's Use of Closed Circuit Television to Monitor Selected Federal Property in Washington D.C., (June 2003), https://www.hsdl?/view&did=437710, 2.

132 Ibid., 8.

collection, storage, and use, these centers can pose serious risks to civil liberties, including rights to free speech, free assembly, freedom of religion, and the right to be free of unnecessary government intrusion.[133] The lack of mandatory compliance to any consistent standards is cited often in reports on state and local fusion centers. The recommendation report points out that any time law enforcement agencies collect information on people in the United States it could result in the creation of vast databases compiled on individuals without reasonable suspicion that they are linked to any terrorism or criminal activity.[134] A lack of proper training, reporting, and oversight came up in this report as well.

One of the most pressing concerns involving fusion centers is a lack of accountability due to the secrecy that surrounds these centers, which makes public oversight more difficult.[135] Secrecy surrounding the domestic intelligence enterprise makes it difficult to determine whether effective and consistent oversight is occurring and whether civil liberties are actually being safeguarded. Authors Priest and Arkin raise the concern of potential civil liberty abuse in the name of national security. They refer to it as government being allowed to *operate in the dark.*[136] In their book, *Top Secret America,* they cite testimony by CIA Counterterrorism Center head, Cofer Black, who told Congress that he had been granted new forms of "operational flexibility" in dealing with suspected terrorists, and followed that up by telling Congress it was all they needed to know.[137] This makes it difficult for Congress to perform effective oversight.

These same authors explore the government's use of Predator drones that had been hidden in layers of government secrecy.[138] The use of drones for surveillance in the United States by domestic intelligence agencies including local police and fusion centers

133 The Constitution Project, Recommendations For Fusion Centers, Preserving Privacy and Civil Liberties. While Protecting Against Crime and Terrorism, (2012), www.constitutionproject.org/pdf/fusion center report.pdf, Preface.

134 Ibid.

135 Ibid.

136 Dana Priest, and William M. Arkin, Top Secret America, (New York: Little, Brown and Company, September 2011), xx.

137 Ibid., 14.

138 Priest and Arkin, Top Secret America, 14.

has become a topic of much controversy, not only in Congress, but in state legislatures as well. Several states have already passed laws and more are drafting legislation banning the use of these surveillance devices, seeing them as too much of an encroachment on privacy and civil liberties.[139]

In a related review of writings on the tug of war to determine just where the line should be drawn between stronger powers the government insists are needed to protect Americans from terror, versus the protections of civil rights and liberties that are fundamental to American democracy, academic Donald Kettl writes and lectures about balancing liberty and protection.[140] In writing about the Patriot Act, he indicates how civil libertarians worried that Congress would rush to enact sweeping new legislation without deliberating on the impact it would have on civil rights and civil liberties, while security experts struggled to find a way to balance civil liberty against the need for a stronger homeland defense.[141]Kettl, like Bovard had mentioned previously, points out that people describing themselves politically as libertarians, conservatives, as well as liberals, worry that post 9/11 changes have the potential to place too many restrictions on liberty.[142]

C. WHERE IS THERE DISAGREEMENT?

A review of the literature citing the need for increased government power for domestic intelligence agencies in the GWOT is framed as the price to be paid in protecting the homeland. Domestic intelligence agencies are one of the few government entities in support of expanded government encroachment at the cost of civil liberties. The literature reviewed in this area does not indicate that government domestic

139Catherine Crump, and Jay Stanley, Why Americans Are Saying No To Domestic Drones, Future Tense, (February 11, 2013), http://www.slate.com/articles/technology/future_tense/2013/02/domestic_surveillance_drone_bans_are_sweeping_the_nation.html.

140Donald F. Kettl, System Under Stress: Homeland Security and American Politics, CQ Press, (2007), 117.

141 Ibid., 104.

142 Ibid., 117.

intelligence agencies come right out advocating for infringing on civil liberties. Instead, their narratives focus solely on the need for more security.

A *New York Times* newspaper article (May 7, 2013), writes about a push by the FBI to overhaul surveillance laws that would make it easier to wiretap people who use the Internet, aimed at preserving law enforcement officials' longstanding ability to investigate suspected criminals, spies and terrorists due to evolving technology.[143] The article points out that this plan will likely set off debate over the future of the Internet, according to lawyers for technology companies, over Internet privacy and freedom.[144]

In a review of a lecture by scholar Tom O'Conner (PhD), he outlines the practice of government's infringing on civil liberty by retaining law and order at any expense, and points out that Thurgood Marshall stated that grave threats to liberty often come in times of urgency.[145] The issue of how to balance fighting terror and protecting liberty is difficult to achieve and even harder to maintain. O'Conner's lecture touches on how terror attacks unfortunately lead to inflating every national security crisis into the need for some overly repressive "do anything, do something" knee-jerk response, but that there may in fact be no need for new laws, new agencies, or new government powers.[146] Expanded government intrusions following 9/11 make it easier today for authorities to justify secret wiretaps and surveillance since probable cause under the Foreign Intelligence Surveillance Act (FISA) lowers the threshold of evidence for warrant approval.[147]

143Charlie Savage, http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?ref=surveillanceofcitizensbygovernment&_r=0.

144 Ibid.

145 Dr. Tom O'Conner's Criminal Justice Megalinks, http://faculty.ncwc.edu/toconner, (May 2004).

146 Ibid.

147 Ibid.

In reviewing an article on the need for fusion centers to spy on U.S. citizens without legal authorization, one Arkansas fusion center director indicated that they spy not on Americans, just on anti-government Americans. He then played the patriotism card saying, "*I do what I do because of what happened on 9/11. There is this urge, this feeling inside that you want to do something.*[148]

The literature generating the most disagreement and controversy is on the Patriot Act. This act, according to a report from the ACLU, expanded government authority to pry into the private lives of people whether or not there is any evidence of wrongdoing.[149] Proponents of the act say that reducing individual liberties during a time of national security crisis is both reasonable and necessary; that if a person isn't doing anything wrong there should be no fear.[150] This report was in anticipation of the reauthorization of certain provisions of the act to be taken up by Congress.

The Department of Justice on its website issued a report defending the need for the Patriot Act, downplaying its controversy by indicating that Congress took existing principles and slightly modified and updated them so law enforcement could deal with new threats and technology used by terrorists in the GWOT. Many others see this as the most substantial change in the government's relationship with its citizens since the American Revolution.[151]

D. CONCLUSION

The question of what should be the reach of government in its domestic intelligence responsibility is as controversial today as it was after the creation of the Department of Homeland Security, the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPR), and the Patriot Act. There are problems with

148 Mike Masnik, Homeland Security, "Fusion Center Director: We're Not Spying on Americans…Just Anti-Government Americans," http://www.techdirt.com/articles/20130402/02150622543/homeland-security-fusion-center-director-were-not-spying-americans-just-anti-government-americans.shtml.

149 American Civil Liberties Union, Reclaiming Patriotism: A Call to Reconsider The Patriot Act, (March 2009), www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf, Executive Summary.

150American Civil Liberties Union, Reclaiming Patriotism, 8.

151Kettl, System Under Stress: Homeland Security And American Politics, 117.

oversight in an area where government secrets preclude outside stakeholders like the ACLU, Congress, and the general public, from effectively keeping watch on government activities. It is being questioned by congressional members, the media and privacy advocates, and will be expanded on in Policy Option Three (More Effective Oversight) whether the government should be allowed to monitor itself or whether a non-governmental entity would build objectivity into the oversight process.

If a gap exists in the literature on civil liberties and domestic intelligence, it surrounds who the arbiter should be as to when intrusion is enough or too much. It is difficult to establish a metric by which to gauge. It comes down to a sentiment on how much latitude Congress and the American people are willing to allow domestic intelligence to intrude into constitutionally protected areas. Since terror attacks happen so infrequently we have to ask ourselves is any of it worth eroding away our deeply held concept of limited government.

Chapter IV will identify the stakeholders involved in balancing security and liberty. These stakeholder groups have quasi-veto power in any policy formation and can derail any alternative policy recommendations by legal means, increased secrecy, political means, and public relations campaigns.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. POLICY ALTERNATIVES

The 9/11 terror attacks on the United States caused a change in the way federal, state and local law enforcement and security agencies go about preventing, detecting and disrupting terror plots and identifying terror suspects, organizations, terror financing, travel, recruitment and communications. Terror suspects and organizations exploit the Internet to accomplish these activities.[152]

The consequence of this is that the rise of the digital era for transfer of information on a never-before-seen level requires new surveillance activities and techniques.[153]The Internet also is used by people who are not suspected of terror involvement. Sorting it out sometimes requires vast collection of private information of Americans not suspected of terror.[154] This is where the balance of security and liberty questions arises. These policy alternatives will explore what operational policy will insure a more consistent application of the law to protect privacy, what policy will keep in place enhanced surveillance techniques, and what policy will lead to more effective oversight?

In order to solve the issue of balancing security and privacy, three stakeholder groups have been identified. They have been determined as stakeholders based on the role they occupy in the apparatus or because their political influence will be needed for acceptance of any policy recommendation that will be made. The stakeholders are civil liberty advocates, namely the American Civil Liberties Union; governing bodies including Congress, the Executive and Judicial branches; federal, state and local law enforcement and national security agencies; and finally advocates for a single streamlined domestic approach. The main issues are privacy protections, effective oversight, and

[152] Michael Jacobsen, *Terrorist Financing and the Internet*, (2010), Studies in Conflict & Terrorism, 33: 4, 353-363, http://dx.doi.org/10.1080/10576101003587184.

[153] Sims and Gerber, Transforming U.S. Intelligence, 7.

[154] Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 311.

effective domestic intelligence operations. We must look across the boundaries that divide these interests and disparate objectives and come to a collaborative policy recommendation that accommodates each entity's needs.[155]

In a representative democracy if stakeholders feel that their views are underrepresented they will go away feeling bitter and will work to undermine the entire process.

A. CIVIL LIBERTY INTEREST GROUPS

The civil liberty organization that has led the way in objecting to the way the U.S. government has reacted in the years following the attacks of September 11, 2001, has been the American Civil Liberties Union (ACLU).

Their objections center on surveillance of anyone generally, but American citizens specifically. The First Amendment's free speech and assembly, and the Fourth Amendment's protection against unreasonable searches and seizures without a warrant, are several of the constitutional protection items usually cited as at issue by privacy advocates.[156] The objections not only involve people in traditional constitutionally protected areas such as their persons, places and effects, but in the public sphere as well, as the use of government security cameras and automated license plate readers used by law enforcement agencies increases.[157] Civil liberty advocates generally hold a mistrust of government and while they see oversight of government operations as somewhat of a check on abuses, they favor more transparency in government operations.[158]

This position comes into conflict with the need to sometimes hide activities to protect informants that can include people from friendly nations. Letting that kind of

---

155 William Bratton, and Zachary Tumin, Collaborate or Perish: Reaching Across Boundaries In A Networked World, (New York: Crown Press, 2012), 3.

156Statement on Reforming the Patriot Act: A Report by the Constitution Project's Liberty and Security Committee, The Constitution Project, (2009), https://www.hsdl.org/?view&did=685217, 1.

157 Justin George, "ACLU says license plate readers violate drivers' privacy," *Baltimore Sun*, July 17, 2013. ACLU says lack of rules for collection, storage of information is too broad. http://www.baltimoresun.com/news/maryland/crime/blog/bs-md-license-plate-readers-20130717,0,4598979.story.

158 German and Stanley, Drastic Measures Required: Congress Needs to Overhaul the U.S. Secrecy Laws and Increase Oversight of the Security Establishment, 23–33.

information out might discourage people and other nations from sharing information with the United States for fear of retaliation by other states, and in the case of individuals it may cost them their lives. Civil liberty groups have offered alternative recommendations that would meet their mission as a government watchdog.[159] The ACLU indicates that Congress has ample constitutional authority to control the "secrecy regime," and that the Constitution gives Congress a pre-eminent role in national security issues under Article I, Section 8, Clause 11 and Section 9, Clause 7.[160]

B. DOMESTIC INTELLIGENCE COMMUNITY

Any policy recommendation will have to satisfy the concerns of agencies with domestic intelligence responsibility. Their concern is having the tools needed to prevent, detect and disrupt terror plots and to identify terror organizations and individuals in a globally connected network with vast digital communications capability.[161] Among those are the National Security Agency, the FBI, DHS I&A, CIA, Immigration and Customs Enforcement (ICE) along with state, local and tribal law enforcement. Law enforcement and security agencies tout that they are sensitive to protecting privacy but their actions sometimes tell a different story.[162] The claim often cited is that everything they (government domestic intelligence agencies) do is in the interest of protecting the nation from future terror attacks. From the White House down to the local level, however, are examples where privacy took a back seat to security interests and that those objectives continually push its boundaries outward.[163] The danger in dismissing this group in any

159 Ibid., 34–38.

160 German and Stanley, Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Security Establishment, 35.

161 Bush, *Decision Points*, NSA chief General Hayden tells President Bush that he had the technical capacity but not the legal authority to do it without getting a court order which he described as difficult and slow, Kindle, loc 3217.

162 German and Stanley, Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Security Establishment, 26–28.

163Charlie Savage, "U.S. Weighs Wide Overhaul of Wiretap Laws," *New York Times*, May 5, 2007, article on how the FBI is looking to expand surveillance authority to include people using the Internet for making phone calls, http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?pagewanted=all.

policy change is that they may as they have in the past exhibit resistance in the form of increased classification of information and decreased transparency.

C. CONGRESS

For members of Congress the issues are more self-interest in nature. No politician wants to be thought of as being soft on national defense, block funding for homeland security needs, or wants to be wrong about the next attack occurring.[164] They know that some government activities, although distasteful, are necessary, and at the same time declare publicly at every opportunity their obligation to uphold the Constitution and to protect privacy. The House of Representatives narrowly defeated a move to shut down the NSA's domestic phone record tracking program amid shifting poll numbers showing public concern for privacy, by a 217-205 vote.[165]

Soon after the 9/11 terror attacks, Congress approved sweeping changes in the passage of the USA PATRIOT Act in the way that domestic intelligence agencies track the origin and destination of electronic communications.[166] This broad wiretap and surveillance authority brought on questions and concerns from civil liberties advocates about oversight mechanisms and systems to prevent government abuse of privacy.[167]

The 9/11 Commission Report pointed out that the system of oversight at the time was dysfunctional and in need of a joint committee to study the activities of intelligence agencies and to report problems to Congress.[168]

Currently many aspects of domestic intelligence oversight take the form of judicial review with the non-judicial review belonging to both the Congress and the

---

164 Priest and Arkin, Top Secret America, xix.

165Charlie Savage, and David E. Sanger, "Senate Panel Presses N.S.A. on Phone Logs," New York Times, July 31, 2013, article underscores the deep divide in Congress on the recently disclosed spying program.

