Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2021

Applying the Narrative Policy Framework to the USA FREEDOM Act of 2015

Michael Sean Hall
Walden University

Follow this and additional works at: https://scholarworks.waldenu.edu/dissertations

 Part of the Law Commons, Public Administration Commons, and the Public Policy Commons

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Michael S. Hall

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Mary Brown, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Michael Brewer, Committee Member,
Public Policy and Administration Faculty

Dr. Ian Cole, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Applying the Narrative Policy Framework to the USA FREEDOM Act of 2015

by

Michael S. Hall

MPA, Grand Canyon University, 2014

BS, Grand Canyon University, 2013

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2021

Abstract

The domestic security dilemma is a recurring problem whereby counterterrorism programs are continuously in a state of flux as demands for increased civil liberties and national security compete, as demonstrated by the USA PATRIOT Act of 2001 and USA FREEDOM Act of 2015. The National Security Agency bulk metadata collection program (NSA Surveillance Program) was created to identify terrorists and prevent terrorist attacks, but the USA FREEDOM Act prohibited the program in 2015. The NSA Surveillance Program's prohibition is problematic because the United States may not obtain the intelligence necessary to prevent a terrorist attack. The purpose of this qualitative narrative case study was to describe how members of the House Judiciary Committee may have used rhetorical speech during the congressional hearing held on July 17, 2013, when speaking about the NSA Surveillance Program. Rhetorical speech is the use of narrative characters (e.g., hero, villain) that may adversely affect rational judgment and policy decisions. The congressional hearing transcript was collected from the Government Publishing Office, and the Narrative Policy Framework's content analysis was used to analyze the data. Four key findings emerged from this study: (a) Congress was most frequently identified as the hero, (b) the Coalition was most frequently identified as the villain, (c) Congress defended the USA PATRIOT Act, and (d) Congress was most interested in the program’s legality/constitutionality rather than its effectiveness. This study may enhance the legislators' proclivity toward informed decision making when confronted with rhetorical discourse, thereby leading to improved policy outcomes that foster positive social change for the United States.

Applying the Narrative Policy Framework to the USA FREEDOM Act of 2015

by

Michael S. Hall

MPA, Grand Canyon University, 2014

BS, Grand Canyon University, 2013

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2021

Dedication

I dedicate this dissertation to my children, Kendahlia, Kaliber, and those yet to come. Never cease to push yourself intellectually and physically. Always stay together and help one another through this life. Most importantly, never lose your faith. I love you now, and I love you always.

Acknowledgments

First and foremost, I give thanks to my Lord and Savior, Jesus Christ, for His enduring love and guidance. Thanks to my Committee Chair, Dr. Mary Brown, for her leadership, encouragement, constructive critiques, and awesome sense of humor. Thanks to my Committee Member, Dr. Michael Brewer, and University Research Reviewer, Dr. Ian Cole, for their constructive critiques and encouragement. Also, thanks to my father, who served as my Committee Mentor, Dr. Steven Hall – I value the very long conversations concerning this dissertation's topic. Lastly, I thank my mother, who served as my Committee Cheerleader, Darlene Hall. This dissertation could not have been possible without my committee, and for that, I am grateful

Additionally, I thank the love of my life, Karla Hall, for her love and support throughout this doctoral journey. Also, I thank my loving children, Kendahlia and Kaliber, for the play dates and decompression time. My family kept me grounded throughout this very long and arduous process, and for that, I am grateful.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Mukasey (2015) contended the National Security Agency telephony metadata surveillance program (NSA Surveillance Program) was a beneficial counterterrorism program permitted under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act of 2001). However, according to Berman (2016), the NSA Surveillance Program was prohibited by the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015). The NSA Surveillance Program was a valuable tool used by the intelligence community to thwart terrorist attacks (Mukasey, 2015). Rhetorical speech used by members of the House Judiciary Committee at a congressional hearing may have contributed toward banning the National Security Agency (NSA) Surveillance Program (Weible & Sabatier, 2018). Rhetorical speech is the use of narrative characters (e.g., hero, villain) that may adversely affect rational judgment and policy decisions (Field, 2017; Jackson, 2005; Pilecki, 2017; Weible & Sabatier, 2018). Policymakers may use rhetorical speech to frame another individual, organization, or policy as the villain or hero to advantageously situate a preconceived policy agenda (Shanahan, Jones, & McBeth, 2018; Weible & Sabatier, 2018).

This research described how rhetorical speech was used by members of the House Committee on the Judiciary to prohibit the NSA Surveillance Program. This study examined the House Judiciary Committee hearing held on July 17, 2013 (Administration's Use of FISA Authorities), that pertained to the NSA Surveillance

Program. This study potentially has a nationally positive social implication as it is an attempt to identify how rhetorical speech adversely affects counterterrorism programs.

This chapter provides a brief background of the literature related to the scope of this topic. Following the background, I introduce the problem statement and purpose for this study. Then I describe the research question and the theoretical framework that confines and guides this study. Additionally, I present the nature of the study, assumptions, scope and delimitations, and limitations. This chapter concludes with the study's significance and a summary.

Background

This background serves as a summary of the research literature related to the scope of this topic by briefly describing the domestic security dilemma, USA PATRIOT Act of 2001, USA FREEDOM Act of 2015, and the NSA Surveillance Program. Additionally, this background identifies a gap in knowledge in this discipline and how this study will address the gap. This section concludes with why this study is needed.

The domestic security dilemma was vital to incorporate into this research as it framed the scope of this study. The scope of this study concerned the NSA Surveillance Program, which was authorized under the USA PATRIOT Act of 2001 and was prohibited under the USA FREEDOM Act of 2015 (Berman, 2016; Mukasey, 2015). However, before discussing the domestic security dilemma, it is necessary to mention its roots.

The domestic security dilemma evolved from the *security dilemma*, which was an international concept that identified when an enhanced security posture of a state takes

place, there is a contrasting effect where other states likewise enhance security measures, and so the process continues, which ironically possesses a counterintuitive result (Tang, 2009). Taking the notion of the security dilemma and applying it through a domestic lens, Field (2017) found that in addition to the ebb and flow of support for counterterrorism policy, the domestic security dilemma also has a counterintuitive result as it renders a "paradoxical effect of making people feel insecure about the excessive power of their own government" (p. 471). Thus, the domestic security dilemma is grounded in the notion that due to the continuous fundamental shift in counterterrorism policy, the U.S. government cannot sustain its terrorist fighting efforts (Field, 2017).

The domestic security dilemma is a recurring problem whereby counterterrorism programs are continuously in a state of flux as demands for increased civil liberties and national security compete (Field, 2017), as demonstrated by the USA PATRIOT Act of 2001 and USA FREEDOM Act of 2015 (Hu, 2018). The USA PATRIOT Act of 2001, which initially garnered much public support after the terrorist attacks on September 11, 2001, was perceived approximately a decade later as a law that granted too much power to the federal government (Field, 2017). One program in particular that captivated much public attention as a result of the USA PATRIOT Act of 2001 was the NSA Surveillance Program, which became publicly known in June 2013 due to an unauthorized disclosure (Forsyth, 2015). The NSA Surveillance Program stored and synthesized large quantities of metadata on U.S. citizens from third-party providers (e.g., Verizon) in order to identify possible terrorist suspects (Mukasey, 2015; Yoo, 2014). However, as a consequence of shifting support for counterterrorism policies, Congress passed the USA FREEDOM Act

of 2015, which restrained the NSA Surveillance Program by prohibiting the mass collection of metadata on U.S. citizens (Forsyth, 2015). This is problematic because the NSA Surveillance Program was deemed lawful and was a valuable tool for the intelligence community (Mukasey, 2015; NSA, 2015).

Legislators are faced with formulating policy in order to equip the government with the means to combat and defend against threats and vulnerabilities to the nation that were rarely contemplated nor encountered before September 11, 2001 (Bendix & Quirk, 2016). In addition to these challenges, members of Congress bear the responsibility of being a representative of their constituents and thereby implement legislation that coincides with their constituents' beliefs (Terchek & Conte, 2001). Paradoxically, while acting in the best interest of the public and in order for enhanced security measures to be enacted to pursue terrorists and defend against terrorist attacks, the erosion of civil liberties takes place (Shor, Baccini, Tsai, Lin, & Chen, 2018). As a consequence, the U.S. public becomes rightfully insecure in its perception of a monarchical type of government (Field, 2017).

The public's lack of sustained commitment to counterterrorism legislation and the NSA Surveillance Program may be predicated on three primary factors. The first is adversely affected behavioral and rational thought proceeding a terrorist attack (Perliger, 2012). Consequentially, Perliger (2012) argued that after a terrorist attack, decision-makers "stray from the conventional patterns of response" (p. 528), thereby preferring to escalate the nation's response to terrorism. The first factor is relevant to this study as it was reflected in the nation's response to the terrorist attacks on September 11, 2001,

which was the enactment of the USA PATRIOT Act of 2001 (Perliger, 2012). The second factor is the rhetorical speech utilized by policymakers to garner public support (Pilecki, 2017; Weible & Sabatier, 2018). Pilecki (2017) contended that politicians might choose to divide groups on a moral basis by strategically leveraging narration (Shanahan et al., 2018; Weible & Sabatier, 2018). Weible and Sabatier (2018) echoed Pilecki's (2017) claim by asserting that "policy debates are necessarily fought on the terrain of narratives" (p. 173). The second factor is relevant to this study as understanding the role of narratives is essential to understanding the policy process and how the process is affected (Weible & Sabatier, 2018). The third factor is the time elapsed since the attack occurred (Field, 2017). As demonstrated by the ebb and flow of public support for counterterrorism legislation, Field (2017) found that public support decreased as time progressed. The third factor is relevant to this study as it embodies the lack of sustainability for the NSA Surveillance Program and frames the scope of this research. All three factors are relevant to this study as they directly lead to the problem statement, which is provided in the next subsection of this chapter.

Although there are several studies pertaining to the NSA Surveillance Program, the USA PATRIOT Act of 2001, and the USA FREEDOM Act of 2015 (Barnett, 2015; Berman, 2016; Hu, 2018; Mukasey, 2015), the drafting phase (e.g., congressional hearings) for counterterrorism legislation is understudied (Pokalova, 2015; Shor et al., 2018). Therefore, if the drafting phase for counterterrorism legislation is understudied, it cannot be certain that politicians utilized and were subjected to rhetorical speech during their congressional hearings that led toward prohibiting the NSA Surveillance Program.

Thus, in this research I sought to examine one congressional hearing pertaining to the NSA Surveillance Program in order to describe how politicians may have used rhetorical speech and were subsequently subjected to its effects.