166Kettl, System Under Stress: Homeland Security And American Politics, 104.

167Reclaiming Patriotism, American Civil Liberties Union, (2009-03), http://www,acle.org/pdfs/safefree/patriot_report_20090310.pdf, 5.

168 The 9/11 Commission Report, 420.

executive branch.[169] Any changes to this responsibility are going to need Congress' approval with the goal of a policy recommendation to improve transparency, and protect privacy in a way that is credible to a wide segment of the public, privacy advocates, domestic intelligence agencies and Congress.[170]

Next will be an examination of three policy proposals:

- Support for maintaining the status quo and the need for increased surveillance authority by domestic intelligence services and agencies.
- Developing/creating a single integrated domestic intelligence service by examining The United Kingdom's (UK) MI5 Service.
- Developing a more effective and streamlined oversight system to ensure checks and balances for privacy and civil liberty protections.

The *findings* chapter that will follow will analyze the strengths against weaknesses of each of these policies and finally a policy recommendation will be proposed.

Since 9/ll struck the gloves came off, that's all you need to know."

Cofer Black, CIA Counterterrorism Center Director

D. POLICY OPTION 1—STATUS QUO/SUPPORT FOR ENHANCED SURVEILLANCE AUTHORITY

1. Overview

This section will describe the current state of domestic intelligence in the United States after the terror attacks of 9/11, a description of the surveillance techniques used, and the legal justification and support for continuing with these policies.

The events of September 11, 2001, took away the sense of security that our borders offered. Our distance from the Middle East and Europe where attacks had happened previously was enough to shield us from terror organizations, people and attacks. Government officials have vowed to never again let an attack like this happen

169Philip B. Heymann, and Juliette N. Kayyem, Preserving Security and Democratic Freedoms in the War on Terror, National Memorial Institute for the Prevention of Terrorism, Harvard University JFK School of Government, http://www.mipt.org/Long-Term-Legal-Strategy.asp, 119.

170 Ibid., 121.

and claim they will do *whatever* is necessary to achieve that end.[171] Did w*hatever*, become an open invitation for government to exceed its limits under the U.S. Constitution?

In order for government to identify this new kind of enemy then they have to be allowed to use everything available. This includes techniques that may from time to time infringe on the privacy of American citizens not suspected of wrongdoing, including criminal or terrorist acts,[172] if government security agencies and state and local law enforcement are going to identify, disrupt, deter and prevent the next terror plot because terrorists circulate among the general population.

2. The Patriot Act

One of the major gaps identified after a review of the terror attacks of 9/11 was in the area of the intelligence community's counterterrorism approach.[173] The law modernized counterterrorism capabilities by giving access to tools like roving wiretaps that allowed investigators to track suspects who changed cell phone numbers, and it authorized aggressive financial measures to freeze terrorist assets.[174] Additionally, it allowed government to seek warrants to examine the business records of suspected terrorists, such as credit card information, [175]apartment leases and library records.

The Act amends 15 separate criminal statutes, creates multiple new federal crimes and greatly expands the authority of the government to conduct surveillance and

171Juliette Kayyem, Never Say "Never Again," Our foolish obsession with stopping the next attack, homeland security advisor to Mass. Governor Patrick Duvall writes this mindset confuses the public's understanding about homeland security, http://www.foreignpolicy.com/articles/2012/09/10/never_say-never_again.

172Bruce Gellman, "NSA broke privacy rules thousands of times per year, audit shows," *New York Times*, August 15, 2013, news story detailing an audit of NSA errors in surveillance operations,http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html?wpisrc=emailtoafriend.

173 Bush, Decision Points, Kindle, loc 3171.

174 Ibid.

175 Ibid.

searches.[176] It contains extensive revisions that expand law enforcement's investigative powers to obtain and analyze personal information and allows for greater authority for tracking and intercepting communications for both foreign and domestic law enforcement collection.[177] The NSA, whose mission had traditionally been devoted to foreign intelligence gathering, is increasing their focus on domestic communications.[178]

The USA PATRIOT Act passed in the U.S. Senate 98-1 and 357-66 in the House.[179] Many of the regulations that governed domestic intelligence operations that were successful during the Cold War had become outdated and they played a crucial role in why the events leading up to the 9/11 attacks were not interrupted.[180]

A White House official said that the expanded authority was needed to protect the nation from terrorist threats.[181] Over the next five years the PATRIOT Act helped disrupt terror cells in New York, Oregon, Virginia and Florida.[182]

A new type of enemy exists, different from the one we could easily identify during the Cold War. The combatants don't wear uniforms nor are they attached to nation states. They use our technology systems, the Internet and other communication avenues to move undetected in the general population.[183] Terrorists use financial system resources such as making credit card purchases, wire transfers and deposits of cash, and travelers checks from overseas and use ATMs to obtain money from foreign accounts.[184]

176Howard A. Johnson, Patriot Act and Civil Liberties: A Closer Look, Army War College, (March 15, 2006), https://www.hsdl.org/?viwe&did=46928.

177 Ibid., 4,8.

178Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 6, 2013, news story on how the NSA collects metadata, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

179 Taken from website *Educate Yourself*, http://educate-yourself.org/cn/patriotact20012006senatevote.shtml.

180 Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 296.

181Michael Winter, "White House defends need to collect phone records," *USA Today*, June 5, 2013, interviews an anonymous staffer who defends collection of phone data on U.S. citizens, http://www.usatoday.com/story/news/nation/2013/06/05/verizon-nsa-millions-phone-records/2394751/.

182 Bush, Kindle, loc 3186.

183Paul Shemella, *Fighting Back: What Governments Can Do About Terrorism, (*Stanford, California: Stanford University Press, 2011, 52.

184 Ibid.

The American financial system is hooked to a global network. No longer is it easy to establish whether a financial transaction is foreign or international.[185]

3. Civil Liberty and Privacy Protection

Surveillance activities might worry civil liberty advocates but this is the way this new enemy conducts operations. The PATRIOT Act includes judicial and congressional oversight mechanisms to protect privacy. The Federal Intelligence Surveillance Court (FISC) acts as the legal approval system for obtaining wiretaps and warrants. FISA judges act as the rule of law in protecting the public interest; they do not do the bidding of the government and are independent of the executive branch.[186] This process is not a rubber stamp. These courts have determined in the past that some collection carried out by the government was unreasonable under the Fourth Amendment.[187]

The Constitution, federal privacy laws and stringent Justice Department counterintelligence guidelines all focus on protecting individual civil rights. The program PRISM, (the code name for a signals intelligence address) enables domestic intelligence officials to collect e-mails, videos, documents and other material from U.S. companies like Google and Microsoft, but the government does not unilaterally seize information from the servers of providers.[188] DNI James Clapper has called the disclosure of this program "rushed and reckless, with inaccuracies that have left

---

[185] Bobbitt, Terror And Consent: The Wars for the Twenty-First Century, 296, 300.

[186] Steven G. Bradbury, "The system works well as it is," *USA Today*, July 19, 2013, Bradbury, former head of the USDOJ's Office of Legal Counsel wrote an op-ed pointing out the strength of the FISA court's warrant and wiretap review process, USA Today, (July 19, 2013), http://www.usatoday.com/story/opinion/2013/07/18/foreign-intelligence-surveillance-court--steven-bradbury-editorials-debates/2567025/.

[187] Barton Gellman, "NSA statements to the Post," *Washington Post*, August 15, 2013, news story details the oversight process within the NSA, http://www.washingtonpost.com/world/national-security/nsa-statements-to-the-post/2013/08/15/f40dd2c4-05d6-11e3-a07f-49ddc7417125_print.html.

[188] Robert O'Harrow Jr., Ellen Nakashima, and Barton Gellman, "U.S., company officials: Internet surveillance does not indiscriminately mine data," *The Washington Post*, June 8, 2013, authors describe what intelligence officials are saying about their surveillance techniques, http://articles.washingtonpost.com/2013-06-08/world/39834622_1_prism-clapper-jr-fisa-court.

significant misimpressions.[189] He ensures that there is an extensive oversight regime in place to protect civil liberties.[190] The system of balance between security and liberty works well.[191]

4. Data Mining

The United States has vast communications technology and it would be foolish not to exploit this technology to prevent, detect, disrupt and deter terror plots.[192] Contemporary communications is divided into packets and in order to target one specific piece of communications requires the scanning and filtering of an entire communications flow.[193] That means that the communications information of persons not being targeted gets caught up in the collection. Terrorists are often not state actors, so data about them ebbs and flows in a sea of information that contains data about ordinary people.[194] To require getting a warrant each time this happens is not only slow and eats up resources, but it is unreasonable for 21st century methods of fighting terrorism because the standard for probable cause to determine that the target is a terror agent cannot be met.[195]

In the global world of communications the difference between persons present or not in the U.S. does not make sense because in counterterrorism intelligence, you don't know whom to suspect and you need surveillance to find out.[196] Communications no longer travel point-to-point or linear.[197] Two people communicating in Europe could find their signal traveling through American switches.[198] The old way of doing things under

---

189 Ibid.

190 Ibid.

191 Steven G. Bradbury, "The System works well as it is," *USA Today*, July 19, 2013, Opinion/News section.

192 Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 311.

193 Ibid.

194 Ibid., 315.

195 Ibid., 311.

196 Bobbitt, Terror And Consent: The Wars for the Twenty-First Century, 311–312.

197 Ibid., 308.

198 Ibid.

FISA was not adequate to address technology advancements.[199] White House Spokesman Josh Earnest indicates that this kind of surveillance has been critical in protecting the nation from terror threats as it allows counterterrorism officials to discover whether known or suspected terror suspects have been in contact with persons in the United States who may be involved in terror activities.[200] Elementary data mining could have easily picked up on the location and activities of all nineteen hijackers involved in the 9/11 attacks.[201] Research of telephone numbers would have identified four of the 9/11 hijackers, who were known to intelligence officials, communicating with each other.[202] Without this capability today domestic intelligence agencies would be asked to go back to finding the pull string in the dark that turns on the light. You might eventually find it but it may be too late. Intelligence agencies, in order to keep up with these technologies and those not yet invented, are going to need the flexibility necessary to act quickly in order to prevent another 9/11 or something worse.

5. The Need for Secrecy

Much of what the government undertakes in the area of domestic intelligence needs to be kept secret so that intelligence operations do not get into the hands of the enemy. Disclosing information about the specific methods that government uses to collect, analyze and disseminate information is like opening up the playbook to those seeking ways to avoid detection.[203]

U.S. Senator Harry Reid stated that, *This surveillance program, imperfect as it may be, has done so much to help keep America safe. We need to keep the program.*[204]

---

[199] Ibid., 312.

[200] Charlie Savage, Edward Wyatt and Peter Baker, "U.S. Confirms That It Gathers Online Data Overseas," *New York Times*, June 7, 2013, authors detail US Internet surveillance program, New York Times, http://mobile.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?from=homepage.

[201] Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 308.

[202] Ibid., 307.

[203] Harrow, Nakashima, and Gellman, *U.S. Company officials: Internet surveillance does not indiscriminately mine data.*

[204] Matt Spetalnick, and Steve Holland, "Obama defends surveillance effort as "trade-off" for security," *Reuters News*, June 8, 2013, article detailing Obama's justification for sweeping U.S. surveillance program, http://www.reuters.com/article/2013/06/08/us-usa-security-records-idUSBRE9560VA20130608.

President Obama believes that we have struck the right balance and that the secret programs, *"Do not involve listening to people's phone calls, reading the e-mails of Americans absent further action by a federal court".*[205]

6. Conclusion

Information turned into intelligence is needed to protect the United States from further terror attacks. That is why the status quo must be maintained. Bruce Hoffman refers to the tactics used as an inherently brutish enterprise, a nasty business.[206] Americans do not yet appreciate the enormous difficulty and morally complex problem entailed in producing reliable, competent, actionable intelligence.[207] How to obtain that information from an enemy that hides in and among ordinary people making them harder to identify and their plots and plans harder to detect presents issues for debate and discussion in a democratic society.

The central dilemma faced by liberal democracies in attempting to effectively combat terrorism has to do with the reality that confronting a serious terror threat requires measures that strengthen the power of government over the individual, and that in turn reduces the freedoms and protections that people have traditionally enjoyed before 9/11 happened.[208]

Government agencies now have the tools, the flexibility and the civil liberty protections in place to create an intimidating environment for terrorist networks and individuals. The rapid evolution of technological change may require even more expanded government authority. This is what Congress and the American people will have to realize in order to prevent another 9/11.

---

[205] Ibid.

[206] Hoffman, A Nasty Business, 1.

[207] Ibid.

[208] Nadav Morag, *Comparative Homeland Security: Global Lessons,* (Hoboken, New Jersey: Wiley Press, 2011), 66.

Chapter V will be an examination of and support for a policy of establishing a single integrated domestic intelligence agency using the United Kingdom MI5 service as a model.

Nobody in their right mind would create the architecture we have in our Intelligence Community.

CIA Veteran Porter Goss commenting on the U.S. approach to domestic intelligence.[209]

E. POLICY OPTION 2—CREATING A SINGLE INTEGRATED DOMESTIC INTELLIGENCE AGENCY: A COMPARATIVE LOOK AT THE UK'S MI5 AGENCY AND PRIVACY PROTECTION

1. Overview

The United States has no intelligence agency fully devoted to internal security like the British MI5 service.[210] Instead we have a disparate collection of agencies shaped by the Cold War, each with its own mission, culture, and operating procedures that report to their own director who reports to an assortment of congressional oversight committees and the Executive branch.[211] This has been the dilemma of U.S. intelligence since the National Security Act of 1947.

This disparate arrangement of domestic intelligence agencies has led to a lack of corporateness, defined as a mission where employees within the intelligence community run, function, and behave as part of a more closely integrated enterprise that works toward a defined common goal.[212] Corporateness would remove redundancy and self-interest, and create efficiencies within the current IC structure, and provide better intelligence products to policy makers.[213] Corporateness would lend itself to a more consistent application of privacy laws and a streamlined oversight process for compliance.

209David E. Kaplan, Mission Impossible, http://www.militaryphotos.net/forums/showthread.php?17875, 2.

210 Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 301.

211IC21: The Intelligence Community in the 21st Century, Staff Study Permanent Select Committee on Intelligence House of Representatives One Hundred Fourth Congress, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/ic21001.htm, 1.

212 Ibid., 5.

213 Ibid.

An attempt to centralize the intelligence function has its origins in the 1947 National Security Act.[214] Prior to that, associates of President Franklin Roosevelt pressed him to set up something similar to the British Secret Intelligence Service MI6.[215] He asked J. Edgar Hoover to expand the FBI to take on domestic intelligence and he obliged with a Secret Intelligence Service resembling the UK MI5.[216] Roosevelt created an Office of Strategic Services (OSS) to be an MI6-like agency that would overlap with the FBI. Truman abandoned the OSS in 1945. What came out of the attempt to centralize intelligence with the National Security Act was the creation of the Central Intelligence Agency (CIA), and in the end this agency became the victim of politics.[217]

The attempts to coordinate intelligence activities in the reform efforts that followed was fought by the Department of Defense (DoD), the Department of State, the FBI and other agencies with intelligence capabilities.[218] Fragmentation is the word used to describe one of the problems with the disparate structure of the U.S. approach to intelligence.[219] One defense intelligence official puts the problem this way: *"We don't have much of a sense of loyalty to the Community. We see ourselves as employees of agencies and when agencies get together each agency tells their people that we are competitors.*[220]

Even after all the reform efforts that followed for nearly a half century after 1947, the attempts to coordinate intelligence left organizational, structural and cultural deficiencies that contributed to or played a role in not adequately warning policy makers of the strategic surprise of 9/11.[221] Several failures that followed the 9/11 attacks,

---

[214]Walker Paper No. 5, *Intelligence Reform, A Question of Balance,* (Maxwell Air Force Base, Alabama: Air University Press, 2001-08), 41.

[215] Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence,* (Washington D.C.: Georgetown University Press, 2005), 9.

[216] Ibid., 10.

[217]Amy B. Zegart, *Spying Blind: The CIA, FBI, and the Origins of 9/11,* (Princeton, New Jersey: Princeton University Press, 2007), 64.

[218] Ibid.

[219] Ibid., 63.

[220] Ibid., 67.

[221] Ibid.

including one by Umar Farouk Abdulmutallab, known as the underwear bomber, and Richard Reid, known as the shoe bomber, demonstrate that structural deficiencies still exist.

The current structure of intelligence operations in the U.S. has set up a competitive environment between the disparate agencies evidenced by debates over budgets and authority. Members of Congress have taken sides in this power struggle by association to agency heads and have shown deference to them in the process. What is recommended by security advisors is more *joint action* between intelligence agencies and operations.[222] That jointness was achieved by the reform act that established corporateness between the military departments in the Goldwater-Nichols Reform Act of 1986.[223]

The 9/11 Commission Report to Congress elaborated on the fragmentation issue concerning the U.S. approach to intelligence and the failure that resulted. The report pointed out that the U.S. government must find a way of pooling intelligence and using it to guide the planning for joint operations.[224]

Jointness also relates to standardizing the use of, the understanding of, and the interpretation of the Patriot Act and privacy protections. The training of collectors and analysts is different due in part to each agency having its own mission. The disparate nature of 16 agencies that make up the IC along with state and local law enforcement results in each agency applying privacy standards differently. The FBI for example determined in the case of the 19 hijackers that the law only allowed them to go so far before what they were doing infringed into constitutionally protected areas.[225] The CIA had a different interpretation because it was interpreting things from a foreign

222Zegart, Spying Blind: The CIA, the FBI and the Origins of 9/11, 66.

223John D. Bansemer, "Intelligence Reform: Question of Balance," (U.S.: Air University Press, 2006-08), https://www.hsdl.org/?view&did=47037, 9.

224 U.S Congress, The 9/11 Commission Report, 357.

225 Bobbitt, Terror And Consent: The Wars for the Twenty-First Century, 299–303.

intelligence investigation viewpoint. This foreign and domestic intelligence divide created confusion in terms of privacy protection as the two organizations worked on intelligence gathering.[226]

Will a single integrated domestic intelligence agency lead to a unified understanding of and application of privacy laws? An examination of the security service MI5, how it functions as a security service to prevent, detect and disrupt terror attacks and its privacy protection review mechanism will be described next.

2. United Kingdom MI5 Security Service-Operations

MI5 is one of four intelligence agencies in the UK.227 Peter Clarke, Deputy Assistant Commissioner of the Metropolitan Police in the United Kingdom articulated a vision for how the United Kingdom approaches counter terrorism since 9/11 when he said,

> So what we have done is to develop a new way of working where the police and Security Service now work together in every case from a much earlier stage then would have happened in the past to where it has become the daily routine.[228] It is no exaggeration to say that the joint working between the police and MI-5 has become recognized as a beacon of good practice where colleagues from across the globe, in law enforcement and intelligence, look to the UK as a model. No longer can the police service feed off the crumbs falling from the end of the intelligence table.[229]

This model defines a very clear role for local police in counter terror operations and investigations and an apparatus for information sharing.

The United Kingdom's strategy for domestic intelligence to contain the threat of Islamic terrorism is CONTEST230. The objectives are:

---

226 Ibid.

227 Morag, Comparative Homeland Security: Global Lessons, 133.

228 Deputy Assistant Commissioner Peter Clarke lecture to Policy Exchange, April 25, 2007, 5, http://content.met.police.uk/News/DAC-Peter-Clarks-speech-on-counter-terrorism/1260267589755/1257246745756.

229 UK Metropolitan Police Assistant Deputy Commissioner Peter Clarke lecture, 5.

230 Christopher Andrew, The Defense of the Realm: The Authorized History of MI-5, (New York: Penguin Books, 2009), 385.

- ***Preventing*** terrorism by tackling the radicalization of individuals
- ***Pursuing*** terrorists and those that sponsor them
- ***Protecting*** the public, key national services and UK interest overseas
- ***Preparing*** for the consequences

The British have had more experience with terrorism on their own soil than many other nation states and that experience can be useful in determining what works and what does not in counter terrorism strategies. Police force actions like traffic stops, and uncovering counterfeiting or fraudulent identification are done with a mindset of thinking terrorism first. This creates a hostile environment for terrorism.[231]

The British Security Service, also known as MI-5, is one of three intelligence services, the other two being the Government Communications Headquarters (GCHQ) and the Secret Intelligence Service known as MI-6.[232]

Responsibility for domestic intelligence is vested in MI-5 and they support the law enforcement efforts of the 56 police forces.[233] The division of labor under the UK model is that MI-5, whose agents have no arrest powers, gather clandestine and open source intelligence, assesses the threat and may take intelligence action to prevent and deter terrorist events. The Special Branches of the police force pursue counterterrorism investigations that may lead to or result in legal action, including criminal prosecution.[234] The relationship between MI-5 and police force Special Branches ensures the flow of information up, down and across the spectrum. MI-5 ensures that information used in national security cases can be used as evidence in court.[235] This ensures that sources are protected and that only information relative to the prosecution is released at trial to protect national security interests.

231Paul Howard, "Hard Won Lessons: How Police Fight Terrorism in the United Kingdom," Manhattan Institute for Policy Research, (December 2012), http://www.manhattan-institute.org/pdf/scr_01.pdf.

232Ibid., 4.

233Masse, 6.

234 Ibid., 5–6, Secret Security Act of 1996 stipulated two separate functions to avoid formation of a secret police organization.

235 Masse, Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States, 6.

3. A Sense of Corporateness

Corporateness here refers to integration between all the disparate individual agencies and organizations that are independent of one another.[236]

One of the biggest differences in the UK approach to domestic intelligence is that they separate their domestic intelligence responsibility/duties from law enforcement in terms of its function only.[237] The Security Service Act of 1996 specifically stipulates that MI-5 was not to act as an independent law enforcement organization.[238] Its closest CT relationship is with the Special Branches of the 56 police forces. Special Branches are explicitly responsible for CT efforts with regional officers in every police force division throughout the UK. Special Branch officers prosecute and assist in both CT collection and counterintelligence operations.[239] Special Branches is vital to the success of MI-5. This joint effort ensures that intelligence drives operations.

The history of collaboration between MI-5 and Special Branches has not been without its challenges. Friction has arisen between MI-5 and the local Special Branches police in which MI-5 desk officers have sometimes sanitized intelligence from covert human sources in joint operations.[240] This can hamper good relations if Special Branches begins to feel that they are getting information that has been filtered of important information before being shared. The same issue plagues the U.S. Intelligence Community. MI-5 gathers clandestine and open source information about covert terror activities and can take action to prevent and deter terror activities.[241] The U.S. approach questions the vast amount of open source material and its reliability.

The UK counterterrorism strategy is shaped by a culture of prevention. MI-5 has no conflicting law enforcement responsibility, which then allows it to stay focused solely

---

[236]Zegart, Spying Blind, The CIA, the FBI and the Origins of 9/11, 34.

[237] Masse, Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States, 5.

[238] Ibid.

[239] Ibid., 6.

[240] Ibid., 4.

[241] Masse, Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States, 6.

on CT intelligence.[242] Instead of having a mindset of arrest and prosecution like we have in the United States, they produce actionable intelligence for police Special Branches. The CT intelligence produced ends up being the catalyst in disrupting, preventing or arrest and prosecution of a terror operation. Most of the information collected by MI-5 comes from local police. The model used brings intelligence operations together with police forces to decide the best approach to countering terrorism. Having no arrest powers as mentioned earlier makes an MI-5 agent's effectiveness in preventing terror attacks dependent upon a close working relationship with local police forces.[243] Everything the Service does has one objective in mind, that being to drive and support police force operations. The MI-5 desk officer gets all the information collected from sources. This centralizes information and prevents stovepipes or silos for information to be held which inhibits the sharing of information. The intelligence report produced by the desk officer asks and answers three vital questions: 1) What does he have? 2) Is it a threat? 3) What is he going to do about it?

A "*Left of Boom"*[244] theory exists where a continuum has been designed that shows the security strategy leading up to and after a terror attack. The objective of the UK strategy is to focus its resources and effort "upstream" in producing intelligence in the zone *prior* to an attack in order to prevent and/or disrupt the attack.[245] The FBI culturally is a "downstream" organization dedicated to reviewing past events that lead to arrest and prosecution.[246] The Tsarnaev brothers' involvement in the Boston Marathon bombing is a case in point. None of what they were doing was believed to be enough to continue to follow them according to the FBI.[247]

242Rand Corporation, Confronting the "Enemy Within: What Can the United States Learn About Counterterrorism and Intelligence From Other Democracies?, Rand Corporation Research Brief (2004), http://rand.org/researchareas/terrorism/index.html.

243 Larry Irons, Recent Patterns of Terrorism Prevention in the United Kingdom," Homeland Security Affairs, January 2008, http://www.hsdl.org/?view &did=482786, 1.

244 Paul A. Smith, PowerPoint lecture, Naval Post graduate School, (January 2013).

245 Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 301.

246 Ibid., 301–302.

247*Feds: Boston suspect downloaded bomb instructions,* Associated Press, (June 27, 2013), describes the Internet activity of the alleged Boston bombing suspect that did not attract the attention of the FBI.

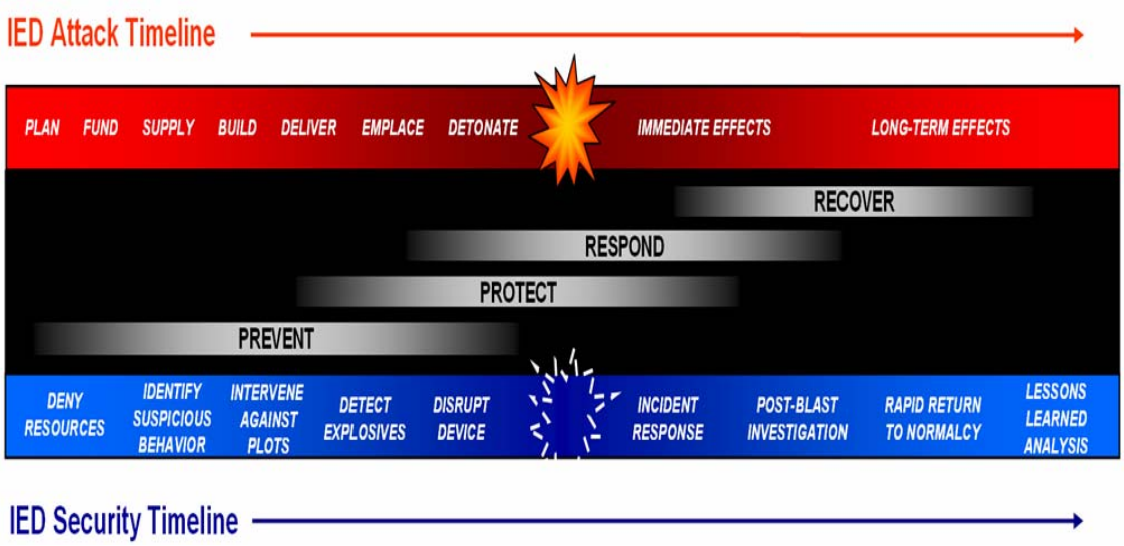

Figure 1. "Left of Boom" timetable before and after a terror attack in UK

The British model of counterintelligence has had its share of successes and failures, which shows that no model of domestic intelligence can prevent all terror attacks.[248] One example of intelligence success is the preempted attack in *Operation Crevice*, which was billed at the time as the most complex counterterrorism operation ever undertaken in the UK that led to life sentences for five men convicted in the plot.[249] On the other hand, some large-scale terrorist attacks were successfully carried out. In July 2007, three explosions rocked the London Underground System while another tore apart a London bus.[250] The point is that no counterterrorism approach designed by other similar democratic nations can eliminate all terror attacks. More important is that the U.S. can continually improve their counter terror strategy by looking at certain aspects of models in effect in other nations that have more experience dealing with terror.

[248] Larry Irons, Recent Patterns of Terrorism Prevention in the United Kingdom, 3.

[249] Ibid.

[250] Ibid.

4. How Does The UK Approach Apply to How We Do Domestic Intelligence in the U.S.?

There are several issues concerning how other democratic countries such as the UK approach domestic intelligence and the relationship between intelligence and law enforcement in those countries. There had been much less attention paid to the role that local police played in homeland security and protecting critical national infrastructure in the United States prior to 9/11.[251] Once inside our borders, it is the police-not the FBI or CIA-who have the best tools for detecting and prosecuting crimes like forged documents, identity theft, illegal narcotic sales, and other minor crimes along with jail and prison radicalization.[252]

The intelligence information is out there but it is fractured among the many layers of law enforcement that characterize America's federal system of government.[253] In the UK, the local police department, Special Branch, and national intelligence agencies are in constant contact with each other.[254] What is missing today in U.S. domestic intelligence is an "all channels network" where expertise and intelligence and information can be disseminated quickly and effectively throughout the law enforcement community from coast-to-coast and from chief executives down to street officers.[255]

U.S. policymakers are going to have to decide whether a domestic intelligence agency separate from the law enforcement function is the way forward for intelligence development to counterterrorism.[256] Numerous intelligence reform commissions have attempted to centralize the intelligence function and have failed due to politics and turf protection. Intelligence failures from inadequate information sharing due to stove-piping, that allowed incidents like the shoe bomber, the underwear bomber and the Boston Marathon bombing to happen, will raise this question once again.