Indeed, the greatest challenge for U.S. counterterrorism efforts is the country's sustained determination to battle terrorism (Pillar, 2004). This study needed to be conducted to understand and describe how politicians may have been subjected to rhetorical speech that prohibited the NSA Surveillance Program. This study is important because rhetorical speech may have adversely affected thought patterns that led to prohibiting the NSA Surveillance Program. Irrational decisions in the political sphere are problematic as this may culminate in counterterrorism legislation that either enhances counterterrorism programs and erodes civil liberties or safeguards civil liberties and promotes less effective counterterrorism programs. However, this study may identify how rhetorical speech was used to prohibit a beneficial counterterrorism program, the NSA Surveillance Program.

Problem Statement

The problem is that Congress banned the NSA Surveillance Program (Field, 2017; Forsyth, 2015; Mukasey, 2015; Oversight of the Foreign Intelligence Surveillance Act, 2019; Stransky, 2015). The prohibition of the NSA Surveillance Program is problematic because the United States may not obtain the intelligence necessary to prevent a terrorist attack (Field, 2017; Mukasey, 2015; Oversight of the Federal Bureau of Investigation, 2013). Although there are several research articles on the effects of counterterrorism programs (e.g., NSA Surveillance Program), there is a lack of research focused on what

influences change in counterterrorism legislation during congressional hearings (Shor et al., 2018). Weible and Sabatier (2018) argued that policymakers might use rhetorical speech at congressional hearings, among other times, to influence change. Rhetorical speech is the use of narrative characters (e.g., hero, villain) that may influence and adversely affect rational judgment and decision making (Field, 2017; Jackson, 2005; Pilecki, 2017; Weible & Sabatier, 2018). However, there is currently a gap in the scholarly literature as there is no research focused on how policymakers used rhetorical speech at congressional hearings on the NSA Surveillance Program. It is essential to understand how policymakers may have used rhetorical speech at congressional hearings in order to describe how rhetorical speech influences counterterrorism legislation and consequently prohibits beneficial counterterrorism programs.

Purpose of the Study

The purpose of this qualitative narrative case study was to describe how members of the House Judiciary Committee may have used rhetorical speech during the congressional hearing held on July 17, 2013, when speaking about the NSA Surveillance Program. This study's results may lead to identifying how members of the House Judiciary Committee used rhetorical speech to prohibit the NSA Surveillance Program.

Research Question

The central research question was:

RQ: How, if at all, did members of the House Committee on the Judiciary use narrative characters during the July 17, 2013, congressional hearing on the NSA Surveillance Program?

The central research question focuses on understanding how, if at all, members of the House Committee on the Judiciary used narrative characters during the congressional hearing about the NSA Surveillance Program. The research question is confined to one hearing held by the House Committee on the Judiciary that pertained to the NSA Surveillance Program. The congressional hearing selected for this study took place on July 17, 2013. It was the first House Judiciary Committee open door congressional hearing that pertained to the NSA Surveillance Program after the program's unauthorized disclosure. The House Committee on the Judiciary was chosen due to the direct oversight the committee has on counterterrorism matters and the fact that Representative Sensenbrenner, a member of the committee, sponsored the USA FREEDOM Act of 2015 and its predecessor, the USA PATRIOT Act of 2001 (Forsyth, 2015).

Theoretical Framework

The Narrative Policy Framework (NPF) is grounded in the notion that narrative is the lifeblood of politics and can influence the outcome for legislation (Shanahan et al., 2018; Weible & Sabatier, 2018). Espousing the notion of the NPF that narrative characters leveraged by members of Congress wields power to influence legislation could detect how rhetorical speech may have affected the USA FREEDOM Act of 2015. Narrative characters are identified in the speech as a hero or villain that may be individuals, groups, or agencies (Shanahan et al., 2018). These narrative characters serve as the segment by which policymakers may infuse their politically-driven speech to influence another individual, group, or polity (Weible & Sabatier, 2018). According to Shanahan et al. (2018), the NPF comprises three levels, *micro*, *meso*, and *macro*.

Microlevel research focuses on the individual, macrolevel has a national focus, and the mesolevel research is concerned with testing its propositions in policy narratives from policy officials engaged in political discourse. This study used the mesolevel as it was the most appropriate for analyzing the policymakers' rhetorical speech at a congressional hearing. Chapter 2 provides a more thorough description of the theoretical framework.

Nature of the Study

The methodology chosen for this topic was a dyadic qualitative case study and narrative inquiry that applies content analysis bounded by the NPF. Qualitative analysis was selected due to its ability to critically evaluate a research question and express findings by way of holistically understanding phenomena (Rudestam & Newton, 2015). Qualitative research is recommended when the analysis concerns an emphasis on description, exploration, or meaning of the subject, and qualitative methods aid in evaluating various text, speeches, or conversations through inductive means (Rudestam & Newton, 2015). Specifically, the qualitative methodology was a logical means to answer a complex research question pertaining to the rhetorical speech utilized by policymakers (see Shanahan et al., 2018; Weible & Sabatier, 2018).

The research design was a coupled case study and narrative inquiry approach. I selected the case study method due to its facility for focusing on an organization, program, and event bounded by time (Rudestam & Newton, 2014). The case study is an effective tool for public administration scholars as its methods align with many policy analyses (Ravitch & Carl, 2016). Narrative inquiry is used when a researcher is seeking to understand phenomena through the exploration and analysis of a story or events

evolved through narration (Ravitch & Carl, 2016). Therefore, the coupled qualitative case study and narrative inquiry design was chosen to achieve an in-depth analysis of how, if at all, policymakers used rhetorical speech during a congressional hearing.

The data collection phase was focused on the speech from members of the House Committee on the Judiciary at a congressional hearing pertaining to the NSA Surveillance Program. The hearing chosen for this study took place on July 17, 2013. The selected congressional hearing was appropriate for this study as it was the first House Judiciary Committee hearing that took place in relation to the NSA Surveillance Program after the program's unauthorized disclosure. Additionally, the focus is on the *collective response* of the congressional committee. Therefore, the collective response comprises the narrative characters spoken by congressmen and congresswomen who communally composed the congressional committee.

The data analysis phase consisted of content analysis (Shanahan et al., 2018; Weible & Sabatier, 2018). Content analysis is a method that has proven effective for other empirical qualitative studies using the NPF at the mesolevel and is congruent with answering the research question (Shanahan et al., 2018; Weible, Olofsson, Costie, Katz, & Heikkila, 2016; Weible & Sabatier, 2018;). Content analysis consists of identifying the narrative characters within a text or speech and partitioning the findings into the appropriate category based on the assigned definition of the character (Shanahan et al., 2018). In this study I used two narrative characters for analysis, the hero and villain. The first character, hero, is an individual/coalition that solves or attempts to solve a problem

(Weible et al., 2016). Villain, the second character, is an individual/coalition "who cause[s] or attempt[s] to make the problem worse" (Weible et al., 2016, p. 423).

For example, a policymaker may speak to the government protecting its citizenry from terrorist attacks. This rhetorical speech would situate government as the perceived hero and terrorist as the villain. Alternatively, a policymaker may speak to the government infringing on the civil liberties of its citizenry. This rhetorical speech would situate government as the villain. Thus, the narrative character (e.g., hero or villain) is predicated on the policymaker's rhetorical speech. Therefore, content analysis is solely grounded in the policymaker's rhetorical speech and not whether the researcher agrees with what is said.

Texts identified as rhetorical speech leveraging the hero effect were assigned to the hero category. Likewise, the texts identified as rhetorical speech leveraging the villain effect were assigned to the villain category. Excerpts from the congressional hearing that were found to be congruent with the narrative character definitions were displayed in this study's findings.

Assumptions

I share the same core assumptions that ground the NPF. The first assumption is that public policy and the policy process vary based on human perception (Weible & Sabatier, 2018). The individual's perception matters in public policy as it contributes to the dialogue used to create policy (Weible & Sabatier, 2018). The second assumption is that individual perception, to some degree, is bounded by ideologies, belief systems, and norms, thereby making the policy process unique (Weible & Sabatier, 2018). In other

words, replacing members of the House Judiciary Committee with other individuals whose background differs would likely not produce the same outcome or dialogue. The third assumption is that narrative characters are generalizable and can be identified in various narrative contexts (Weible & Sabatier, 2018). The third assumption is relevant to this study as this research seeks to identify and analyze the narrative characters within a policy debate. The fourth core assumption of the NPF is that policy narratives operate simultaneously at three interacting levels: microlevel, mesolevel, and macrolevel (Weible & Sabatier, 2018). This fourth assumption is relevant to this research because a coalition (i.e., House Judiciary Committee) was being analyzed at the mesolevel; however, it is understood that the policy process is simultaneously affected by the microlevel and macrolevel. The fifth assumption is that people use the power of narrative to communicate, understand, and process information (Weible & Sabatier, 2018). Therefore, to some degree and no matter how minute, members of the House Judiciary Committee were likely to use rhetorical speech at the congressional hearing pertaining to the NSA Surveillance Program. Lastly, I assumed that NSA leadership and the Obama Administration were truthful when expressing concern regarding the program's legitimacy and benefit to the intelligence community and law enforcement (Mukasey, 2015; NSA, 2015; Obama Administration, 2013), rather than an attempt to save face or status.

Scope and Delimitations

Field (2017) addressed that narration played a role in the domestic security dilemma, and Pilecki (2017), Perliger (2012), and Pillar (2004) echoed this notion. The

most effective way to discover the utilization of narration in a policy subsystem is through employing a narratological framework grounded in the policy process (Weible & Sabatier, 2018). Therefore, for this study I chose the NPF as it is a narratological framework that can be applied to understand how narration may have been utilized to prohibit the NSA Surveillance Program.

This study is bound by the initial House Judiciary Committee congressional hearing that focused on the NSA Surveillance Program after the program's unauthorized disclosure to the public. I chose the House Judiciary Committee hearing that took place on July 17, 2013, for this study due to the fact it focused on the NSA Surveillance Program, and it was after the program's unauthorized disclosure. To understand the various themes that may have been discussed during the hearing, it was important for me to understand the multiple variables associated with the NSA Surveillance Program, including its legality, constitutionality, ethicality, and contribution to the intelligence community apparatus. Chapter 2 of this dissertation provides the literature review that discusses the aforementioned multiple variables in depth.

Although for this study I considered other means for data inquiry, it would not have been practical due to my limited available resources. Other sources of information for analysis would include analyzing the narrative climate that may have taken place during congressional hearings by other congressional committees. However, because Representative Sensenbrenner sponsored both the USA PATRIOT Act of 2001 and the USA FREEDOM Act of 2015, it seemed appropriate to choose the committee for which he was assigned and that oversaw intelligence collection/analysis matters (Forsyth, 2015).

Additionally, choosing to assess the narrative climate that may have taken place via media or social media outlets could prove to be beneficial at the microlevel or mesolevel of analysis. However, congressional hearings seemed to be the most appropriate setting for analysis per the NPF as it directly corresponds to the *agora narrans* concept where legislators may employ impassioned narratives to develop policy (Weible & Sabatier, 2018).

This study has the potential for transferability as the same framework may be used to analyze the narrative climate surrounding other counterterrorism policies. By applying the same framework and mode of analysis, separate pieces of counterterrorism legislation may be examined, such as the rhetorical/narrative climate leading to the enactment of the USA PATRIOT Act of 2001 or the Foreign Intelligence Surveillance Act. If those studies were to take place, the findings could be analyzed across a broad time continuum for counterterrorism legislation to identify any pattern analysis that may exist for the narrative/rhetorical climate that corresponds to counterterrorism policy outcomes. Also, any pattern analysis across the time continuum may enhance policy narrative learning, which could be extrapolated to predict future counterterrorism policy outcomes. Thus, the transferability for this study possesses the potential to deepen our understanding of the domestic security dilemma.

Limitations

The veracity of this research is limited to its scope. As the data includes identifying narrative characters at a congressional hearing, this research excludes press hearings, public speeches, media, social media, and other sources of potential data that

may enrich understanding regarding the effects of narration prohibiting the NSA Surveillance Program. The congressional hearing considered as data for this research is unclassified and is currently available to the public; thus, data will not consist of any classified or closed-door hearing. Also, for this research I only used the historical transcript and not the visual data that displayed or broadcasted the historic hearing. The use of the transcript was to ensure uniformity amongst the data collected and to exclude any visual interference that may subject me to biased conclusions.

I am the only researcher gathering and analyzing the data; therefore, it is not feasible nor practical for this study to include several congressional hearings or other sources of data. For example, conducting content analysis on the congressional hearings leading to the USA PATRIOT Act of 2001 and juxtaposing those findings to the discoveries presented from this study may prove to be very beneficial toward understanding how rhetorical speech affects counterterrorism legislation across a broad time continuum. Unfortunately, assistance would be required for such an undertaking.

As the sole researcher, issues of dependability arise regarding the analysis of narrative characters. Therefore, every excerpt from the congressional hearing transcript that applies to the particular narrative character is displayed in this study. Furthermore, to ensure the integrity of this research, each excerpt is explained as to why it is applicable to the narrative character per the NPF. Also, only the hero and villain are considered for this study, thus, not incorporating other possible characters such as the victim, opponent, or ally. Lastly, I sorted and analyzed data using NVivo 12 Plus software; therefore, any impairments with the software may present itself in the findings of this study.

Significance of the Study

The significance of this study is that it may advance the knowledge of this discipline by applying a narratological lens to understanding why the NSA Surveillance Program was banned, despite the fact that it was a counterterrorism program deemed lawful under the USA PATRIOT Act of 2001 and was considered beneficial to the intelligence collection apparatus (Mukasey, 2015; Yoo, 2014). Rhetorical speech influences legislation, and if left unchecked, it may adversely commandeer rational logic and decision making (Perliger, 2012; Pilecki, 2017; Weible & Sabatier, 2018;). Therefore, in this study I sought to reveal whether lawmakers used rhetorical speech during a congressional hearing and were consequently subjected to its effect. This study may enhance the legislators' proclivity toward informed decision making when confronted with rhetorical discourse and thereby lead to better policy outcomes, thus fostering positive social change for the United States (Weible & Sabatier, 2018). Additionally, this study contributes to the limited scholarly literature that uses content analysis. By contributing to the content analysis paradigm, this study is situated as a standard or example that other studies may resemble while using the NPF as a theoretical framework.

Summary

The problem is that Congress prohibited the NSA Surveillance Program from collecting bulk metadata on U.S. citizens (Field, 2017; Forsyth, 2015; Mukasey, 2015; Oversight of the Foreign Intelligence Surveillance Act, 2019; Stransky, 2015). The gap in the literature is in describing how members of Congress may have used rhetorical speech

during a congressional hearing on the NSA Surveillance Program. The purpose of this qualitative case study was to describe how members of the House Judiciary Committee may have used rhetorical speech during a congressional hearing on the NSA Surveillance Program. Therefore, in this research I sought to answer the central research question:

> RQ: How, if at all, did members of the House Committee on the Judiciary use narrative characters during the July 17, 2013, congressional hearing on the NSA Surveillance Program?

The significance of this study is that it may advance the knowledge of this discipline by applying a narratological lens to understanding why the NSA Surveillance Program was banned, despite the fact it was legal and a beneficial contribution to the intelligence community (Mukasey, 2015; Yoo, 2014). Additionally, this study contributes to the limited NPF scholarly literature that uses content analysis. The NPF was appropriate for this project as the framework evaluates and analyzes narration leveraged by policymakers within political subsystems (Weible & Sabatier, 2018). The dyadic qualitative case study and narrative inquiry was most appropriate for this project as it correctly aligned the study's rudiments in terms of scope and data sample and directly answered the research question. However, before deciding the methodology and conceptual framework, I became thoroughly immersed in the literature. The literature review consisted of studies related to the domestic security dilemma, the USA PATRIOT Act of 2001, the USA FREEDOM Act of 2015, and the NSA Surveillance Program. This literature review is described in detail in Chapter 2.

Chapter 2: Literature Review

The problem is that Congress banned the NSA Surveillance Program (Field, 2017; Forsyth, 2015; Mukasey, 2015; Oversight of the Foreign Intelligence Surveillance Act, 2019; Stransky, 2015). The prohibition of the NSA Surveillance Program is problematic because the United States may not obtain the intelligence necessary to prevent a terrorist attack (Field, 2017; Mukasey, 2015; Oversight of the Federal Bureau of Investigation, 2013). Weible and Sabatier (2018) argued that policymakers might use rhetorical speech at congressional hearings, among other times, to influence change. Rhetorical speech is the use of narrative characters (e.g., hero, villain) that may influence and adversely affect rational judgment and decision making (Field, 2017; Jackson, 2005; Pilecki, 2017; Weible & Sabatier, 2018). It is essential to understand how policymakers may have used rhetorical speech at congressional hearings in order to describe how rhetorical speech influences counterterrorism legislation and consequently prohibits beneficial counterterrorism programs.

Supporters for the NSA Surveillance Program argued it was: (a) beneficial to the intelligence community (Mukasey, 2015; Oversight of the Federal Bureau of Investigation, 2013), (b) approved several times by the Foreign Intelligence Surveillance Act Court (FISC), (c) legal per section 215 of the USA PATRIOT Act of 2001 (Berman, 2016), and (d) did not violate the U.S. Constitution (Mukasey, 2013; Obama Administration, 2013; Yoo, 2014). However, critics contended the NSA Surveillance Program violated civil liberties by intruding upon a person's reasonable expectation of privacy (Berman, 2016; Donohue, 2014) and that the collection of telephony metadata on

U.S. citizens was unconstitutional per the Fourth Amendment (Donohue, 2014; Liu, Nolan, & Thompson, 2015; Thompson, 2014).

This chapter outlines the literature search strategy used to obtain information regarding the domestic security dilemma, the USA PATRIOT Act of 2001, the USA FREEDOM Act of 2015, and the NSA Surveillance Program. I describe the NPF as the theoretical framework in greater detail and discuss why I chose the NPF as a framework. The third subsection is the literature review, which is a thorough analysis of studies related to the domestic security dilemma, the USA PATRIOT Act of 2001 and USA FREEDOM Act of 2015, and the NSA Surveillance Program. Lastly, this chapter concludes with a summary.

Literature Search Strategy

The literature search strategy was straightforward and concise. Key search terms consisted of a carefully chosen combination of words utilizing navigational, informational, and transactional search queries in order to narrow the results field. I used keywords such as *Narrative Policy Framework, rhetoric, domestic security dilemma, USA PATRIOT Act of 2001, USA FREEDOM Act of 2015,*and *National Security Agency bulk metadata surveillance* to conduct the literature search. Literature was primarily derived from the Thoreau database, although ProQuest Central, ResearchGate, and Academia proved useful and provided applicable scholarly articles. The articles selected for this study were peer-reviewed, and due to the contentious nature of the topic, sources that exhibited an extraordinary wealth of bias were not included in this research. In addition to scholarly articles, federal government reports, judicial decisions, and various

law journals played an invaluable role in contributing to this body of literature and framework.

Theoretical Framework

The NPF is grounded in the belief that narratology is fundamentally and inescapably vital to understanding communication (Weible & Sabatier, 2018). Narratives have a powerful impact on a person's decision/opinion toward a topic, and it is frequently employed by individuals, coalitions, and society (Weible & Sabatier, 2018). Used to enhance and diminish particular aspects of reality, a narrative is frequently utilized to entice, influence beliefs, and sway public opinion in order to support public policy (Jones & McBeth, 2010; Shanahan, Jones, & McBeth, 2011; Weible & Sabatier, 2018).

In response to debates exploring the collection of policy theories, the NPF serves as a bridge between two camps, the postpositivists, and positivist-oriented theorists. Collectively they enable policy analysis to be socially constructed and empirically measured (Shanahan et al., 2011). Postpositivists recognize policy as situated by narratives and social constructions, whereas positivist-oriented theorists rely on "clear concepts and propositions, causal drivers, prediction, and falsification" (Weible & Sabatier, 2018, p. 174). The blend of both camps is vital to the construct of the NPF as they foster an environment grounded in scientifically repeatable metrics flexible enough to analyze complex narrative elements.

Narrative Elements

Since its inception, the NPF has been used to understand complex public policies in the United States and on the international stage, with new methodologies employed

that expanded its application with political dilemmas (Weible & Sabatier, 2018). This is accomplished by identifying the narrative elements based upon micro, meso, or macro factors (Shanahan et al., 2018). The researcher chooses the level of analysis based on the object or phenomenon under study (Shanahan et al., 2018). Once the level of analysis is determined, the researcher extracts the appropriate data and identifies the appropriate elements (e.g., setting, characters, plot, moral of the story) within the policy narrative (Jones, Shanahan, & McBeth, 2014). The elements remain flexible based on differing parameters unique to the research, and they are acceptable so long as the scholar is clear about "which definition they adhere to and why" (Weible & Sabatier, 2018, p. 176).

In this study I applied one subsection of narrative elements, the characters. The characters consisted of the hero and villain (see Weible et al., 2016). The rationale for selecting characters was due to the belief that it would best answer the research question and fulfill the purpose statement. Chapter 3 provides greater depth and a rich description of the narrative characters.

Qualitative Method of Analysis

The qualitative method of analysis consists of content analysis. Content analysis is the initial identification of the narrative characters (Shanahan et al., 2018). Weible et al. (2016) emphasized the importance of congruency among narratological studies in terms of character definitions and means of utility regarding content analysis. Therefore, for the sake of replicability, transparency, and congruency, this study aligned with the same character definitions used by Weible et al. (2016). Content analysis is explained in greater depth in Chapter 3.