---

251 Safe Cities Project Report 1, December 2004, 3.

252 Ibid.

253 Ibid.

254 Safe Cities Project Report 1, 16.

255 Ibid., 3.

256 Rand Corporation, *Confronting the Enemy Within*, 2.

Separating these functions has its advantages with a major one being that without arrest powers an intelligence agency is dependent on working closely with law enforcement. It almost forces the relationship that the US intelligence community has resisted. The result will be a breakthrough in the cultural barriers that have plagued information sharing between federal and local agencies.

Keeping the intelligence function separate from law enforcement, as with the UK model, will provide an added level of safeguarding civil liberty protections. MI-5 officers are not evaluated by how many cases are brought in for prosecution or on how many arrests are made like FBI agents. As a result they are less likely to engage in activities that skirt the law. Arrests and cases made for prosecution can have a positive impact for evaluation of FBI agents.

5. Privacy and Civil Liberty Protections in Domestic Intelligence in the UK

The first and most important difference is that the U.S. government is based on being a constitutional republic with rights attached to individuals. Power is shared between three separate branches, and a Supreme Court has the final say in interpreting laws duly passed.[257] The UK does not have a written constitution giving rights to individual people and it focuses national political power in a Parliament.[258]

Civil liberty protection is important to liberal democracies like the U.S. and the UK. Great care with oversight for privacy protections in the U.S. rests with our Congress and judicial system, both of who have the final say on the constitutionality of intelligence activities like wiretaps and other surveillance operations.

[257]Todd Masse, Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States, Summary.

[258]Ibid.

Whether to approach terrorism as a criminal act or a war is causing some of the confusion in the American approach to counterintelligence. The President's War Powers under Article II of the U.S. Constitution give him a lot more leverage in counterterrorism than domestic intelligence agencies conducting counterintelligence inside the U.S.[259]

For liberal democracies, the counterterrorism strategy chosen must, regardless of which approach is decided on, either as a law enforcement or war continuum, not lose sight of what is being protected, the very existence of a liberal democratic state based in the rule of law.[260] The liberal democratic state must provide for the maximum number and type of rights and freedoms for its inhabitants.[261]

In the UK, Parliament plays a role along with security commissioners to oversee intelligence operations. High court judges in the UK spot-check activities and operations of the security service for legal compliance on a routine basis.

There are strict limitations on what MI5 can and cannot do when investigation individuals.[262]

- An individual's right to privacy cannot be overridden without *very good cause.*
- The authorizations are reviewed by independent commissioners to ensure that they comply with the law.
- In order to intercept telephone communications, interfere with property or conduct "*intrusive surveillance"* a warrant *must* be obtained which authorizes *precisely* what actions will be taken. These warrants last for up to six months.
- In urgent cases warrants may be signed by a senior official in the Home Office but only after the Secretary of State has granted permission. These warrants last from two to five days.
- The warrant and authorization system, together with the independent review process, is a legal safeguard, which ensures that MI5 does not use any intrusive techniques without good reason.

---

259 Bush, Kindle, loc, 3037.

260 Morag, Comparative Homeland Security: Global Lessons, 65.

261 Ibid., 66.

262 Morag, Comparative Homeland Security: Global Lessons, 111.

- Emergency regulations must be geographically specific, cannot amend basic guarantees of human rights and must be limited in time.
- If an organization is labeled as a terror group by the Home Secretary, there is a provision to appeal that decision to a judicial body called the Proscribed Organizations Appeals Committee.

The Terrorism Act passed in 2000, gave the UK a piece of non-emergency legislation but also provided for stronger guarantees for rights of suspects and greater allowance for judicial scrutiny.[263] Detainees suspected of terror involvement can appeal their status to a special immigration appeals commission that at least ensures some sort of judicial oversight.[264]

6. Prosecuting Terror Through The Criminal Justice System Versus War-fighting

The UK MI5 model of prosecuting acts of terror is via the criminal justice system route relying on criminal procedures for arrest, prosecution and incarceration.[265] The United States since 9/11 has approached terror for the most part as a blend between a war-fighting approach (GWOT) as they would a war against a nation state, including the use of military trials for prosecution, and a law enforcement approach (Boston Marathon Bombing).[266]

The war-fighting approach allows for the use of any and all means of intelligence gathering with little attention paid to safeguarding rights to privacy and other civil liberties.[267] The law enforcement approach is based on an entirely different philosophy in that it views the "enemy" not collectively, but as individuals carrying out specific criminal acts.[268]

---

[263] Ibid., 84.

[264] Morag, Comparative Homeland Security: Global Lessons, 84.

[265] Ibid. 94.

[266] Ibid., 65.

[267] Ibid., 64.

[268] Ibid., 65.

The United States has been criticized for an overly militaristic approach to counterterrorism and that an erosion of civil liberties results.[269] Calling the reaction to the 9/11 terror attack an act of war ensured that the U.S. government could justify hiding its activities by classifying information as secret.[270]

The law enforcement approach means spending much of the time operating within the borders of a democratic state and are subject to the legal restrictions designed to protect the basic rights of the population.[271] The UK has had success in approaching terror as a criminal matter. Since 2005, Britain has prosecuted all terror acts in criminal courts and has achieved a 90 percent conviction rate.[272] The trials are pursued with full respect for civil rights according to the head of the Crown Prosecution Service, Ken MacDonald.[273]

7. Comparing and Contrasting U.S. and UK Approach to Counter Terror

The single integrated domestic intelligence service approach is based on lessons from the United Kingdom's decades of experience with strategy in countering the Irish Republican Army terror attacks.[274] The UK has more experience in CT operations than their U.S. counterparts.[275] The single domestic intelligence agency approach enhances accountability. It eliminates fragmentation of domestic intelligence responsibility and establishes clear lines of authority, mission, application of laws, training and responsibility.

269Raymond Bonner, "Two British Anti-terror Experts Say U.S. Takes Wrong Path," New York Times, article critical of the war-fighting approach to terror taken by the U.S., http://www.nytimes.com/2008/10/22/world/europe/22britain.html?_r=0.

270Zegart, Spying Blind: The CIA, the FBI and the Origins of 9/11, xx.

271 Ibid.

272 Ibid.

273 Ibid.

274Paul Howard, Hard Won Lessons: How Police Fight Terrorism in the United Kingdom, Manhattan Project Report 1, December 2004, (2001-12), http://www.manhattan-institute.org/pdf/scr_01.pdf, 5.

275 Ibid.

A major difference is that the UK as policy prosecutes terror attacks through their criminal courts rather than the war-making process. The criminal justice approach affords suspects more civil liberties protections in the form of legal representation, an adversarial court process and rules of evidence for wiretap and warrant applications.

It has been suggested in an essay by Stewart A. Baker, former Assistant Secretary for Policy at DHS that in the post-Cold War period the U.S. government should have shed illusions about the cooperation between intelligence operations and law enforcement operations.[276]

The UK has fewer police forces and agencies than the U.S. and this makes a community-wide culture more achievable. The Security Service MI5 pursues closer cooperation and trust with police services because they have no executive authority. Because MI5 has no conflicting law enforcement responsibilities like the FBI does and state and local law enforcement do, they have been able to focus exclusively on gathering information to prevent terror attacks.[277] There is no FBI-type agency in the UK that has dual law enforcement and intelligence responsibility. The domestic intelligence model employed in the UK has elements that can assist the approach taken in the U.S. to provide better security and to protect privacy and civil liberties.

If the U.S. had a fully functioning internal security service acting in seamless coordination with the CIA, according to Charles Cogan, former Chief Director of Operations in the CIA, it would have had a major impact on the unfolding of the 9/11 attacks before it could have taken place.[278] The goals outlined in Policy Option 1 can still be achieved under this model.

276Stewart A. Baker, "Should Spies Be Cops?" Source: Foreign Policy, No. 97 (Winter, 1994-1995), 36–52 Publisher(s): Washington Post.Newsweek Interactive, p. 47 LLC Stable URL: http://www.jstor.org/stable/1149438.

277Confronting the Enemy 'Within': What Can the United States Learn About Counterterrorism and Intelligence from Other Democracies?,RAND Corporation, (2004), http://www.rand.org/pubs/monographs/MG100.html.

278 Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 302.

Another emerging issue concerning local and federal intelligence operations is that civil liberty violations can and have occurred because of inadequate training.[279] Standardizing the U.S. domestic intelligence approach by a single integrated security service would standardize operating procedures, training, reporting systems and mission similar to MI5. The original goal of the 1947 National Security Act to create a single service agency responsible for domestic intelligence has still not been achieved mainly due to turf wars, power struggles, turf protection and politics.[280]

Balancing the need of domestic intelligence agencies to engage in activity that can prevent, disrupt and identify terror plans, plots and suspects with privacy and civil liberty protection is not a zero sum game as some suggest.[281] This is a fluid state that from time-to-time requires recalibration and retooling. Strengthening the relationship between democratic principles and security through transparency and effective oversight is critical to maintaining public confidence.[282] An adversarial appeal process in the U.S. system under FISA and the FISC, similar to what MI5 operates under would create balance. This will address civil liberty and privacy advocate concerns about activities and operations that have the potential to infringe on civil liberties. Public trust is essential to the acceptance of government investigations in intelligence operations.

Chapter V will examine policy option three, which is how to create a more effective oversight process in the wake of more aggressive and enhanced surveillance techniques used in domestic intelligence operations in the United States. The recent disclosure of those techniques leaked by NSA contractor Edward Snowden in *The Guardian* newspaper in the UK has revived the privacy/civil liberty protection debate and

279 Permanent Subcommittee on Investigations, Committee on Homeland Security and Government Affairs: Federal Support for and Involvement in State and Local Fusion, Centers, (October 3, 2012), 26.

280Zegart, Spying Blind: The CIA, the FBI and the Origins of 9/11, 63.

281Matt Spetalnick, and Steve Holland, "Obama defends surveillance effort as "trade-off" for security," Reuters News, article detailing Obama's justification for sweeping U.S. surveillance program, http://www.reuters.com/article/2013/06/08/us-usa-security-records-idUSBRE9560VA20130608.

282 The 9/11 Commission Report, 424.

the public acceptance for those techniques. The details of how these techniques are targeted at Americans and non-Americans not suspected of terrorism have gotten the attention of Congress.[283]

If men were angels there would be no need for government, however men are no angels.

James Madison

F. POLICY OPTION 3—CREATING AN EFFECTIVE OVERSIGHT PROCESS FOR PRIVACY AND CIVIL LIBERTY PROTECTION

1. Overview

At the center of the debate is providing government security agencies with the tools needed to protect the United States against terror attacks before it begins to encroach too far into the private lives of Americans and others not suspected of terror involvement. The following questions will be answered in this policy option. What checks and balances are needed? Is effective oversight occurring? How will it be attained?

One of the findings in the 9/11 Commission report to Congress was that congressional oversight for intelligence and counterterrorism is dysfunctional.[284] From this finding the report concluded that the current oversight apparatus needed to be consolidated. One of the *9/11 Commission Report* recommendations is for Congress to create a single principal point of oversight for review of homeland security activities with one in the House and one in the Senate and a nonpartisan staff.[285]

The goal of oversight is to instill trust through an objective verification about government operations. If government is not trusted, it will be difficult for it to claim the moral high ground with the public that they can be trusted with activities like secret surveillance programs and things that are necessary to prevent terror attacks.[286] The

283The 9/11 Commission Report, 104.

284The 9/11 Commission Report, 420.

285 Ibid., 421.

286 Bobbitt, Terror AND Consent: The Wars of the Twenty-First Century, 348.

reason is because terror attacks are extremely rare and the public will begin to wonder if the trade-off of a more intrusive government is worth it.

The first line of oversight is self-monitoring due to the secrecy requirements and internal controls that are vital to improving and maintaining accountability.[287] Internal oversight processes in the law enforcement and security apparatus may not be proving to be very effective.[288] As former Secretary of Defense Robert M. Gates put it, there has been so much growth since 9/11, not just within the CIA, that getting your arms around it is a challenge.[289] Instead of having the Justice Department act as the internal review process for compliance with privacy and civil liberties, scrutiny from an unbiased and disinterested party is recommended.[290]

Previously mentioned in this thesis is that oversight of domestic intelligence activities by law enforcement and security agencies, is the province of Congress and the FISA courts. Congressional scholar Norman J. Ornstein counted thirteen Congressional committees and more than sixty subcommittees with at least some jurisdiction over homeland security operations.[291] The 9/11 Commission Report identified 88 just for DHS.[292] This makes effective oversight difficult at best.

The concern with the FISC and oversight is that it operates in secret, keeping its opinions sealed and has no adversarial process.[293] It operates like no other court in America. This one-sided government process exists nowhere else in our democratic state. A recommendation for more transparency in the FISC will be discussed later.

---

287 John Maris, Institutional Reform: An Application of Organizational Theory to Reform of the Intelligence Community, (1997-01), Federation of American Scientists, http://www.fas.org/irp/eprint/snyder/organization.htm, 7.

288Dana Priest, and William M. Arkin, A hidden World Growing Beyond Control, interview discussing how unwieldy and secret government operations have become in fighting the GWOT, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/, 2.

289 Ibid.

290 John Maris, Institutional Reform, 9.

291Kettl, System Under Stress: Homeland Security And American Politics, 137.

292The 9/11 Commission Report, 421.

293*Lift the veil of secrecy on the nation's security court*, USA Today Editorial Opinion on the FISA court, (2013-07-18), http://www.usatoday.com/story/opinion/2013/07/18/foreign-intelligence-surveillance-court-nsa-editorials-debates/2567127/.