Core Assumptions

Weible and Sabatier (2018) identified several core assumptions of the NPF. Firstly, objects and processes exist independently of human perception, and those objects and methods vary based on a person's perception. Known as *social construction*, these objects and processes flux in meaning dependent on assigned perceptions of a particular group or individual. Secondly, social construction is varied based on *bounded relativity* and is thereby influenced by ideologies, dogma, normative axioms, and/or religious beliefs. Thirdly, it is assumed that *narrative elements are generalizably structured* and that these elements (i.e., characters) are identified in various policy narratives. Fourthly, *policy narratives take place at three levels simultaneously*: microlevel, mesolevel, and macrolevel, each level respective to the scope of impact and the object of study (e.g., individual, group, or nation). Lastly, the *homo narrans model of the individual* is based on the assumption that narrative plays a pivotal role in how individuals "process information, communicate, and reason" (Weible & Sabatier, 2018, p. 179).

Previous Applications of the Narrative Policy Framework

I have yet to identify scholarly research that applied the NPF in the context of this research. However, the closest research related to the scope of this study was conducted by Osinowo (2019). Osinowo applied the NPF in conjunction with another theoretical framework and sought to identify how the NSA obtained compliance from third party organizations (i.e., Internet and telecommunications industry) to obtain metadata. Though Osinowo's research was related to counterterrorism measures and involved the NSA Surveillance Program, it did not explicitly contribute to the scope of this study.

Rationale for the Narrative Policy Framework

I selected the NPF due to its ability to identify if narrative characters were utilized by the members of the House Committee on the Judiciary at one congressional hearing. The NPF was best suited for this analysis due to its application of positivist and postpositivist ideations, as well as enabling the ability to analyze scientifically and the flexibility to identify and gather narrative data (Weible & Sabatier, 2018). Additionally, the NPF aligned with this research as it was utilized to identify the narrative in a policy debate and, therefore, answer the research question and fulfill the purpose of this study. Lastly, as there are limited scholarly studies centered on utilizing the NPF for analysis (Shanahan et al., 2018), this research builds upon the existing theory by contributing to the content analysis repertoire.

Literature Review

This section presents a literature review related to the constructs for this study. One of the core constructs for this study was the domestic security dilemma, which is the lack of sustained commitment to counterterrorism legislation and, consequently, the United States' inability to effectively combat and defend against terrorism (Field, 2017). The domestic security dilemma applies to this study as two acts that highlight the lack of sustained commitment to counterterrorism legislation are the USA PATRIOT Act of 2001 and the USA FREEDOM Act of 2015, where the former permitted the NSA Surveillance Program and the ladder prohibited the NSA Surveillance Program (Field, 2017; Forsyth, 2015; Hu, 2018; Ombres, 2015; Congressional Digest, 2015). As this literature review is centered around the USA PATRIOT Act of 2001 and the USA

FREEDOM Act of 2015 as they pertain to the NSA Surveillance Program, it is necessary to specifically review section 215 of the USA PATRIOT Act of 2001 as that section was the provision under which the NSA Surveillance Program operated (Obama Administration, 2013). Thus, the domestic security dilemma is described below, along with how the NSA Surveillance Program operated under the confines of the USA PATRIOT Act of 2001 and then how the NSA Surveillance Program was altered by the USA FREEDOM Act of 2015.

Domestic Security Dilemma

Coined the *domestic security dilemma*, Field (2017) posited that after a terrorist attack occurs, public support for counterterrorism legislation/programs is strong and as time progresses and fear of a looming terrorist attack subsides, so does public support for such legislation. As evidenced shortly after the terrorist attacks on September 11, 2001, Pillar (2004) contended that the greatest challenge to the United States in combating terrorism is maintaining an unwavering, sustained determination of the public to battle it. Perliger's (2012) seminal work found that after a terrorist attack, behavioral and rational thought patterns are adversely affected, which ultimately elicits an emotional response enacted through aggressive counterterrorism policy. Similarly, Weible and Sabatier (2018), and Shanahan et al. (2018) inexplicitly supported the belief that an emotional response is the consequence of a terrorist attack by affirming that people make irrational decisions bounded by time and supported with limited information that is subjected to rhetorical speech.

Thus, if a terrorist attack possesses an adverse behavioral and rational thought pattern that is further subjected to rhetorical speech, then it is plausible to postulate that the terrorist attacks on September 11, 2001, adversely affected judgment resulting in the USA PATRIOT Act of 2001 and, as time progressed and fear of a looming terrorist attack diminished, the USA FREEDOM Act of 2015 was borne, thereby consequently prohibiting the NSA Surveillance Program. Romero (2015) supported this plausibility as he argued the USA FREEDOM Act of 2015 marked the "first time since 9/11 that the surveillance powers of the US government have been curtailed" (p. 1). Romero's sentiment was echoed by Mukasey (2015) when he implied that the magnitude of the criticism toward the NSA Surveillance Program was the "first time [] it's happened [toward the intelligence community] on this scale" (p. 207). However, to obtain a comprehensive understanding of the domestic security dilemma, it is essential to begin with the dilemma's roots.

Origins. The domestic security dilemma was espoused from the security dilemma, which was considered one of the most important contributions to the international relations field (Tang, 2009). The theoretical idea of the security dilemma was developed in the early 1950s by John Herz and Herbert Butterfield (Field, 2017), and it has been used to explain various significant events, such as the First World War, the Cold War, and conflicts in Africa (Tang, 2009). Additionally, the security dilemma has been utilized as a proactive effort for determining policies regarding international politics, such as the management of arms and fostering a climate of deconfliction between China and the United States (Tang, 2009).

Although Herz and Butterfield worked on the security dilemma concept separately, they shared similarities regarding the security dilemma's roots. For example, both Herz and Butterfield argued that polities are insecure about their survival and therefore take steps to ensure safety by enhancing their security (Field, 2017) – as observed by the USA PATRIOT Act's enactment in 2001 and implementation of the NSA Surveillance Program. The security enhancement has a paradoxical effect where other nations likewise compete to bolster security and military readiness (Field, 2017; Tang, 2009). However, although the pedagogy delivered by Herz and Butterfield aligned and shared similarities, the Herz perspective was grounded in humanity's insecurities regarding readiness, and the Butterfield perspective was centered on humanity's intrinsic fear of being attacked (Field, 2017; Tang, 2009).

Expanding upon the security dilemma as described by Herz and Butterfield, it seems plausible to surmise that man is not inherently malice, though his fear and insecurity grounded in a lack of trust/guarantee from whom he perceives as the threat drives him to actions which possess an inherent paradoxical effect that culminates in conflict. After the terrorist attacks on September 11, 2001, the 9/11 Commission report was borne and criticized the Intelligence Community for not sharing information with law enforcement agencies that may have prevented the devastating attacks in New York and Washington D.C. (Mukasey, 2015). The 9/11 Commission report, along with other publications criticizing the Intelligence Community, pressured the NSA to engage in controversial action in the name of national security that was later subject to reproach

(Mukasey, 2015) – thus, internal strife paradoxical effect, hence, the domestic security dilemma.

USA PATRIOT Act of 2001

As a response to the terrorist attacks on September 11, 2001, Congress convened to improve the U.S. government's capability to detect and deter future terrorist attacks against the United States (Bendix & Quirk, 2016; Boyle, 2008; Copeland, 2004; Ebenger, 2007; Young, 2011). The result was the USA PATRIOT Act of 2001, which was the unity of two bills (Kerr, 2003). The U.S. Senate passed the Uniting and Strengthening America Act by a 96 to 1 vote, and the U.S. House of Representatives approved the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act by a 337 to 79 vote (Kerr, 2003). The merged bill combined both titles to create the USA PATRIOT Act of 2001 and passed both chambers of Congress and was signed by President George W. Bush on October 26, 2001 (Kerr, 2003).

The USA PATRIOT Act of 2001, or HR 3162, amended the Electronic Communications Privacy Act, the Communications Act, the Foreign Intelligence Surveillance Act, and the Computer Fraud and Abuse Act (Ebenger, 2007). Prior to the USA PATRIOT Act of 2001, law enforcement was mostly reactive as authorities investigated incidents after an alleged crime occurred to establish probable cause and obtain access to sensitive data (Taylor, Fritsch, & Liederbach, 2015). Since the USA PATRIOT Act of 2001's passage, information sharing has improved among law enforcement agencies and the Intelligence Community (Berman, 2014); however, this improvement was made at the consequence of negatively impacting civil liberties

(Berman, 2016). Although the USA PATRIOT Act of 2001 enhanced information sharing and investigative capabilities in various ways, the most fundamental was the NSA Surveillance Program (Banks, 2009; Bendix & Quirk, 2016; Kerr, 2003).

NSA Surveillance Program under the USA PATRIOT Act of 2001. Section 215 of the USA PATRIOT Act of 2001 allowed the government to obtain tangible things pertinent to an ongoing investigation (Banks, 2016). The collection of tangible things was permissible so long as there were "reasonable grounds to believe that the tangible things sought [were] relevant to an authorized investigation" (Berman, 2016, p. 1201). Thus, section 215 was interpreted by the FISC and the NSA to authorize the bulk collection of metadata from telecommunications service providers (Berman, 2016).

The bulk collection of telephony metadata was approved several times by the FISC under the "business records provision of the Foreign Intelligence Surveillance Act [], 50 USC. § 1861, enacted as section 215 of the USA PATRIOT Act of 2001" (Obama Administration, 2013, p. 1). As a means for preservation, the metadata was collected in bulk from telecommunications service providers and stored within an extensive database controlled by the NSA so that it may be accessed when/if needed (Mukasey, 2013; Obama Administration, 2013). Reasons for the preservation was that several telecommunication companies were discarding metadata after a certain period due to routine business practices, therefore deeming the metadata inaccessible if that telecommunication company was subpoenaed (Mukasey, 2013).

Required via court order issued by the FISC, telecommunications service providers were compelled to provide the government with metadata related to telephone

calls made within the United States and between the United States and foreign countries (Obama Administration, 2013). The NSA queried and analyzed the metadata for counterterrorism purposes (Mukasey, 2013). Conducting a query for any purpose other than counterterrorism matters was not authorized (Obama Administration, 2013). The metadata obtained was limited to the telephone number that initiated the call, the telephone number that received the call, the date and time the call occurred, and the call duration (Mukasey, 2013; Obama Administration, 2013). The information obtained via this court order did not include the telephone call's content (Mukasey, 2013; Obama Administration, 2013; Yoo, 2014).

The method of query employed by the NSA was complex. Before beginning the search, a telephone number (i.e., identifier) associated with a foreign terrorist organization had to be identified and approved by the FISC (Obama Administration, 2013). To obtain approval, there had to be a "reasonable, articulable suspicion that a [] identifier used to query the data for foreign intelligence purposes [was] associated with a particular foreign terrorist organization" (Obama Administration, 2013, p. 3). Once approved, the search could be conducted, and the identifier initially used for approval became the "seed identifier" (Obama Administration, 2013, p. 3-4). Information obtained in response to the query included the telephone numbers and associated telephony metadata that were in contact with the seed identifier (Mukasey, 2013; Obama Administration, 2013). Additionally, the NSA could identify a second or third-tier (i.e., hop) contact associated with the seed identifier (Mukasey, 2013). The first "hop" referred to the telephone number directly associated with the seed identifier, the second "hop"

referred to the telephone number directly associated with the first "hop," and the third "hop" was the telephone number directly associated with the second "hop" (Mukasey, 2013; Obama Administration, 2013). The cross triangulation of metadata enabled NSA analysts to locate telephone numbers associated with terrorist activity (Obama Administration, 2013).

Advocates. Mukasey (2013) and the Obama Administration (2013) argued section 215 and the NSA Surveillance Program was a valuable counterterrorism tool that the US government used to prevent terrorist attacks. Mukasey (2015) stressed the program was "virtually the only way that the government [could] look outward from the United States to see what's coming in from overseas" (p. 199). The cross triangulation of telephony metadata allowed the government to "determine whether known or suspected terrorists contacted individuals within the United States (Obama Administration, 2013, p. 3).

The ability to leverage this analytical capability in order to identify suspected terrorist communications was beneficial in detecting terrorist operatives who solely operated domestically, operated domestically and placed calls outside the United States, or operated abroad and placed domestic calls (Mukasey, 2015). The Obama Administration (2013) claimed the NSA Surveillance Program "help[ed] close critical intelligence gaps that were highlighted by the September 11, 2001 attacks" (p. 3). Additionally, without the large pool of telephony metadata to draw from, this program would have mostly been ineffective as the numbers (e.g., hops) are not known in advance to the authorized queries (Obama Administration, 2013) – this was helpful as service

providers would purge the metadata due to routine business practices and thus render the metadata irretrievable (Mukasey, 2015).

The Obama Administration (2013) claimed oversight for the program was rigorously monitored by the Department of Justice, the FISC, Congress, and the Office of the Director of National Intelligence. Mukasey (2015) also stressed the program had strict measures in place; first, it was only accessible to approximately two dozen people; second, the program must only have been accessed for counterterrorism purposes; and third, the program was overseen by the intelligence committees and judiciary committees from both houses of Congress, as well as the FISC which ensured all queries and metadata were handled correctly.

A threshold of reasonable, articulable suspicion had to be identified by one of the 22 designated NSA officials in order for the seed identifier to be established and the request to search authorized (Obama Administration, 2013). During internal oversight, if a compliance violation was found, the matter would be reported to the FISC, which would implement remedial action (Obama Administration, 2013). On at least one occasion, the NSA had searched beyond the scope of what was permissible, and this excessive search was brought before the FISC; the judge who heard this instance criticized the NSA but nonetheless reauthorized the program (Mukasey, 2015, p. 198).

The bulk collection of telephony metadata records was compliant with section 215, had been authorized 34 times by 14 different judges of the FISC, and arguably did not violate the Fourth Amendment to the United States Constitution (Mukasey, 2013; Obama Administration, 2013; Yoo, 2014). Particularly concerning the Fourth

Amendment, Yoo (2014) and the Obama Administration (2013) leveraged the *third-party doctrine* as a defense when they argued the NSA Surveillance Program did not violate one's *reasonable expectation of privacy*. The third-party doctrine was a Supreme Court privacy precedent that declared one could not have a reasonable expectation of privacy for information voluntarily provided to third parties or telecommunication service providers (Thompson, 2014). Lastly, the Obama Administration (2013) and Mukasey (2015) declared the NSA Surveillance Program was not in violation of the First and Fourth Amendment as the content was not collected – only metadata as an investigative/intelligence tool.

Critics. Berman (2016) argued that the bulk collection of telephony metadata was the most controversial program authorized by section 215 of the USA PATRIOT Act of 2001. The bulk metadata collection program was subject to scrutiny by civil liberty organizations, politicians, and academics (Berman, 2016; McGowan, 2014). The NSA Surveillance Program was controversial because critics questioned the constitutionality of the program regarding the mass collection of metadata on US citizens (Donohue, 2014; Berman, 2016). The premise for the bulk collection program was primarily indicative of the judicial ruling in *Smith v. Maryland*, in which the Supreme Court found that one does not have a reasonable expectation of privacy for information voluntarily relinquished to third parties (Berman, 2016; Donohue, 2014; Liu et al., 2015; Rapisarda, 2015; Yoo, 2014). However, several scholars raised concern to the applicability of the aforementioned jurisprudential justification as the basis by claiming the bulk metadata

collection program operated within constitutional parameters (Donohue, 2014; Liu et al., 2015; Thompson, 2014).

After reviewing the literature, it appeared there are four primary concerns for the third-party doctrine and, therefore, the justification for the NSA Surveillance Program. The first concern is that privacy is not all lost when disclosed to another organization or person (Thompson, 2014). Thompson (2014) suggested it is not plausible that any information relinquished to a controlled environment (i.e., third party) could subsequently be released to anyone for any reason. The second concern is information obtained by third parties is not voluntarily relinquished by the individual (Shamsi & Abdo, 2011; Thompson, 2014). Shamsi & Abdo (2011) argued that, due to technological advancements, people routinely engage in cyber and digital communications in order to maintain pace with the developing world; thus, specific information that may be revealed within the metadata is practically unavoidable. The third concern is that the third-party doctrine lacks a comprehensive analysis and is antiquated (Rapisarda, 2015; Shamsi & Abdo, 2011; Thompson, 2014). Thompson (2014) found that the judiciary should not claim a reasonable expectation of privacy test without a comprehensive study. The fourth concern is that the third-party doctrine fosters a climate of distrust among the polity, and such distrust may manifest itself toward degrading a free society (Thompson, 2014).

The *Smith v. Maryland* case that established the grounds by which the third-party doctrine was established was also questioned (Donohue, 2014; Liu et al., 2015; Rapisarda, 2015; Thompson, 2014). In *Smith v. Maryland*, law enforcement had reasonable suspicion that the subject for data collection was involved in criminal activity,

unlike the mass collection of bulk metadata from every U.S. citizen (Donohue, 2014). Additionally, the metadata obtained by the NSA was more detailed and differed from that of the *Smith v. Maryland* case that occurred in 1976 (Rapisarda, 2015; Thompson, 2014; Donohue, 2014). For example, several technological advancements such as cellular devices and Internet communications were available during the NSA Surveillance Program that was not available in 1976 (Galicki, 2015; Rapisarda, 2015; Thompson, 2014), and the NSA programs collected metadata on hundreds of millions of people, whereas the *Smith v. Maryland* case was restricted in the duration of metadata collection and the target for surveillance (Donohue, 2014; Rapisarda, 2015;). Thus, in aggregate and the long-term collection of bulk metadata, big data analytics (Reilly, 2015) could be applied through the NSA Surveillance Program to determine lifestyle patterns and behavioral analysis (Donohue, 2014; Galicki, 2015; Liu et al., 2015;) – this is also known as the mosaic theory (Jaffer, 2010; Pozen, 2005).

USA FREEDOM Act of 2015

After the unauthorized disclosure of the NSA Surveillance Program in June 2013, U.S. intelligence/surveillance became the topic of interest for public and political discourse, which began to erode the public's trust in the U.S. government and confidence in their electronic communications (Berman, 2016; Casarez, 2016;). Shortly after the NSA Surveillance Program disclosure in June 2013, Congressman Sensenbrenner introduced the USA FREEDOM Act of 2015 later that fall along with support from 152 cosponsors, privacy groups, and technology companies (Forsyth, 2015). The U.S. House passed the USA FREEDOM Act of 2015 by a 338 to 88 vote, and it passed the U.S.

Senate by a 67 to 32 vote (HR 2048, n.d.). On June 2, 2015, President Barrack Obama signed the USA FREEDOM Act of 2015 (Stransky, 2015) and Casarez (2016) argued that the USA FREEDOM Act of 2015 was the "most significant surveillance reform in decades" (p. 2).

In addition to changes regarding the NSA Surveillance Program, the USA FREEDOM Act of 2015 provided greater oversight for the FISC as well as an expertise *amicus curiae* on matters concerning civil liberties and various advanced technologies (Berman, 2016). Also, as an effort to deter support for terrorist organizations, the maximum sentence for providing material support to terrorism increased from 15 years to 20 years (HR 2048, n.d.).

Regarding alterations to the NSA Surveillance Program, the Judiciary Committee (2015) surmised that the USA FREEDOM Act of 2015 reformed intelligence-gathering programs in five ways; (a) ended bulk collection of data, (b) prevented government overreach, (c) strengthened protection for civil liberties, (d) increased government transparency, and (e) reinforced national security. Although the USA FREEDOM Act of 2015 made a few notable changes that superseded the USA PATRIOT Act of 2001, the end of the NSA Surveillance Program as it functioned under section 215 of the USA PATRIOT Act of 2001 was the most significant (Berman, 2016). Therefore, this subsection will focus on how the USA FREEDOM Act of 2015 altered the NSA Surveillance Program.

NSA Surveillance Program under the USA FREEDOM Act of 2015. The USA FREEDOM Act of 2015 ended the bulk collection of metadata (Forsyth, 2015; Stransky,

2015), which was essentially the cornerstone of the NSA Surveillance Program. Under the USA FREEDOM Act of 2015, the U.S. government may no longer collect bulk telephonic metadata from a broad region (e.g., zip or area code) within the United States, limiting the collection to the greatest extent reasonably practicable (HR 2048, n.d.) by incorporating a "specific selection term" to acquire data (Forsyth, 2015). The specific selection term must be "used to limit, to the greatest extent reasonably practicable, the volume of tangible things sought consistent with the purpose for seeking the tangible things" (Forsyth, 2015, p. 1337).

Requiring greater specificity, the USA FREEDOM Act of 2015 defined a specific search as identifying a person, account, address (physical or electronic), or personal device (HR 2048, n.d.). Additionally, the government must show, (a) reasonable grounds to believe that the metadata sought is relevant to protect against international terrorism and (b) reasonable, articulable suspicion that the metadata is linked with a foreign power (HR 2048, n.d.). Furthermore, the NSA Surveillance Program was restricted to collecting metadata from up to "two hops" concerning a suspect rather than three hops as it were under the USA PATRIOT Act of 2001, be it the government has reasonable suspicion that a nexus exists to link the suspect to international terrorism (Forsyth, 2015).