2. Classified Document Process Prevents Effective Oversight

Since so much of what goes on in the domestic intelligence enterprise is classified as confidential, secret or top secret it allows for government to operate with little transparency for the public and makes it difficult for Congress to know about possible illegal government action.[294]

Only certain members of Congress are privy to secret briefings from executive branch agencies and domestic intelligence agencies. The shroud of secrecy surrounding the recently leaked surveillance programs hamstrung those members in what they could disclose and many felt that their only recourse was to file secret letters of concern or protest.[295] Jane Harman, a former Ranking Member of the House Intelligence Committee indicated that you can't talk to anybody about what you learn in briefings and there is no way then for staff to do research, which would make for more successful oversight.[296]

Hiding information from Congress and judicial oversight allows the Executive Branch to keep itself free from public criticism and increases the likelihood of illegal and improper activity.[297] It is OK to have faith in government but asking intelligence officials to prove what they are saying is true is healthy.

The authority to classify documents is done to protect information from getting into the wrong hands that might expose the identity of informants or sensitive information on investigations.[298] Much of this information has been determined to pose no threat to national security if released.[299] Former Secretary of Defense Donald Rumsfeld believes that as a general rule too much material across the federal government is classified.[300]

294Elizabeth Goiten, and David M. Shapiro, Reducing Overclassification Through Accountability, Brennen Center for Justice, (2011), https://www.hsdl.org//?view&did=689494, 7.

295 German and Stanley, Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Secret Security Establishment, 22.

296 Ibid.

297 Ibid., 10

298Goiten and Shapiro, Drastic Measures Needed, 1.

299 Ibid.

300Goiten and Shapiro, Drastic Measures Needed, 1.

Overclassification is an ongoing problem. According to the 9/11 Commission Report, overclassification may have inhibited information sharing that may have pieced together bits of information that may have made it possible for intelligence and security agencies to have at least anticipated the September 11 attacks.[301] In addition to the classification process throttling information flow it is a waste of taxpayer money.[302]

As stated previously in this thesis, Congress has the authority and must take the lead in challenging laws and practices that allow little transparency in our national security and domestic intelligence operations. We cannot expect officials and agencies in the domestic intelligence enterprise that benefit from a lack of accountability and transparency to change on their own.[303] Change is going to have to be mandated by Congress and the court.

Congress has the right under the Intelligence Oversight Act of 1980 and the Intelligence Whistleblower Protection Act of 1998, to organize and manage executive branch activities.[304] They need to leverage this authority. The Executive branch does not have the right to tell members of the Intelligence Oversight Committee that they cannot share what they learn in briefings with other members of Congress.[305] Many members outside of the intelligence committees of Congress and several who are members of those committees were unaware of the extent of the spying program.[306] These rank and file members of Congress still have an electorate that they are accountable to and therefore must have access to at least redacted reports on activities of the executive branch as a check and balance, and for enhanced transparency.

---

301 Goiten and Shapiro, Reducing Overclassification Through Accountability, 1.

302 Ibid., 7.

303 German and Stanley, Drastic Measures required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Security Establishment, 34.

304 Ibid., 36.

305 German and Stanley, Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Security Establishment, 38.

306 *Republican lawmakers: NSA surveillance news to us,* news story detailing that rank and file members were not informed of PRISM program, confirmed by Senator Dick Durbin, http://www.politico.com/story/2013/06/republicans-nsa-surveillance-92418.html.

An effective oversight process is one that has people assigned to it who possess expert knowledge about the field of intelligence. It would allow for probative and pointed questions to be asked to prevent heads nodding affirmatively about what they are being told. The tendency with intelligence officials who testify before Congress is to inform lawmakers on what they want them to hear instead of on what they need to know.[307] A bipartisan report in February 2003, by senior members of the Senate Judiciary Committee expressed great frustration with the Justice Department's refusal to submit to Congressional oversight.[308] This is done sometimes to head off public criticism of some of their activities.[309] In 1997, an attempt was made to rein in the classification "regime" when the bipartisan Commission on Protecting and Reducing Government Secrecy determined that the classification system is often used to deny the public an understanding of the policymaking process.[310]

The NSA surveillance program that was leaked by Edward Snowden is a case in point. Although a few members were privy to the program, they could not share it with the public or the media because of the claim of damage to national security. This claim cannot however be substantiated and is oftentimes an exaggeration.[311] It is thrown up to anyone in Congress questioning intelligence officials because they either do not have the answer, or to avoid exposing mistakes or having to disclose questionable activity as in the case of DNI James Clapper cited previously.

Most members of Congress rely on staff members to keep up with the volumes of intelligence reporting. This staff needs expertise and time on a subject in the area of

---

[307]No author, *Key Loophole Allows NSA to Avoid Telling Congress About Thousands of Abuses,* article details how thousands of abuses of privacy by NSA spying go unreported to congressional oversight committees. http://www.techdirt.com/articles/20130817/02451024219/key-loophole-allows-nsa-to-avoid-telling-congress-about-thousands-abuses.shtml.

[308] Ann Beeson and Jameel Jaffer, Unpatriotic Acts: The FBI's Power to Rifle through Your records and Personal Belongings without telling You, 11.

[309]Goiten and Shapiro, Reducing Overclassification Through Accountability, 10.

[310]Ibid. 5.

[311]Aamer Madhani and David Jackson, "With NSA controversy, debate over secrecy revived," *New York Times*, June 20, 2013, story on claims by former counterintelligence official and others that disclosing too much about domestic intelligence activities and operations causes damage to national security may be an exaggeration. http://www.usatoday.com/story/news/politics/2013/06/12/nsa-secrecy-necessary/2416393/

intelligence to maintain that proficiency.[312] Intelligence community veterans who have been known to offer dissent or complain about the internal goings on would be helpful today as advisers to congressional oversight committees. They have been previously vetted with security clearances, eliminating the need to exclude them from closed-door hearings.

Much of the controversy over domestic intelligence surveillance programs could be resolved by declassifying documents, having a more rigorous approval process to keeping secrets and releasing redacted intelligence reports that may contain sensitive information. Congress through legislation can and must mandate that this take place.

3. FISA Court Reform to Achieve Balance

In November 2002, the secret FISC handed the government broad authority to conduct surveillance on electronic communications conducted on the Internet.[313] As a result it is so much easier now for domestic intelligence agencies to justify secret wiretaps and surveillance under FISA.

The objective is to instill balance in the FISA court process, objectivity in its decisions and more transparency. One way to achieve that is to tweak the FISC so that the process includes procedural aspects similar to the court process used in criminal and civil courts all across the United States, that being the opportunity to challenge the government's or plaintiff's assertions.[314] Traditional courts in the U.S. are based on an adversarial process. In criminal proceedings the burden of proof is on the government. In a civil case it is based on a preponderance of evidence. If one side makes a claim, the other has an opportunity to contest or challenge it. This is not currently available under FISA court rules.

---

312 Sims and Gerber, Transforming U.S. Intelligence, 241.

313 Tom O'Conner, PhD., Civil Liberties and Domestic Terrorism, Dr. O'Conner's Criminal Justice megalinks, (2004-05-06), https://www.hsdl.org/?view&did=44798.

314Byron Acohido, and Jon Swartz, "Google challenges U.S. gag order in NSA flap," *USA Today*, June 12, 2013.

Senior Federal Judge James G. Carr, who served on the Foreign Intelligence Surveillance Court from 2002 through 2008, offers a model to improve the court that should be implemented.[315] The highlights of his model are the following:

- The Court was created in 1978 as a check on Executive branch authority
- The legitimacy of the court has come into question because of near total approval of surveillance requests
- The court works off the radar screen (no transparency)
- Congress could restore confidence in the court's impartiality and integrity by authorizing judges to appoint lawyers to serve "pro bono public" for the public interest when legal issues come before it
- The naming of an advocate with high level security clearance to argue against government filings for a higher level of reasonable suspicion
- Having lawyers challenge legal assertions would result in better outcomes and more fully developed reasons for its decisions
- The appointed lawyer could appeal a decision in the governments favor to a FISA court of review and then to the Supreme Court
- In an ordinary search warrant request the target is notified at some point about the warrant and if indicted he can challenge the warrant or sue for damages. This is not the case under FISC.
- This puts basic constitutional protections at risk and casts doubts about the legitimacy of these courts

Redacting FISA court decisions of sensitive information that might disclose a source or information that might need to be kept secret would then allow the legal decision to be reviewed, which is another way of increasing transparency.

The experience of a judge who sat on the FISA court has to be given heavier weight in terms of a policy change recommendation. Judge Carr's suggestion for more transparency and balance should be considered objective because it goes against the status quo. This is not typical of a government insider.

315 James G. Carr, "A Better Court," *New York Times* article by a former FISC judge outlining a model to insert more balance in the FISA process, http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html?_r=0.

4. Conclusion

The focal points of this third policy option are an effective oversight policy to create more transparency and balance in security and privacy. Congress can create transparency in the classification of secrets about government surveillance activities through more mandated disclosure. Redacting the information that needs to be kept secret, while releasing the rest of the report, will allow Congress to play its rightful role of oversight.

Judicial oversight of domestic intelligence agencies and officials will be enhanced by implementing an appeals process and an adversarial process in applications for wiretaps and warrants similar to the one suggested in Section C by former FISC Judge Carr.

In order for any policy recommendation to be enacted that better balances security and liberty, it will have to be **politically acceptable to Congress**, it will have to address the **concerns of privacy and civil liberties advocates** (the public interest in this area is taken up by them) and it will have to be something that continues to **provide the domestic intelligence enterprise the tools needed** to prevent, deter and disrupt terror plots and identify suspects in an age of digital information that rapidly changes.

Chapter V will provide an analysis of the three policy options that have been outlined and how the three affected advocacy groups might react to them. The policy options offered are to:

- Maintain the status quo of the surveillance state by government officials
- Create a single integrated domestic intelligence agency for more accountability
- Methods to improve congressional/judicial oversight for more transparency and privacy protection.

V. ANALYSIS

A. OVERVIEW

This chapter will cross-reference each policy option proposed in Chapter III and cross-reference it with how willing the three stakeholder groups with a vested interest in balancing security and liberty in government surveillance activities to prevent, deter, disrupt terror plots and identify terror suspects, will be in accepting the trade-offs to achieve balance.

I will assess the acceptance of the policy options by the three stakeholder groups on the following scale. This score given to their position on each policy option will be based on the statements attributed to each and the accompanying citations contained in the policy option.

- Strongly Oppose
- Somewhat Oppose
- Ambivalent
- Somewhat Support
- Strongly Support

At the end of this assessment I will recommend a policy option that will have the best chance of gaining consensus from the stakeholder groups.

1. Civil Liberties Groups Position on Maintaining the Status Quo

As I have indicated throughout this thesis, civil liberty advocates whose mission statements advocate privacy protection for Americans have railed against the rise of the surveillance state post 9/11. They believe it is too intrusive into the private lives of Americans and non-Americans not suspected of terror involvement. Maintaining the status quo is a non-starter. The revelation made by the Edward J. Snowden leaks about NSA surveillance activity has only heightened their call to end electronic surveillance practices. ACLU executive director Anthony D. Romero has called for these programs to

be shut down.[316] He called the program dragnet surveillance and recommendations for improvement, too little too late.[317] The government is losing the argument with this group on convincing them that there are enough safeguards and that domestic intelligence officials can be trusted to monitor themselves.[318]

Civil liberties advocates will ***strongly oppose*** this policy option for reasons explained throughout this thesis that essentially is too much intrusion into areas traditionally protected by the U.S. Constitution, no adversarial challenge in the FISC and too many secrets that prevent effective oversight.

2. Grade (1)—Civil Liberties Advocates and Position of a Single Integrated Domestic Intelligence Agency

Although mistrustful of government intelligence operations, a single agency dedicated to domestic intelligence would allow for privacy groups to better coordinate their watchdog activities. The current fragmented state of agencies makes it difficult for them to navigate through the maze of information, rules of compliance and what congressional committee to report abuses to. This streamlined and seamless domestic intelligence model is more conducive to assigning accountability.[319] This is at a time when the approach to change domestic intelligence in the U.S. is by adding layers of bureaucracy, like the creation of the DHS.[320]

Civil liberties and privacy advocates will ***somewhat oppose*** the creation of a more seamless single integrated domestic intelligence agency similar to the UK's MI5.

316Charlie Savage, and Michael D. Shear, "President Moves to Ease Worries on Surveillance," New York Times, August 10, 2013, story on how President Obama trying to get control of growing controversy over NSA spying. http://www.nytimes.com/2013/08/10/us/politics/obama-news-conference.html?pagewanted=all&_r=0, 1.

317 Ibid., 2.

318Scott Shane, "Challenges to U.S. Intelligence Agencies Recall Senate Inquiry of '70s," New York Times news story on a decline in public support for government surveillance programs. http://www.nytimes.com/2013/07/26/us/politics/challenges-to-us-intelligence-agencies-recall-senate-inquiry-of-70s.html?pagewanted=all.

319 Priest and Arkin, Top Secret America, 133.

320Kettl, System Under Stress: Homeland Security And American Politics, 51–52.

3. Grade (2)—Civil Liberties and Privacy Advocates Position for More Congressional and Judicial Oversight

This policy option has the best chance at receiving the support of these groups. As explained throughout this thesis the biggest complaint about domestic intelligence activities since 9/11 has been too much intrusion in exchange for a little more security.[321] Congressional oversight is one of the few areas where civil liberties groups can file grievances to claims of privacy abuse since they have no standing to make claims in the FISC.[322] Congressional hearings as a result of the Snowden leaks have provided a renewed debate on privacy and have made the public more aware of the extent of the spying.

Civil liberties and privacy advocates will **strongly support** more effective oversight through a process of redacting and releasing more classified documents for more transparency. They would also strongly support an adversarial and appeals process in the FISA court. This would create the balance that privacy groups seek. They would also strongly support Congress using the authority they already possess by law to rein in domestic intelligence activities. This has been mentioned in the Congressional oversight policy option.

4. Grade (5)—Domestic Intelligence Agencies/Officials and Maintaining the Status Quo

This stakeholder group includes officials from the DHS, FBI, CIA, NSA, and state and local law enforcement. Any policy change has to take into account the needs of this group in the digital age and with the advancements in technology in providing them with the tools and flexibility to prevent, disrupt, deter and identify terror plots and suspects.

321Eric Dahl, Domestic Intelligence Today: More Security but less Liberty, Naval Postgraduate School (U.S.), Center for Homeland Defense and Security, (2011). https://www.hsdl.org/?view&did=691059, 1.

322Ann Beeson, and Jameel Jaffer, ACLU, Unpatriotic Acts: The FBI's Power to Rifle through Your Records and Personal Belongings Without Telling You, (2003-07), https://www.aclu.org/FilesPDFs/spies_report.pdf, 3.

This stakeholder group led by the executive branch lobbied hard for the passage of the Patriot Act. They maintained that terror groups were so intertwined in the use of global communications that unless they had access to personal communication technology without having to go back to the court each time for warrant or wiretap approval they would always be one step behind the next terror attack.[323]

This broad surveillance authority has helped thwart more than 50 potential attacks all over the world according to the NSA, including a plot to bomb the New York Stock Exchange.[324] To end or even return to the surveillance rules for domestic intelligence agencies and services pre-Section 215 of the USA PARTIOT Act would put national security at risk. Maintaining this authority is imperative and would be **strongly supported** by the domestic intelligence enterprise.

5. Grade (5)—2) Domestic Intelligence Officials/Agencies Support for a Single Integrated Domestic Intelligence Service Similar to UK MI5

This would require long-established agencies giving up turf. This has been an obstacle that has not been overcome since the passage of the 1947 National Security Act that attempted to put this function under one agency, the CIA. Numerous congressional reform efforts that followed all met with the same resistance that it always has, and nothing more than moving furniture around occurred. The biggest reason has been agency self-interest, agency culture, politics, and turf protection.[325] This stakeholder group would **strongly oppose** a move toward a single domestic intelligence service. A history of reform effort failure supports this.

6. Grade (1)—Domestic Intelligence Officials/Agencies Support for More Effective Congressional/Judicial Oversight

Calls by privacy advocates and members of Congress for more transparency and oversight into domestic intelligence activities, has been a game of cat and mouse. Domestic intelligence officials testified on Capitol Hill that they are sensitive to privacy

323 Bush, Kindle, loc, 3172, 3188, 3023, 3219.

324Josh Gerstein, "NSA: PRISM stopped NYSE attack," The Politico, June 18, 2013, http://www.politico.com/story/2013/06/nsa-leak-keith-alexander-92971.html, 1.

325Zegart, Spying Blind: The CIA, the FBI and the Origins of 9/11, 62–68.

and self-monitor for compliance. The response over and over again is that too much disclosure presents a national security risk. Former intelligence officer veteran Philip Mudd indicates that he sees little advantage an adversary gets by learning that U.S. domestic intelligence is collecting phone calls and e-mail records.[326] One promising aspect in terms of reining in the vast authority given to domestic intelligence services and agencies is that a lawyer in the Office of the DNI recently indicated in testimony on Capitol Hill that the Obama Administration is open to re-evaluating this (surveillance) program.[327]

Domestic Intelligence officials have resisted calls and attempts for more oversight saying it would make it more difficult to track terror plots and would **somewhat oppose** attempts at additional oversight or transparency.

7. Grade (2)—1) Congress and Support for Maintaining the Status Quo

In the decade following the 9/11 terror attacks, congressional support for increased surveillance authority in domestic surveillance operations is waning.[328] Unable to use the emotion of another catastrophic attack against the nation as support for the imbalance in security and liberty that is trending toward more intrusion into the private lives of individuals, the pendulum is swinging back toward more transparency.

The NSA has been reacting to the pressure for more transparency by declassifying previously labeled top-secret documents for congressional hearings.[329] Since so much of what occurs in the domestic intelligence enterprise is done in secret compounded by the experience and time needed to navigate through this specialized activity, it makes effective oversight difficult. Political pressure due in part to the Edward Snowden leak of

---

[326]Madhani and Jackson, "With NSA controversy, debate over secrecy is revived," *USA Today*, June 12, 2013, https://www.google.com/#q=with+nsa+controversy%2C+debate+over+secrecy+is+revived.

[327]Savage and Sanger, "Senate Panel Presses NSA on Phone Logs," *New York Times*, July 31, 2013, http://www.nytimes.com/2013/08/01/us/nsa-surveillance.html?pagewanted=all&_r=0.

[328]David Rogers, "NSA vote splits parties, jars leaders," *The Politico*, July 24, 2013, http://www.politico.com/story/2013/07/nsa-amendment-fails-94721.html.

[329]Jessica Meyers, "Calls mount for more transparency," *The Politico*, August 1, 2013, http://www.politico.com/story/2013/08/calls-mount-for-nsa-transparency-95020.html.

NSA surveillance programs has Congress succumbing to media and public pressure to scale back encroachment by domestic intelligence services and agencies.

Congress' support for continuing the status quo of enhanced surveillance programs is **ambivalent** at best as some members are somewhat opposed and others showing some support.

8. Grade (3+ or 3-)—2) Congress and Support of a Single Integrated Domestic Intelligence Service along the lines of the UK MI5

The 9/11 Commission Report that followed the terror attacks gave consideration to a new agency dedicated to intelligence collection and analysis in the United States.[330] They quickly went away from that direction in favor of adding yet another layer onto an already bureaucratic enterprise with a national intelligence center.[331]

The upside to creating one service responsible for the collection and analysis of intelligence has been examined in Policy Option 2. A downside is that too narrow of a focus on domestic intelligence does not necessarily eliminate concerns about civil liberty and privacy abuses and effective oversight.[332]

The reality is that a single integrated domestic intelligence service in the United States is highly unlikely due to congressional opposition. Congress appears to be **ambivalent** to **somewhat opposed** to the U.S. having a single domestic intelligence service. New developments like another intelligence failure or continued privacy and civil liberty abuses or continued oversight dysfunction due to a fragmented approach could begin a groundswell of support toward this concept.

330The 9/11 Commission Report, 423.

331 Ibid.

332James Burch, A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security, http://www.hsaj.org/?fullarticle=3.2.2, 1.

9. Grade (4)—2) Congress' Support for Improving its Oversight Function and Judicial Oversight as Well

Congress has admitted that the current oversight mechanism for intelligence is dysfunctional.[333] This acknowledgment is encouraging because denial of the problem would continue oversight ineffectiveness. They have recommended creating a single point of oversight and review for homeland security.[334] This consolidation has support among members of Congress.

Effective oversight to prevent privacy and civil liberty abuses by domestic intelligence services and agencies has been a struggle for Congress. Few members have a good base of knowledge on intelligence activities or the know-how about the technologies being used by domestic intelligence agencies to feel assured that effective oversight is occurring.[335]

There are indications, however, that Congress is beginning to exercise its oversight responsibilities by creating special commissions for more familiar committee hearings.[336] The purpose here is to decrease partisanship out of what is becoming a very political process.

Congress is demonstrating **strong approval** for significantly improving judicial and legislative oversight in calling for changes that increase transparency and protect government secrets at the same time. No longer are they willing to give a blank check to national security interests over privacy and civil liberties.[337]

---

[333] The 9/11 Commission Report, 420.

[334] Ibid.

[335] Ibid.

[336] Heymann and Keyyem, Preserving Security and Democratic Freedoms in the War on Terrorism, 6.

[337] Scott Shane, "Challenges to U.S. Intelligence Agencies Recall Senate Inquiry of '70s," *New York Times*, July 26, 2013, http://www.nytimes.com/2013/07/26/us/politics/challenges-to-us-intelligence-agencies-recall-senate-inquiry-of-70s.html?pagewanted=all&_r=0.

	Policy Option 1 **Expanded Surveillance Authority**	**Policy Option 2** **Single Domestic Intelligence Service**	**Policy Option 3** **More Effective Oversight from Congress and Courts**
Privacy / Civil liberties advocates	Strongly Oppose	Somewhat Oppose	Strongly Support
Domestic Intelligence Officials	Strongly Support	Strongly Oppose	Somewhat Oppose
Congress / Judiciary	Ambivalent / Divided Support	Somewhat Support	Strongly Support

Figure 2. Stakeholder groups and policy position

B. CONCLUSION

The pros and cons for support of each of the Policy Options have been discussed here, and the strengths and weaknesses have been detailed. The next chapter will propose a policy recommendation based on each stakeholder interest to keep a sustained balance to security and privacy.

VI. POLICY RECOMMENDATION

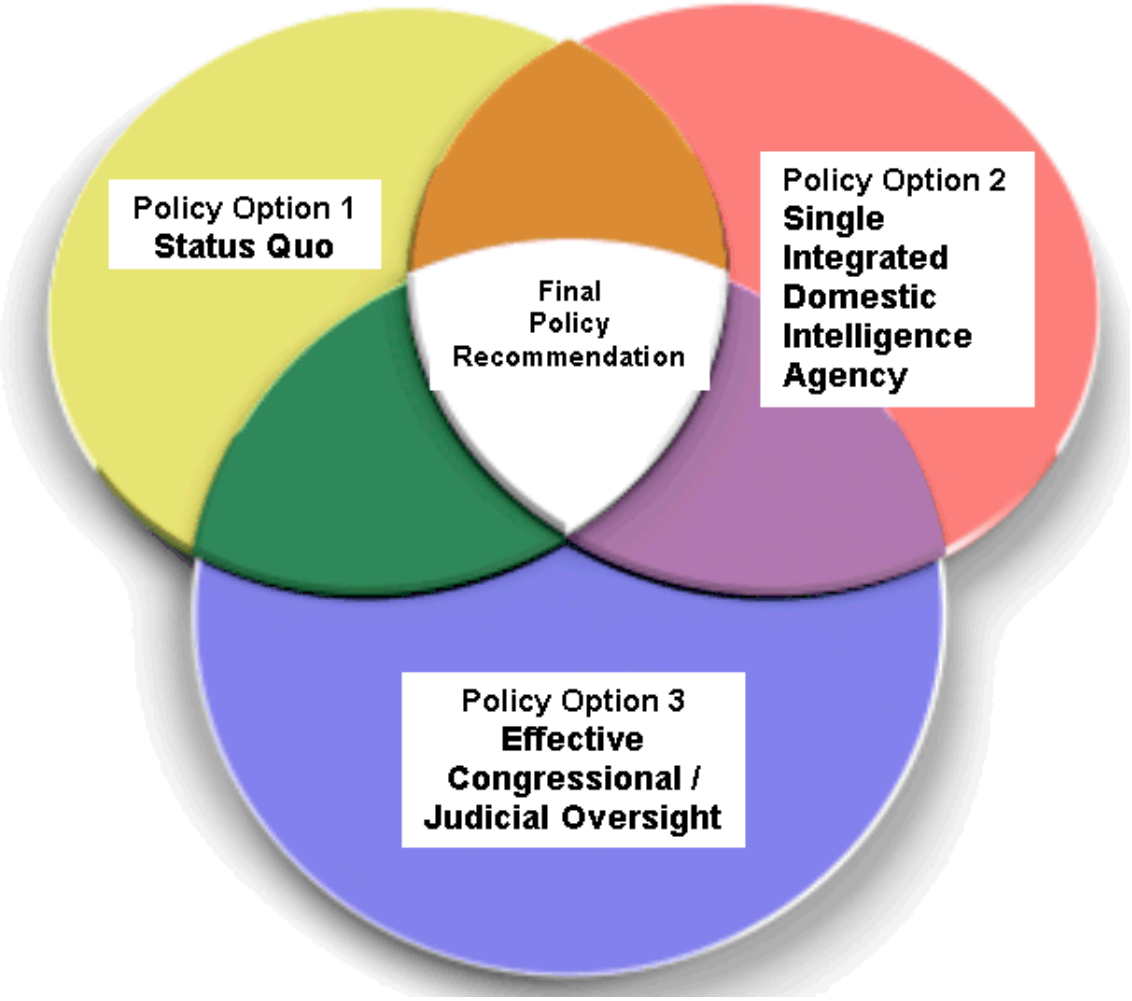

Figure 3. Policy recommendation incorporating elements of 3 policy options

A. OVERVIEW

This thesis has laid out the issues and concerns surrounding the growing gap between how best to empower domestic intelligence agencies due to the new threat presented by terror attacks, while maintaining the rule of law that protects privacy and ensures civil liberties.[338] These are not polar opposites.[339] The above image highlights

[338] Bobbitt, Terror And Consent: The Wars of the Twenty-First Century, 289.

[339] Clovis, Letter to the Editor: Twelve questions Answered, 7.

that I do not see this as a zero sum game where only one of the policy options is the best way forward. The policy recommendation will incorporate the strengths of each option examined. In doing so I am recommending incremental change, change that will not require a huge policy shift that is not likely to happen with the current gridlock due to partisan bickering in the U.S. Congress.

The issues I have identified are keeping surveillance operations secret and out of the hands of the opposition yet with enough transparency of these operations for Congress and the public to be able to debate their effectiveness and the costs associated with them, and finally a system of fairness consistent with a democratic state. The policy being recommending is keeping enhanced surveillance techniques in place in exchange for an adversarial process in the FISC, releasing more redacted classified reports frequently, including through the Freedom of Information Act so that a streamlined Congress oversight committee can effectively assess these activities.

B. I.D.E.A.S. POLICY RECOMMENDATIONS

Following are policy recommendation called **I.D.E.A.S.**

- **Incorporating** an adversarial process for wiretap and warrant applications as put forth by former FISC Judge James Carr.
- **Declassifying** documents more frequently after redacting them, as we have seen done by domestic intelligence officials in Capitol Hill hearings by DNI Jams Clapper and other intelligence officials for more transparency.
- **Educating** Congress and the public on the tactics of enhanced surveillance by government domestic intelligence agencies on things that do not compromise the methods used.
- **Authority** for domestic intelligence services and agencies to continue surveillance techniques.
- **Streamlined** congressional oversight that contains One House and one Senate Committee overseeing domestic intelligence agencies and services.

It will require trade-offs where domestic intelligence agencies and services allow more light to shine on their activities and do not reveal sensitive information, in exchange for keeping secret some aspects of surveillance operations. It will insert an adversarial process into a very one-sided FISC for balance. It does not pass the smell test when

15,000 wiretap and surveillance applications were made by the FBI to the FISC since 1978, and all but five were approved, and not even one was rejected.[340]

With the flurry of activity in Congress over NSA collecting wide swaths of personal data it should be apparent to most objective observers that there is a problem with what is being referred to as the *surveillance regime* by the ACLU.[341] It had been estimated that the NSA now collects 1.7 billion pieces of intercepted communications every twenty-four hours that includes cell phone conversations, e-mails, text and Twitter messages, instant messages, billboard postings, radio signals IP addresses and website changes.[342] This collection authority must be managed with a balance of privacy protections.

The domestic intelligence agencies are losing the argument for continuance of the programs, techniques and operations they are engaged in. What began as a fringe movement against these surveillance techniques to identify terror plots and suspects, years and even months ago, has built into momentum against these government activities.[343]

After initially indicating that they were comfortable with the scope of NSA collection of Americans' personal communication data, lawmakers are now signaling a willingness to use legislation to curb those actions.[344] The danger is that these agencies may have to begin to protect the country from terror with one hand tied behind their back like they did prior to 9/11 if they continue to resist calls for more transparency and more privacy and civil liberty protections. If domestic intelligence officials do not acquiesce to

---

[340] Beeson and Jaffer, Unpatriotic Acts: The FBI's Power to Rifle through your records and Personal Belongings without Telling You, 3.