USA FREEDOM Act of 2015 controversy. Former President Barack Obama and former FBI Director James Comey were advocates for the elimination of bulk metadata (FBI, 2014; The White House, 2015;). Although Obama and Comey do not explicitly mention that the bulk metadata collection under the NSA Surveillance Program was not beneficial to the intelligence collection apparatus, they did, however, emphasize

the protection of civil liberties and greater government transparency (FBI, 2014; The White House, 2015). However, it is worth noting that the Obama Administration (2013) initially defended the NSA Surveillance Program and argued its legitimacy, constitutionality, and legality.

Former NSA Director Michael Rogers expressed concern that the elimination of bulk metadata collection would adversely affect the NSA's ability to detect imminent terrorist threats (NSA, 2015). Rogers confirmed that ending bulk collection would diminish the NSA's operational aptitude and that there was no replacement for the benefit of bulk metadata collection (NSA, 2015). Supporting Rogers' position on bulk metadata collection, Mukasey (2015) and Yoo (2014) argued that the NSA Surveillance Program was a vital tool for the Intelligence Community that was legal and constitutional.

Summary of Literature Review

Indeed, the NSA Surveillance Program's application of collecting bulk metadata on U.S. citizens from telephony service providers was controversial. The controversiality lay within the appropriate balance of civil liberties (e.g., one's reasonable expectation of privacy) and national security or the greater good (Mukasey, 2015). Congress (Forsyth, 2015) and several legal scholars argued the NSA Surveillance Program needed to be restricted (Berman, 2016; Donohue, 2014), whereas executives of the intelligence community claimed the collection of bulk metadata was beneficial to national security (Mukasey, 2013; NSA, 2015; Obama Administration, 2013; Yoo, 2014). The collection of bulk metadata on U.S. citizens was controversial, lawful, and constitutional (Mukasey, 2013; NSA, 2015; Obama Administration, 2013; Yoo, 2014); however, the majority of

congressional members and the Obama Administration acknowledged that the bulk metadata program was too powerful and that the scales of civil liberty and national security were not appropriately balanced (FBI, 2014; Forsyth, 2015; The White House, 2015), thereby resulting in the USA FREEDOM Act of 2015.

Several studies considered the NSA Surveillance Program's constitutionality and its legality under section 215 of the USA PATRIOT Act of 2001. Moreover, many legal scholars examined case law and applicable judicial decisions regarding the third-party doctrine and one's reasonable expectation of privacy regarding the mass collection of metadata on U.S. citizens. However, although copious amounts of research were conducted concerning the appropriate balance for civil liberties and national security, it appears much remains unknown regarding this topic.

Conclusion

This chapter covered the NSA Surveillance Program, surveillance authorities that governed the collection of bulk metadata, and various judicial cases regarding one's reasonable expectation of privacy and the third-party doctrine. Additionally, this chapter included an overview of the domestic security dilemma and the NPF theoretical framework. The topics introduced in this chapter were fundamentally important to understand while applying the NPF to assess the House Judiciary Committee hearing's narrative climate analytically. Understanding the variables associated with the NSA Surveillance Program is necessary as they were discussed during the House Judiciary Committee congressional hearing. The research method is described thoroughly in chapter 3.

Chapter 3: Research Method

The purpose of this qualitative narrative case study was to describe how members of the House Judiciary Committee may have used rhetorical speech during the congressional hearing held on July 17, 2013, about the NSA Surveillance Program. This study's results may lead to identifying how members of the House Judiciary Committee used rhetorical speech to prohibit the NSA Surveillance Program. This chapter will expand upon the research design and rationale, the role of the researcher, and the methodology. Additionally, this chapter will address issues of trustworthiness and ways they are mitigated.

Research Design and Rationale

The central research question was:

RQ: How, if at all, did members of the House Committee on the Judiciary use narrative characters during the July 17, 2013, congressional hearing on the NSA Surveillance Program?

Central Concept

The domestic security dilemma is the central concept that drove this research. Field (2017) described this concept as an ebb and flow of political support for counterterrorism legislation that renders the United States ineffective for combating and defending against terrorism. After a terrorist attack, political support is initially high for counterterrorism legislation/programs but, as time progresses and fear of a looming terrorist attack subsides, the political support for the same programs enacted as a consequence of the attack is low (Field, 2017). The NSA Surveillance Program is one

example of the ebb and flow of political support for counterterrorism programs (Field, 2017; Forsyth, 2015; Mukasey, 2015; Oversight of the Foreign Intelligence Surveillance Act, 2019; Stransky, 2015;). Field (2017), Shanahan et al. (2018), and Weible and Sabatier (2018) observed that rhetorical speech used by legislators influences the outcome for legislation. Thus, this research collected and analyzed the congressional hearing transcript to identify if members of the House Judiciary Committee used rhetorical speech during the NSA Surveillance Program discussion. It is important to understand how policymakers used rhetorical speech, if at all, in order to describe how rhetorical speech may influence counterterrorism legislation and consequently prohibit beneficial counterterrorism programs. Rhetorical speech is the use of narrative characters (e.g., hero, villain) that may adversely affect rational judgment and policy decisions (Field, 2017; Jackson, 2005; Pilecki, 2017; Weible & Sabatier, 2018). Policymakers may use rhetorical speech to frame another individual, organization, or polity as the villain or hero to advantageously situate a preconceived policy agenda (Shanahan et al., 2018; Weible & Sabatier, 2018). The use of narrative characters is discussed in depth later in this chapter.

Research Design

The research design I chose for this dissertation was a dyadic qualitative narrative inquiry and case study approach. The selection of two approaches for this qualitative research was based on the fact that this dissertation entailed both elements for a case study as well as narrative inquiry. Though this research focused on a defined set of parameters bounded by time and centered on a political subsystem (i.e., congressional

hearing), the data analysis phase situated on the congressional hearing transcript. Implementing the coupled design that supports this study's principles fosters a climate of inclusion, which enables the design to best answer the research question.

Qualitative analysis is imperative for social progress, and in fact, several colonized nations relied on “human disciplines, especially sociology and anthropology, to produce knowledge about strange and foreign worlds” (Denzin & Lincoln, 2013, p. 1). Qualitative research has no theory or paradigm of its own and is rather difficult to clearly define (Denzin & Lincoln, 2013). Ravitch and Carl (2016) broadly defined qualitative research as a “methodological pursuit of understanding the ways that people see, view, approach, and experience the world and make meaning of their experiences as well as specific phenomena within it” (p. 7). Erickson (2011) defined qualitative inquiry as a means to discover “meaning-relevant kinds of things in the world” (p. 43) and describe the phenomena through narrative reporting. Denzin and Lincoln (2013) described qualitative review as a

> situated activity that locates the observer in the world. It consists of a set of interpretive, material practices that make the world visible. These practices transform the world. They turn the world into a series of representations, including field notes, interviews, conversations, photographs, recordings, and memos to the self. At this level, qualitative research involves an interpretive, naturalistic approach to the world. This means that qualitative researchers study things in their natural settings, attempting to make sense of, or interpret, phenomena in terms of the meanings people bring to them. (p. 4)

To combine these broad definitions of qualitative research, I identified qualitative study as a means to describe meaningful phenomena that are explored by adopting qualitative methods and describing the researcher's understanding and interpretation through narration.

Although several definitions of qualitative research exist, the methodological intent remains the same, to obtain a comprehensive understanding of a contextual phenomenon through a subjective world with no "goal of finding an objective or immutable truth" (Ravitch & Carl, 2016, p. 9). The method of analysis and the central research question for this research design aligned with the qualitative research methodology. Thus, qualitative research best supported this study because in this research I sought to understand how policymakers may have used rhetorical speech during a congressional hearing. Furthermore, for this research I used qualitative methods to describe how rhetorical speech may consequently prohibit beneficial counterterrorism programs. Therefore, the rationale for choosing a qualitative methodology was that it was most appropriate as the scope of this research falls within its purview.

Narrative inquiry. Though scholars disagree on roots and precise description, narrative inquiry could have begun in the early 20th Century and had roots in organizational studies, sociology, occupational science, and cognitive science, as well as realist, modernist, postmodern, and constructionist strands (Noffke &Somekh, 2009). This method is used to identify and describe the role narrative plays in a phenomenon (Ravitch & Carl, 2016). Narrative inquiry can also be paired with other qualitative approaches, such as a case study (Lichtman, 2014). Narrative inquiry extracts data from

several sources such as stories, journals, letters, conversations, interviews, pictures, litigation, and legislation (Ravitch & Carl, 2016). Thus, the rationale for choosing narrative inquiry aligned with this study's research question as the nexus of this research was gathering data for the purpose of analyzing narrative.

Case study. Bounded by time, case studies describe real-life events that focus on an individual, organization, event, or policy, among others (Rudestam & Newton, 2015). Case studies are frequently used in the public administration field to understand and evaluate phenomena (Rudestam & Newton, 2015). Burkholder, Cox, and Crawford (2016) posited the benefit of using a case study approach is the ability to confine the study within a specific set of parameters to prevent the research from "expanding beyond [its] original intent" (p. 228) and to observe/compare restricted data to obtain an in-depth analysis. Therefore, I selected the case study method because this research focuses on one congressional hearing that may have led toward prohibiting a counterterrorism program through legislation.

Quantitative research is grounded in hypothesis-testing through the application of mathematical theory and scientific operation (Martin & Bridgmon, 2012). I did not select quantitative analysis as for this study I did not seek to conduct a statistical analysis of narrative characters that may exist within the congressional hearing transcript. Quantitative research would not have answered this study's research question, nor would it contribute to filling the research gap this study was intended to address. However, taking a qualitative approach that describes how rhetorical speech may have prohibited

the NSA Surveillance Program best answers this study's research question and contributes to filling the research gap.

Role of the Researcher

Ramos (1989) identified two problems that may negatively affect the quality of qualitative studies and compromise ethics: (a) relationship between data and researcher, and (b) researcher bias. Taking into consideration the breadth of means in which qualitative review is conducted regarding the collection and analysis of empirical data, the scholar-practitioner must consider a position apropos the subject matter (Karagiozis, 2018; Ravitch & Carl, 2016). I was the observer and participant who collected and analyzed the transcript from a congressional hearing. It behooves the researcher who is the observer and participant to adopt the relational research role, which critically examines relational subtleties between scholar-practitioner and participant(s), as well as experiences amongst participants regarding the core of the study (Ravitch & Carl, 2016). Although there was no direct interaction between the participants and me in this analysis and therefore no professional relationship with the participants, there existed a direct interaction between me and the content because I analyzed the congressional transcript to interpret the meaning to identify if narrative characters exist. However, I adhered to relational research ideologies, which ensure the researcher is open to change opinions, research methods, and other critical elements that may alter the study (Ravitch & Carl, 2016).