[341] American Civil Liberties Union, "Reclaiming Patriotism: A Call to Reconsider the Patriot Act," 2001-03.

[342] Priest and Arkin, Top Secret America, 77.

[343] Jonathon Weisman, "Momentum Builds Against N.S.A. Surveillance," *New York Times*, July 29, 2013, A2.

[344] Ibid.

more transparency and privacy protections, Congress and the courts will do it for them.[345] People and business will seek relief through legislation and through non-Federal Intelligence Surveillance Courts.

Members of both political parties are indicating that they will introduce new legislation that would restrict surveillance to only those named as targets, make changes to the secret courts that oversee such programs and allow businesses permission to reveal their dealings before the court.[346] According to the Declaration of Independence, government derives its power to act by the consent of the governed. Citizens need to be aware of the balance between government control and individual freedoms in order to prevent the government from exceeding its powers and control.

C. MORE TRANSPARENCY CAN EDUCATE THE PUBLIC

Intelligence has been said to be the key to countering terrorism. These sensitive government activities might receive more public acceptance if there was more understanding about them.[347] That is the secrecy dilemma. The domestic intelligence enterprise might do well to establish a public relations department to keep the media and other interested parties apprised of some of the activities going on, and at the same time answer questions of concern from privacy and civil liberty advocates, instead of wrapping themselves around the cliché that everything is classified to protect national security interests.

Too much secrecy garners a sense of public mistrust no matter how well intentioned these officials are. This will be accomplished with more, instead of less, disclosure of reports with redactions to protect sensitive information about domestic intelligence operations and activities. Several classified documents were quickly declassified and used by domestic intelligence officials on Capitol Hill after the NSA

[345]Ellen Nakashima, Lawmakers, privacy advocates call for reforms at NSA," *Washington Post*, August 16, 2013, http://articles.washingtonpost.com/2013-08-16/world/41416448_1_nsa-national-security-agency-chief-judge.

[346] Ibid.

[347]Clovis, "Letter to the Editor: Twelve Questions Answered," *7.*

leaks.[348] In another instance, DNI James Clapper said he declassified aspects of NSA surveillance and intelligence programs to dispel some of the myths about government surveillance activities.[349] This makes one wonder about the classification process if reports can be top-secret one day and declassified the next.

Michigan Congressman John Conyers (D) asked why the Intelligence Community doesn't just tell people what they are doing. He answers by saying because people would be outraged. He adds that just because the intelligence community can demonstrate success in a handful of cases does not justify this level of intrusion. Republican Representative Bob Goodlatte of Virginia asks why government secrets should be indefinitely kept. An FISA court judge in closed testimony before a House Intelligence Committee hearing indicated that the one-sided nature of these courts might need to be restructured.

D. CONCLUSION

In summary, my policy recommendation **I.D.E.A.S.** creates the balance between broadened authority for domestic security initiatives and increased civil liberty protections in a way that improves both efforts at the same time. Domestic intelligence agencies keep the increased authority that is currently in place under the USA PATRIOT Act in exchange for quick reaction and flexibility to keep pace with cyber technology changes. The balance and trade-off will be to insert an adversarial process in the FISC recommended by Judge James Carr in Policy Option 3. Congress must take their own recommendation from the 9/11 Commission Report and streamline the oversight process of having only *one* House and *one* Senate select committee, instead of the dozens currently involved, for a more focused, effective and consistent oversight of homeland security agency accountability.

---

[348]Meyers, "Calls mount for NSA transparency," *Politico*, 1.

349Donna Leinwand, "Part of NSA's PRISM program declassified," *USA Today*, June 8, 2013, http://www.usatoday.com/story/news/nation/2013/06/08/dni-declassifies-prism-data-collection-nsa-secret-program-obama/2403999/.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. THESIS IMPLEMENTATION PLAN

A. HOW WE GOT HERE

The question asked at the start of this thesis was how to better balance security and privacy in the post 9/11 era. By using policy analysis as a methodology, I made a policy recommendation in Chapter VI that focused on a more transparent process for effective oversight and an adversarial FISC process that protects civil liberties. Taking a domestic intelligence enterprise that is shrouded in secrecy and making it more transparent so that the public in a representative democracy can provide input into whether it approves or disapproves of government activities will require give and take.

The policy recommendation that I arrived at includes streamlining the congressional oversight process of domestic intelligence operations that has become unmanageable. One count earlier cited in the analysis had different domestic intelligence agencies and services reporting to 88 different congressional committees and sub-committees. This adds to an already politicized process.

B. INCREASING PUBLIC TRUST

One problem is that there is no trust from civil liberties advocates and very little trust from the public and congressional members about privacy safeguards in enhanced government surveillance activities and operations. In a written statement by Judge Reggie B. Walton, the chief judge of the FISC, he acknowledged that the court lacks the tools to independently verify how often government surveillance breaks court rules that aim to protect privacy.[350] They have to rely on the honor system because they do not have the capacity to investigate noncompliance with its orders.[351] This is in stark contrast to what the executive branch has been saying in trying to reassure the public about the

[350]Carol D. Leonnig, Court: "Ability to police U.S. spying program limited," *Washington Post*, August 15, 2013, http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

[351] Ibid.

court's oversight role.[352] They have been saying that the court provides central checks and balances on government spying and that people should feel comfortable with that.[353]

C. HOW TECHNOLOGY ADVANCEMENTS CHANGED SURVEILLANCE METHODS

The explosion of new technologies since 9/11 has exponentially increased trails of data that Americans leave behind. Just about every movement a person makes, from smart phone use, to credit card purchases, to computer use, including sites visited and Internet searches, leaves a data trail. As I detailed in Policy Option 1, the law governing the use and exploitation of this data by domestic intelligence agencies and services lags behind the speed at which new technologies emerge. As was indicated in the previous section, courts cannot keep up with the volume of information coming in.

D. OBJECTIVES

My policy recommendation **I.D.E.A.S.** calls for adjustments that both sides of the aisle in Congress are calling for to recalibrate the scale of balancing security and liberty that achieves *more* security and *more* privacy.[354] We can have both.

E. WHAT DIFFERENCE WILL IT MAKE?

It will improve trust and understanding about domestic intelligence operations. For government to be successful in the area of homeland security, law enforcement agencies will need public help, public input and public acceptance.[355]

If the public finds government operations untrustworthy in the area of safeguarding privacy and civil liberties, then they are unlikely to participate in what they see as an illegitimate initiative.

---

352 Ibid.

353 Ibid.

354David Rogers, "NSA vote splits parties, jars leaders," The Politico, July 2013, http://www.politico.com/story/2013/07/nsa-amendment-fails-94721.html.

355The 9/11 Commission Report, 424.

F. WHO CARES?

The American people care, Congress cares, civil liberty and privacy advocates care, domestic intelligence officials care and as a student of the Naval Post Graduate school, I care. The recent reaction to the Eric Snowden leaks, the congressional response, media response and public discussion that followed demonstrate that these groups care. This discussion dominated the news for a significant period of time in an age where our 24-hour news cycle only allows for stories to dominate the front page a day or two at most.

G. WHAT IS NEW IN MY APPROACH?

I am not trying to reinvent the wheel here. Congressional action will be required for my policy recommendation of **I.D.EA.S.** to take place. Congress is a status quo town. The immigration debate is an example where the two political parties are gridlocked on reform. Huge leaps in change like we have seen in the passage of the Affordable Care Act, and creation of the DHS and TSA are rare. Incremental change that results in *more* security and *more* privacy protection is the optimal goal I am working toward in proposing this policy option.

H. COSTS

This is difficult to gauge because of, well, secrets. It is estimated that federal domestic intelligence agencies and services spend about ten billion dollars per year on keeping secrets.[356] Setting up a mechanism for more transparency and an adversarial system in the FISC will obviously incur some cost, but will be more than offset by money saved keeping secrets.

I. CREATING THE PLATFORM

Upon completion of this thesis I will distribute this **I.D.E.A.S.** policy recommendation for reading and discussion to Wisconsin Senator Ron Johnson, who sits on the Senate Homeland Security Committee. This Senate committee has as a

[356] Priest and Arkin, Top Secret America, 24.

subcommittee called the Permanent Subcommittee on Investigations (PSI) that has the responsibility of studying and investigating the efficiency and economy of operations relating to all branches of government.[357] The efficiency and economy of the current classification process can begin in this committee.

On the House side, I will distribute to Wisconsin Congressman James Sensenbrenner, the former head of the House Judiciary Committee, and to Congressman and former Vice Presidential Candidate Paul Ryan. These are three main players in Congress from Wisconsin and they wield a lot of influence in Washington. Congressman Sensenbrenner is the author of Section 215 of the USA PATRIOT Act. Paul Ryan is chairman of the House Budget Committee. This committee has leverage in forcing or influencing change in domestic intelligence services and agencies through the power of the purse.[358] This leverage was discussed in Policy Option 3.

Should domestic intelligence officials and the FISC slow walk the **I.D.E.A.S.** policy recommendation of more transparency and an adversarial process in exchange for continued surveillance authority then Congress' funding and legal authority in the oversight area can be used as a carrot.

I applied for this program at NPS and indicated that I was pursuing this degree to gain a base of knowledge necessary to speak intelligently about an array of homeland security issues, and to gain the credibility that goes along with a degree from the Naval Post Graduate School. I have an established relationship with these three members of Congress and will use those relationships as my platform by acting as a policy advisor, including giving testimony before this committee.[359]

Additionally, I will continue to write issue papers on homeland security-related topics for submission to journals, periodicals and newspapers.

---

[357] U.S Senate Committee On Homeland Security & Governmental Affairs, www.hsgac.senate.gov/about.

[358] House of Representatives Committee On The Budget, http://budget.house.gov/about.

[359] Bratton and Tumin, The 8 Tests of Readiness on Collaboration. Test 5 is having top performers backing you and test 7 is to mind your political support and stay in its headlights, 4–5.

J. HOW LONG WILL IT TAKE?

The Platform building discussed in section G will begin immediately after this thesis is published by NPS. With change there is no finish line. The process of balancing security and privacy will always need to be recalibrated.

K. CLOSING/AREAS FOR FURTHER STUDY

An area that I see in need of further study that could not be fully expanded on here because that is a thesis unto itself is whether the policy of the U.S. for terror attacks that occur in the United States should be handled as a war-fighting strategy or through law enforcement and our criminal justice system. The pros and cons of each approach with policy analysis as a methodology would be my recommendation. A model based on risk instead of hype should be examined.

To prosecute terror on a war-fighting continuum leaves the psyche of the American people in a perpetual state of war, and the level of heightened fear that goes along with that strategy.[360] On the other hand a war-fighting approach allows for more flexibility in intelligence collection and analysis as discussed in this paper in Policy Option 1.[361]

One advantage to prosecuting these terror acts from a law enforcement/criminal court angle is that many of the privacy issues talked about in this thesis would be addressed; for instance, an adversarial court process that provides clearer constitutional protections and more judicial oversight and transparency.[362] MI5 uses this approach. The cost aspect both financially and psychologically can be weighed and compared in this further study.

---

[360]Bonger, Brown, Beutler, Breckenridge, and Zimbardo, *Psychology of Terrorism*, Oxford Press, New York, (2007), *Terrorism Stress Risk Assessment and Management*, Douglas Paton and John M. Violanti, 228.

[361] Morag, Comparative Homeland Security: Global Lessons, 64.

[362] Ibid., 64–65.

There is no one right way or best practice when it comes to confronting terror while protecting privacy. A continual review through study and analysis of strategies, policies and laws will be required.

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.
>
> Supreme Court Justice Louis D. Brandeis

LIST OF REFERENCES

The 9/11 Commission Report. New York: W. W. Norton & Company.

Ackerman, Spencer, and Paul Lewis. 2013. U.S. Senators Rail Against Intelligence Disclosures Over NSA Practices. *The Guardian*, June 18, 2013.

ACLU. Reclaiming Patriotism: A Call to Reconsider the Patriot Act. Accessed September 12, 2013, http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf.

———. What's Wrong With Fusion Centers? Accessed September 13, 2013, www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

———. American Civil Liberties Union. Insatiable Appetite: The Government's Demand for New and Unnecessary Powers After September 11. Accessed September 13, 2013, https://www.aclu.org/national-security/insatiable-appetite-governments-demand-new-and-unnecessary-powers-after-september-.

Adachi, Ken. October 27, 2006. Senate and House Vote Roll Call on U.S. Patriot Act 2001 & 2006. Year. Educate Yourself. Accessed September 16, 2013, http://educate-yourself.org/cn/patriotact20012006senatevote.shtml.

Andrew, Christopher. 2009. *The Defense of the Realm: The Authorized History of MI-5*. New York: Penguin Books.

The Aspin-Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission. Accessed September 14, 2013, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article01.html.

Austin Center for Design. Understanding Wicked Problems. Accessed September 13, 2013, http://www.ac4d.com/home/philosophy/understanding-wicked-problems/.

Bansemer, John. 2008. Intelligence reform: A Question of Balance, Air University Press.

Best, Richard. 2010. Intelligence Reform After Five Years: The Role of the Director of National Intelligence. Darby: Diane Publishing Company.

Bobbitt, Philip. 2009. Terror and Consent: The Wars for the Twenty-First Century. New York: Anchor Books.

Bongar, Bruce, Lisa Brown, Larry Beutler, James Breckenridge, and Philip Zimbardo. 2007. *Psychology of Terrorism.* New York: Oxford Press.

Bonner, Raymond. 2008. Two British Anti-terror Experts Say U.S. Takes Wrong Path. *New York Times*, October 22, 2008.

Bowden, Mark. 2003. The Dark Art of Interrogation. *The Atlantic,* October 1, 2003.

Bradbury, Steven G. 2013. The System Works Well as It Is. *USA Today*, July 19, 2013.

Brafmann, Ori, and Robin Dunbar. 2006. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations.* New York: Penguin Books.

Bratton, William, and Zachary Tumin. 2012. *Collaborate or Perish: Reaching Across Boundaries in a Networked World.* New York: Crown Press.

Breckenridge, James N., and Philip G. Zimbardo. 2007. *The Strategy of Terrorism and the Psychology of Mass Murder*. New York: Oxford University Press.

Burch, James. 2007. A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implication for Homeland Security. *Homeland Security Affairs* III, no. 2 (June 2007). Accessed September 14, 2013, http://www.jsaj.org/?fullarticle=3.2.2.