Although I acknowledge that I am a United States citizen and, therefore, am affected by U.S. policy, I did not possess strong biases regarding the outcome of this

study. Instead, I understood the importance of counterterrorism programs as well as the necessity for upholding civil liberties as outlined in the U.S. Constitution. It would be my hope that if members of Congress utilized rhetorical speech at the congressional hearing on the NSA Surveillance Program, the rhetorical speech would be exposed in order to increase understanding of the use of narrative characters that may prohibit counterterrorism programs. I did not strive to obtain the answer to balancing civil liberties and national security matters. Instead, I intended to contribute and further expand upon the existing body of knowledge regarding the domestic security dilemma.

To mitigate and manage biases, I aligned this study with the four key pillars as outlined by Ravitch and Carl (2016): (a) criticality, (b) reflexivity, (c) collaboration, and (d) rigor. *Criticality* considers the researcher's positionality among the theoretical, conceptual, and methodological levels of the study (Ravitch & Carl, 2016). *Reflexivity* is the conscious assessment of the researcher's identity, influence, positionality, and subjectivities in relation to the research (Ravitch & Carl, 2016; Thurairajah, 2019). *Collaboration* is the fundamentally valuable means of challenging the researcher's biases or elements of the research that the author may have taken for granted or excluded (Ravitch and Carl, 2016; Ravitch & Riggan, 2012; Rule, 2011). Ravitch and Carl (2016) spoke to the importance of *rigor* when they argued the "rigorous research process will result in more trustworthy findings" (p. 17). I maintained rigor, collaboration, reflexivity, and criticality throughout this study.

Methodology

Participant Selection Logic

This narrative case study used the transcript from one congressional hearing as data. The data consisted of the words spoken by members of the House Judiciary Committee per the transcript in order to identify if narrative characters existed within the political discourse of that one hearing. Only the hearing on July 17, 2013, about the NSA Surveillance Program by the House Committee on the Judiciary was considered as data for this study. The House Committee on the Judiciary was chosen due to the committee's direct oversight on counterterrorism matters and the fact that Representative Sensenbrenner, a member of the committee, sponsored the USA FREEDOM Act of 2015 and its predecessor, the USA PATRIOT Act of 2001 (Forsyth, 2015). The hearing on July 17, 2013, was considered for this study as it was the first House Judiciary Committee hearing on the NSA Surveillance Program since the program’s unauthorized disclosure in June 2013 (Government Publishing Office, n.d.). The selected congressional hearing was obtained through the Government Publishing Office website. The Government Publishing Office (n.d.) is a federal agency within the legislative branch that provides public access to official publications from all three federal government branches.

Instrumentation & Data Collection

As previously mentioned, the historical congressional transcript was used as data for this study. I obtained the congressional transcript from the Government Publishing Office website. The Government Publishing Office (n.d.) is a reputable source provided

by the government that offers services such as providing congressional transcripts to the public. The data collection phase was relatively quick as the congressional hearing transcript was already accessible online. Should the Government Publishing Office not have had the congressional hearing transcript within its archives, then I would have contacted the House Judiciary Committee directly to request a copy of the transcript. Should the committee not have able to provide a copy of the transcript, then I would have submitted a Freedom of Information Act request requiring the House Judiciary Committee to provide the document. Lastly, only transcriptional format was considered as data, thus excluding audiovisual versions of the congressional hearing. As this is an independent study, respectively, only I collected the data.

Data Analysis

Weible et al. (2016) argued, "A fundamental challenge in understanding policy narratives is the inconsistency and lack of precision in how policy narratives, and their constitutive elements, are defined" (p. 420). To ensure replicability and transparency, the data analysis method for this research closely aligned with the analysis paradigm employed by Weible et al. (2016). This current research incorporated the NPF's meso-level methodology to evaluate the use of narrative characters at the political subsystem level (e.g., congressional committee). At the meso-level, the NPF employs two main features for conducting qualitative research; content analysis and network analysis (Shanahan et al., 2018). However, this research only utilized content anlaysis.

Content analysis, the most frequently utilized by NPF scholars and determined "a priori of the empirical material" (Weible et al., 2016, p. 426), is used to analyze and

identify policy narratives (Shanahan et al.,2018). Shanahan et al. (2018) defined policy narratives as being comprised of narrative elements, which consist of the setting, *characters*, plot, moral of the story, belief systems, and strategies. However, this study only considered one substratum of the policy narrative construct, the characters (e.g., heroes and villains). Since I independently conducted this rigorous study, it was not feasible nor practical to analyze all or additional narrative elements as this would have required a research team. The analysis of characters is described more thoroughly below.

Animate objects may adopt the role of a character, whereas inanimate objects or anthropomorphized nouns may not (Weible et al., 2016). Animate characters are comprised of one of two characters (Weible et al., 2016). The first character, heroes, are individuals/coalitions that solve or attempt to solve a problem (Weible et al., 2016). Villains, the second character, are individuals/coalitions "who cause or attempt to make the problem worse" (Weible et al., 2016, p. 423). For example, a policymaker may speak to the government protecting its citizenry from terrorist attacks. This rhetorical speech would situate government as the perceived hero and terrorist as the villain. Alternatively, a policymaker may speak to the government infringing on the civil liberties of its citizenry. This rhetorical speech would situate government as the villain. Thus, the narrative character (e.g., hero or villain) is predicated on the policymaker's rhetorical speech. Therefore, content analysis is solely grounded in the policymaker's rhetorical speech and not whether the researcher agrees with what is said.

The qualitative software NVivo 12 Plus was utilized to store and analyze the congressional hearing transcript about NSA Surveillance Program. Every narrative

character found within the transcript was categorized based on the rhetorical speech. The data was then partitioned into themes to describe how members of the House Judiciary Committee may have used rhetorical speech during the congressional hearing on the NSA Surveillance Program.

Trustworthiness

It is accurate to mention that, regardless of any profound findings, if I reveal untrustworthy results, then my efforts are void. Validity is an "active methodological process, a central value of qualitative research, and a research goal" (Ravitch & Carl, 2016, p. 185). To ensure qualitative validity, I ensured findings were congruent with credibility, transferability, dependability, and confirmability (Shenton, 2004). This section defines the aforementioned themes and how I maintained each value throughout the duration of this research.

Within the confines of this study, *credibility* is ensured by prudent examination of the theoretical framework, literature review, data analysis, and self-reflection of the researcher (Ravitch & Carl, 2016; Shenton, 2004). Synonymous with internal validity (Shenton, 2004), credibility is my ability to synthesize all complexities of the study and the means to deal with matters not easily explained (Ravitch & Carl, 2016). Credibility maintains that methods and findings are inseparable, and there is no checklist (nor should there be) for achieving validity; however, there exist methods for execution when striving to achieve validity (Ravitch & Carl, 2016). Therefore, I sought complexity in this research design, authenticity in data selection and saturation, alignment with research approach and research question, understanding and engagement with patterns in data,

challenged assumptions and biases, and synthesis of findings. This chapter further contributes to the authentic research methodologies and transparency, thereby fostering credibility

Transferability is implemented as the method in which data is collected, the number of data sources analyzed, and how the data is aggregated (Ravitch & Carl, 2016). The intent of qualitative research is "not to produce true statements that can be generalized to other people or settings but rather to develop descriptive, context-relevant statements" (Ravitch & Carl, 2016, p. 189). With transferring to the broader context in mind, transferability maintains richness in context-specific material in order for the audience (readers and researchers) to make comparisons to various contexts (Ravitch & Carl, 2016). Similar to its counterpart, external validity, transferability entails that I learn how and to what degree the findings have applicability in other settings/contexts (Shenton, 2004). To achieve transferability, I sought a rich description of the contextual factors that frame the study, authenticity in data interpretation, and overall clarity.

Dependability is synonymous with stability, where dependability is the core constructs and concepts of the study (Ravitch & Carl, 2016). Essential for stability, dependability is where another researcher discovers the same findings at the end of a study where s/he applied the same methods to the same data in the same context (Shenton, 2004). Dependability safeguards the methods in which the data was gathered, codified, and appraised (Ravitch & Carl, 2016). Articulating the triangulation of methods for data collection and rationale for analysis based on research questions communicates the level of dependability to the researcher's audience (Ravitch & Carl, 2016). Thus, I

sought clarity in why the research method was chosen and simplicity in mapping the research design to the research question. Additionally, I sought to apply similar analytical methods previous NPF studies have used to ensure dependability/reliability among policy narrative analysis (Weible et al., 2016).

Confirmability, equivalent to its quantitative counterpart for the concept of objectivity, adheres to the notion that "qualitative researchers do not claim to be objective" (Ravitch & Carl, 2016, p. 189) and, in fact, researcher's biases are inevitable (Shenton, 2004). Qualitative researchers must acknowledge that bias is unavoidable and exists intrinsically; however, it is essential to maintain a neutral posture (to the best of one's ability) and posit that findings are free from researcher bias (Shenton, 2004). Therefore, to obtain confirmability, I adhered to structured reflexivity processes and triangulation strategies (Ravitch & Carl, 2016; Shenton, 2004), such as exploring how biases may infringe upon the data analysis phase and then mitigating the effects of bias to the greatest extent possible.

Ethical Procedures

In order to adhere to ethical procedures that govern doctoral research, I needed to obtain approval from the Walden University Institutional Review Board (IRB) and obtain the Collaborative Institutional Training Initiative (CITI) doctoral student researchers certification. I had to obtain IRB approval before advancing to data collection and analysis. Although the overall ethical risk for this research was minimal, as the data entailed documentation that was widely available to the general public and was not confidential, classified, or sensitive; nonetheless, I completed the appropriate

documentation. My IRB application was approved on September 22, 2020, and the approval number is 09-22-20-0670414. My CITI certification is available in Appendix D.

Summary

This chapter outlined the plan for the study and described its methodology. The concept of the study centered on the NSA Surveillance Program and the House Judiciary Committee hearing on July 17, 2013. The centrality of this research sought to answer the research question: How, if at all, did members of the House Committee on the Judiciary use rhetorical speech during the congressional hearing held on July 17, 2013, that pertained to the NSA Surveillance Program? This methodology, to include data collection and analysis, aligned with answering the research question and maintains validity while mitigating ethical risks. Additionally, issues of trustworthiness (i.e., credibility, transferability, dependability, and confirmability) were discussed, and approaches/methods on how they were mitigated were described. Lastly, after IRB approval, I did not have issues of trustworthiness during the data collection and analysis phase.

Chapter 4: Results

The purpose of this qualitative narrative case study was to describe how members of the House Judiciary Committee may have used rhetorical speech during the congressional hearing held on July 17, 2013, about the NSA Surveillance Program. The results of this study may lead to identifying how members of the House Judiciary Committee used rhetorical speech to prohibit the NSA Surveillance Program. The central research question was:

> RQ: How, if at all, did members of the House Committee on the Judiciary use narrative characters during the July 17, 2013, congressional hearing on the NSA Surveillance Program?