Bush, George W., eds 2010. *Decision Points.* New York: Crown Publishers. Kindle.

Carr, James G., 2013. A Better Secret Court. *New York Times,* July 23, 2013, Opinion Section.

Chalk, Peter, and William Rosenau. 2004. *Confronting the "Enemy Within:* Security Intelligence, the Police, and Counterterrorism in Four Democracies. Santa Monica: Rand Corporation.

Clarke, Peter. 2007. Learning from Experience: Counter Terrorism in the UK since 9/11. Paper presented at the Colin Crampton Memorial Lecture Policy Exchange, April 24, 2007, in UK.

Crump, Catherine, and Jay Stanley. 2013. Why Americans Are Saying No to Domestic Drones. *Slate.com*, February 11, 2013. Accessed September 12, 2013, http://www.slate.com/articles/technology/future_tense/2013/02/domestic_surveillance_drone_bans_are_sweeping_the_nation.html.

Davis, James. 2013. The Role of the Fusion Center in COUNTERTERRORISM OPERATIONS. The Police Chief, February 2013.

Editorial Board Opinion. 2013. Lift the Veil of Secrecy on the Nation's Security Court. *USA Today,* July 18, 2013.

Everett, Burgess, and Jake Sherman. 2013. Republican Lawmakers: NSA Surveillance News to Us. *Politico.com*, June 7, 2013. Accessed September 11, 2013, http://www.politico.com/story/2013/06/republicans-nsa-surveillance-92418.html.

Federation of American Scientists. Institutional Reform: An Application of Organizational Theory to Reform the Intelligence Community, (1997–2001). Accessed September 15, 2013, http://www.fas.org/irp/eprint/snyder/organization.htm.

Fox 6 Now. 2013: Accessed May 30, 2013, http://fox6now.comtsa-removes-body-scanners-as-too-revealing.

George, Justin. 2013. ACLU Says License Plate Readers Violate Drivers' Privacy. *Baltimore Sun,* July 17, 2013.

Gellman, Barton. 2013. NSA Statements to the Post. *Washington Post,* August 15, 2013.

Gellman, Bruce. 2013. NSA Broke Privacy Rules Thousands of Times Per Year, Audit Shows. *New York Times*, August 15, 2013.

Gerstein, Josh. 2013. NSA: PRISM stopped NYSE attack. *Politico,* June 18, 2013. Accessed September 14, 2013, http://www.politico.com/story/2013/06/nsa-leak-keith-alexander-92971.html, 1.

Gibson, Ginger. 2013. Amash, Conyers introduce NSA bill. *Politico,* June 18, 2013.

Global Research. Secret FISA Court Redefines Law to Justify Illegal Spying Operations. Global Research. Accessed September 14, 2013, http://www.global research.ca/secret-fisa-court-redefines-law-to-justify-illegal-spying-operations/5342183.

Greenwald, Glenn. 2013. NSA Collecting Phone Records of Millions of Verizon Customers Daily. *New York Times,* June 6, 2013.

Hoffman, Bruce. 2002. A Nasty Business. *The Atlantic,* January 2002.

House of Representatives COMMITTEE ON THE BUDGET. 2008: About the Budget Committee. http://budget.house.gov/about.

Institute for Intergovernmental Research. Criminal Intelligence Systems Operating Policies (28 CFR Part23) Training and Technical Assistance Program.

Jackson, David. 2013. Obama Defends Surveillance Programs. *USA Today,* June 7, 2013. News section.

Johnson, Kevin, and David Jackson. 2013. Holder says Four U.S. Citizens Killed in Drone Strikes. *USA Today,* May 22, 2013. News section.

Johnson, Loch J., and James J. Wirtz, 2008. *Intelligence: The Secret World of Spies.* New York: Oxford University Press.

JSTOR Digital Library. Should Spies be Cops? Accessed September, 16, 2013, http://www.jstor.org/stable/1149438.

Kayyem, Juliette. 2012. Never Say "Never Again." FP National Security. September 11, 2012.

Keller, Susan Jo. 2007. Judge Rules Provisions in Patriot Act to be Legal. *New York Times,* September 27, 2007.

Kettl, Donald. 2007. Systems Under Stress: Homeland Security and American Politics. Washington D.C.: CQ Press.

Leinwand, Donna. 2013. Part of NSA's PRISM Program Declassified. *USA Today*, June 8, 2013.

Leonnig, Carol D. 2013. Court: Ability to Police U.S. Spying Program Limited. *Washington Post*, August 15, 2013.

Madhani, Aamer, and David Jackson. 2013. With NSA Controversy, Debate Over Secrecy Revived. *USA Today*, June 12, 2013.

Mazzetti Mark, and Shane Scott. 2013. Threats Test Obama's Balancing Act on Security. *New York Times,* August 9, 2013. U.S. Section.

Meyers, Jessica. 2013. Calls mount for more transparency. *The Politico,* August 1, 2013. Accessed September 14, 2013, http://www.politico.com/story/2013/08/calls-mount-for-nsa-transparency-95020.html.

Morag, Nadav. 2011. *Comparative homeland security: Global lessons.* Hoboken, New Jersey: Wiley Press.

Mueller, John, and Mark G. Stewart. 2011. *Terror, Security and Money: Balancing Risks, Benefits, and Costs of Homeland Security.* New York: Oxford University Press.

Nakashima, Ellen. 2013. Lawmakers, Privacy Advocates Call for Reforms at NSA. *Washington Post*, August 16, 2013.

National Commission on Terrorism Report. Background and Issues for Congress. Accessed September 14, 2013, https://www.hsdl.org/?view&did=144.

———. Leashing the Surveillance State: How to Reform Patriot Act Surveillance Authorities. Accessed September 15, 2013, *h*ttps://www.hsdl.org/?view&did=5259.

———. Letter to the Editor: Twelve Questions Answered, Accessed September 14, 2013, http://www.hsdl.org/?view&did=34925.

———. United States Department of Defense, Office of the Inspector General, 2003: DoD addressing concerns of Senators Grassley, Nelson, and Hagel on safeguards against governmental abuse of power in developing technology programs, United States Department of Defense. Accessed September 14, 2013, http://www.hsdl.org/?view&did=443324.

———. From Stove-pipe to Network Centric Leveraging Technology to Present a Unified View. Accessed September 14, 2013, https://www,hsdl.org/?view&did=455174.

———. Patriot Act and Civil Liberties; A Closer Look Accessed September 15, 2013, https://? https://www.hsdl.org/?view&did=469628.

———. Reducing Overclassification Through Accountability. Accessed September 14, 2013, https://www.hsdl.org/?view&did=689494.

———. Defining Homeland Security: Analysis and Congressional Considerations, Congressional Research Service Report for Congress. Accessed September 14, 2013, https://www.hsdl.org/?view&did=728387.

———. Are Democrats Better on Privacy and Surveillance? Accessed September 14, 2013, https://www..org/?view&did=231875.

———. Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You, September 15, 2013, https://www.aclu.org/FilesPDFs/spies_report.pdf.

———. Privacy: Key Recommendations of the 9/11 Commission. Accessed September 15, 2013, https://www.hsdl.org/?view&did=727019.

———. More Security but Less Liberty? Accessed Septenber 15, 2013, https://www.hsdl.org/?view&did=691059.

———. Federal Support for Involvement in State and Local Fusion Centers, Majority and Minority Staff Report, Permanent Subcommittee on Investigations, United States Senate, United States Congress. Accessed September 14, 2013, https://www.hsdl.org/?view&did=723145.

———. Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States. Accessed September, 16, 2013. https://www.fas.org/irp/crs/RL31920.pdf.

———. IC 21: The Intelligence Community in the 21st Century: Staff Study, Permanent Select Committee on Intelligence, House of Representatives, 104th Congress. Accessed September 16, 2013, https://www.hsdl.org/?view&did=439040.

———. Information Sharing Environment: Annual Report to the Congress (2011). Accessed September 16, 2013, https://www.hsdl.org/?view&did=489520.

———.Recent Patterns of Terrorism Prevention in the United Kingdom. Accessed September 16, 2013, https://www.hsdl.org/?view &did=482786.

———. Summary of Fusion Centers; Core Issues and Options for Congress, CRS Report for Congress. Accessed September 14, 2013, https://www.hsdl.org/?view&did=479037.

———. Countering the Threat of International Terrorism, Report of the NCT, 105th Congress, Accessed September 14, 2013. https://www.hsdl.org/?view&did=992.

———. Civil Liberties and Domestic Terrorism. Accessed September 14, 2013. https://www.hsdl.org/?view&did=44798.

———. Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center. Accessed September 14, 2013, https:www.hsdl.org/?view&did=35177.

———. Information on Law Enforcement's Use of Closed Circuit Television to Monitor Selected Federal Property in Washington D.C. Accessed September 14, 2013, https://www.hsdl?/view&did=437710.

———. What's Wrong with Fusion Centers? Accessed September 14, 2013, https://www.hsdl.org/?view&did=20071212.pdf.

———. Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress, March 19, 2010. Accessed September 16, 2013, https://www.hsdl.org/?view&did=27362.

———. Intelligence Reform: Question of Balance. Accessed September 16, 2013, https://www.hsdl.org/?view&did=470737.

———. Statement on Reforming the Patriot Act: A Report by the Constitution Project's Liberty and Security Committee. Accessed September 15, 2013, https://www.hsdl.org/?view&did=685217.

———. Hard Lessons Won: How Police Fight Terrorism in the United Kingdom. Accessed September 15, 2013, http://www.manhattan-institute.org/pdf/scr_01.pdf.

National Memorial Institute for the Prevention of Terrorism. Long-Term Strategy Project for Preserving Security and Democratic Freedoms in the War on Terrorism. Accessed September 13, 2013, http://www.mipt.org/Long-Term-Legal-Strategy.asp.

O'Harrow, Robert, Jr., Ellen Nakashima, and Barton Gellman. 2013. U.S., Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data. *The Washington Post*, June 8, 2013.

Pew Research Center. Government Surveillance: A Question Wording Experiment. Accessed September 15, 2013, http://www.people-press.org/2013/07/26/government-surveillance-a-question-wording-experiment/.

Priest, Dana, and William M. Arkin. 2010. A hidden world growing beyond control. *Washington Post*, July 19, 2010.

———. 2011. *Top Secret America.* New York: Little Brown and Company.

Recommendations for Fusion Centers, Preserving Privacy and Civil Liberties While Protecting Against Crime and Terrorism. The Constitution Project. Accessed September 15, 2013, www.constitutionproject.org/pdf/fusioncenter.report.pdf.

Response to the Senate PSI Report Joint Statement. Accessed September 12, 2013, https://nfcausa.org/default.aspx?menuitemid=167&menugroup=Home+New.

Rogers, David. 2013. NSA vote splits parties, jars leaders. *Politico.com*, July 24, 2013. Accessed September 14, 2013, http://www.politico.com/story/2013/07/nsa-amendment-fails-94721.html.

Savage, Charlie. 2007. U.S. Weighs Wide Overhaul of Wiretap Laws. *New York Times*, May 5, 2007.

Savage, Charlie, and David E. Sanger. 2013. Senate Panel Presses NSA on Phone Logs. *New York Times*, July 31, 2013.

Savage, Charlie, Edward Wyatt, and Peter Baker. 2013. U.S. Confirms That it Gathers Online Data Overseas. *New York Times*, June 7, 2013.

Savage, Charlie, and Michael D. Shear. 2013. President Moves to Ease Worries on Surveillance. *New York Times,* August 10, 2013.

Shane, Scott. 2013. Challenges to U.S. Intelligence Agencies Recall Senate Inquiry of 1970s. *New York Times*, July 26, 2013.

Shemella, Paul. 2011. *Fighting Back: What Governments Can Do About Terrorism.* Stanford: Stanford University Press.

Sims, Jennifer, and Berton Gerber. 2005. *Transforming U.S. Intelligence*. Washington D.C. : Georgetown University Press.

Smith, Paul A. 2013. Counter Terrorism Contingency Planning. Lecture at the Naval Post Graduate School, January 29–30, in Monterey California.

Snider, Britt L. The Center for Studies of Intelligence. A Different Angle on the Aspin-Brown Commission. Accessed September 15, 2013, https://www.cia.gov/library/center-for-the-study-of-intelligence.

Social Science Research Network. A False Sense of Insecurity. Accessed September, 14, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=604063.

Spetalnick, Matt, and Steve Holland. "Obama Defends Surveillance Effort as 'Trade-Off' for Security," *Reuters News*, June 8, 2013, article detailing Obama's justification for sweeping U.S. surveillance program, Accessed September 15, 2013. http://www.reuters.com/article/2013/06/08/us-usa-security-records-idUSBRE9560VA20130608.

Stimeare, R. 2005. Is It Really Possible to Prevent Interagency Information-Sharing from Becoming an Oxymoron? Master's Thesis, Army War College, Naval Postgraduate School, Monterey, CA.

Techdirt. Homeland Security 'Fusion' Center Director: We're Not Spying On Americans..Just Anti-Government Americans. Accessed September 14, 2013, http://www.techdirt.com/articles/20130402/02150622543/homeland-security-fusion-center-director-were-not-spying-americans-just-anti-government-americans.shtml.

———. Key Loophole Allows NSA to Avoid Telling Congress About Thousands of Abuses. Accessed September 15, 2013, http://www.techdirt.com/articles/20130817/02451024219/key-loophole-allows-nsa-to-avoid-telling-congress-about-thousands-abuses.shtml.

Terrorist Financing and the Internet. Accessed September 16, 2013, http://www.tandfonline.com/doi/abs/10.1080/10576101003587184#preview.

U.S. Intelligence Community Reform Studies Since 1947. Accessed September 16, 2013, https://www.hsdl.org/?view&did=457744.

U.S. Sente Committee on Homeland Security & Governmental Affairs. Accessed September 13, 2013, www.hsgac.senate.gov/about.

Weisman, Jonathon. 2013. Momentum Builds Against N.S.A. Surveillance. *New York Times*, July 29, 2013.

Winter, Michael. 2013. White House Defends Need to Collect Phone Records. *USA Today*, June 5, 2013.

Yahoo News. 2013: Feds: Boston Suspect Downloaded Bomb Instructions. Accessed September 14, 2013, http://news.yahoo.com/feds-boston-suspect-downloaded-bomb-instructions-195945432.html.

Zegart, Amy B. 2007. *Spying blind: The CIA, FBI, and the Origins of 9/11*. Princeton, New Jersey: Princeton University Press.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California