This chapter covers the research setting, demographics, data collection, data analysis, evidence of trustworthiness, and the results of the study. I conclude with a summary to highlight and recapture the key themes that emerged as a result of the analysis.

Research Setting

This research was a historical analysis of rhetorical speech uttered by members of the House Judiciary Committee during the hearing on July 17, 2013, about the NSA Surveillance Program. Therefore, because this study took place after the fact, the participants (i.e., members of the House Judiciary Committee) were not influenced during the study. However, it is worth noting that the members of the House Judiciary Committee may have been influenced during the congressional hearing by rhetorical speech that adversely affected behavioral and rational thought proceeding from the unauthorized disclosure of the NSA Surveillance Program (Field; 2017; Perliger, 2012).

Additionally, Field (2017) contended that as time progresses, fear of a looming terrorist attack subsides, and therefore public support for counterterrorism legislation declines. Thus, these factors (i.e., rhetorical speech and adversely affected behavioral and rational thought) may have affected the members at the congressional hearing; however, no influence occurred at the time of analysis that would impact the data analysis or interpretation of results.

Demographics

Considering the demographics and characteristics of the members who composed the House Judiciary Committee at the time of the hearing was outside the scope of this study. However, I compiled a list of the House Judiciary Committee members who attended the hearing on July 17, 2013. Demographics such as sex, gender, or party affiliation were not considered during the data analysis phase or data interpretation/results. The list below is to inform the reader which representatives were present during the congressional hearing.

Table 1

Representatives Present During Congressional Hearing

Name	State	Name	State
Goodlatte	Virgina	Conyers	Michigan
Sensenbrenner	Wisconsin	Nadler	New York
Coble	North Carolina	Scott	Virginia
Smith	Texas	Lofgren	California
Chabot	Ohio	Jackson Lee	Texas
Bachus	Alabama	Cohen	Tennessee
Forbes	Virginia	Johnson	Georgia
King	Iowa	Chu	California
Gohmert	Texas	Deutch	Florida
Poe	Texas	DelBene	Washington
Chaffetz	Utah	Garcia	Florida
Gowdy	South Carolina	Jeffries	New York
Labrador	Idaho		
Farenthold	Texas		
Holding	North Carolina		
Collins	Georgia		
DeSantis	Florida		

Data Collection

As previously mentioned, the historical House Judiciary Committee hearing that took place on July 17, 2013, was used as data for this study. I obtained the House Judiciary Committee hearing transcript from the Government Publishing Office website. Once collected, the data was uploaded into the NVivo 12 Plus software. There were no unusual circumstances that occurred while the data were being downloaded from the Government Publishing Office website or uploaded into NVivo 12 Plus. Thus, there were no variations in the data collection method as described in Chapter 3.

Data Analysis

This qualitative case study and narrative inquiry employed the NPF. Specifically, this data analysis used the content analysis method at the mesolevel unit of analysis (see Weible & Sabatier, 2018). I only analyzed the words spoken by members of the House Judiciary Committee, as indicated on the July 17, 2013, hearing transcript about the NSA Surveillance Program. To ensure replicability and transparency, the data analysis method for this research was closely aligned with the analysis paradigm employed by Weible et al. (2016). Weible et al. (2016) argued that content analysis is determined as “a priori of the empirical material" (p. 426). Therefore, the subcategories were characterized as a hero or villain prior to analysis.

The same definitions for the hero and villain were adhered to as described in Chapter 3. The first character, heroes, are individuals/coalitions who solve or attempt to solve a problem (Weible et al., 2016). Villains, the second character, are individuals/coalitions "who cause or attempt to make the problem worse" (Weible et al.,

2016, p. 423). Because the hero or villain must be an individual or coalition, the four members who testified before Congress were grouped into one alliance and were referred to as the "Coalition" during coding. The four members who testified were James Cole representing the U.S. Department of Justice, Robert S. Litt representing the Office of Director of National Intelligence, John C. Inglis representing the NSA, and Stephanie Douglas representing the Federal Bureau of Investigation (FBI) National Security Branch. Thus, the members who testified before Congress composed the Coalition and this Coalition was considered as a subcategory under the hero and villain partitions. The House Judiciary Committee members present during the hearing composed the "Congress" alliance; therefore, Congress was also considered as a subcategory under the hero and villain partitions.

Other considerations for possible hero/villain subcategories were: media, U.S. citizens, foreign citizens, and Edward Snowden. Edward Snowden was included as a possible character as it was presumed that Snowden would be referenced because he was the one who revealed the classified NSA Surveillance Program. The only category exclusive to the villain partition was the term "terrorists." The reason why terrorists were not included as a hero subcategory was due to the U.S. government's definition of the term. The FBI defined international terrorism as "violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations" (n.d.). Additionally, the FBI defined domestic terrorism as "violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social,

racial, or environmental nature" (n.d.). However, U.S. designated terrorist groups (e.g., Al-Qaeda) may be categorized as a hero or villain based on the content of the rhetorical speech and whether the content matched a hero or villain definition. If additional subcategories surfaced while analyzing the transcript, then additional subcategories were created under the hero and villain partition.

Once the hero and villain partitions were created and all subcategories were placed within their respective partition, I read the transcript in its entirety before coding the characters. Reading the entire transcript was necessary to obtain a comprehensive understanding of the content of the transcript to ensure greater familiarity with the content and accuracy with coding. After the initial read, I then reread the transcript to identify character references. If a passage in the transcript identified an individual/coalition that met the definition of a hero or villain, I copied that passage into the corresponding partition in the respective subcategory (e.g., Congress, Coalition, media, etc.). I reviewed the transcript several times, and the codes were also reviewed several times for refinement and to ensure only those passages which met the definition of a hero or villain were included.

Each passage from the transcript that met the hero/villain definition is displayed under the results section of this chapter. Under each excerpt, an explanation is provided to clarify how that specific excerpt met the hero/villain definition. Due to the nature of the dialogue in a congressional hearing, I had to make inferences predicated on previous statements the legislator made and also had to infer whom the legislator was addressing at

the time the statement was made. No inferences were made that were not grounded in the dialogue in the congressional hearing transcript.

Evidence of Trustworthiness

Credibility

The methods and findings of this study were inseparable. Although there is no checklist for ensuring credibility (Ravitch & Carl, 2016), the intent was to ensure that if another researcher were to conduct this exact study in the same fashion, the findings would remain the same. Credibility was achieved by the prudent examination of the theoretical framework, literature review, data analysis, and personal self-reflection (Ravitch & Carl, 2016; Shenton, 2004). Furthermore, I synthesized complexities from this study and the analysis that were not easily explained (see Ravitch & Carl, 2016). Lastly, I sought complexity in the research design, authenticity in data selection and saturation, alignment with research approach and research question, understanding and engagement with patterns in data, to challenge assumptions and biases, and synthesis of findings. There were no deviations/adjustments during the data collection and analysis to ensure credibility as described in Chapter 3.

Transferability

I sought a rich description of the contextual factors that framed this study, authenticity in data interpretation, and overall clarity. The method in which the data were collected, the amount of data analyzed, and how the data were aggregated is replicable in other settings (see Ravitch & Carl, 2016). Transferability was achieved as these findings have applicability in other settings/contexts (see Shenton, 2004). For example, a

researcher may apply the same methodology, research design, and mode of collection and analysis toward another congressional hearing related or unrelated to this study's topic. There were no deviations or adjustments during the data collection and analysis to ensure transferability as described in Chapter 3.

Dependability

Essentially, dependability is where another researcher discovers the same findings at the end of a study where the researcher applied the same methods to the same data in the same context (Shenton, 2004). The method for data collection and rationale for analysis based on the research question communicates the level of dependability for this study (Ravitch & Carl, 2016). The research question required a qualitative answer that could be best achieved through a dyadic narrative inquiry and case study approach. Though this research focused on a defined set of parameters bounded by time and centered on a political subsystem (i.e., congressional hearing), the data analysis phase situated itself on the congressional hearing transcript. Therefore, the selection of two approaches for this qualitative research was based on the fact that this dissertation entailed both elements for a case study as well as narrative inquiry. Implementing the coupled design that supported this study's principles fostered a climate of inclusion, which enabled the design to best answer the research question. Additionally, this study applied similar analytical methods previous NPF studies have used to ensure dependability among policy narrative analysis (Weible et al., 2016). There were no deviations/adjustments during the data collection and analysis to ensure dependability as described in Chapter 3.

Confirmability

Bias is inevitable (Shenton, 2004), and "qualitative researchers do not claim to be objective" (Ravitch & Carl, 2016, p. 189). Qualitative researchers must acknowledge that bias is unavoidable and exists intrinsically; however, it is essential to maintain a neutral posture and posit that findings are free from researcher bias (Shenton, 2004). I have acknowledged my bias, and I suspended my bias so that interference would not impede this study's rudiments. In addition to acknowledging my bias, I provided excerpts for each code from the congressional hearing transcript, and I explained how each excerpt aligned with the hero and villain characters. By displaying the data, the researcher is held accountable and unable to label an excerpt in a particular manner that is inconsistent with the corresponding character definition. Finally, there were no deviations/adjustments during the data collection and analysis to ensure confirmability as described in Chapter 3.

Study Results

Hero and villain excerpts are displayed below. The excerpts were divided into a hero subsection and a villain subsection. Excerpts that have a hero reference were placed under the hero subsection, and excerpts that have a villain reference were placed under the villain subsection. However, excerpts that have hero and villain references were placed under the hero subsection. Therefore, only excerpts that have a villain reference and do not have a hero reference were placed under the villain subsection. Additionally, I provided brackets within the excerpts to provide context to assist the reader. Since the entire transcript is not displayed in this chapter, the brackets assist the reader with understanding whom the congressional member was referring to at the time s/he was

speaking. For authenticity and dependability purposes, the data below were direct excerpts from the transcript; therefore, any grammatical errors present in the excerpts below were inherent within the transcript. Lastly, I synthesized these findings prior to this chapter's summary.

Hero Characters

Mr. Deutch stated:

> Now the PATRIOT Act was passed in response to the horrific attacks on 9/11, designed to bolster national security by expanding the investigative techniques used by the Government [Coalition] and law enforcement officials to hunt down suspected terrorists, something that we all agree is important. (Administration's Use of FISA Authorities, 2013, p. 53)

Mr. Deutch situated Congress and the Coalition as the hero and terrorist as the villain in this statement. The problem was the attacks on September 11, 2001, and Congress's attempt to solve the problem was passing the USA PATRIOT Act of 2001. Mr. Deutch did not explicitly mention terrorists as the entity that perpetrated the attacks on September 11, 2001; however, it is plausible to infer that is what Mr. Deutch meant given the context of his previous statements. Although Mr. Deutch did not explicitly mention Congress in his statement, it is reasonable to suggest that he meant Congress due to the fact that Congress is the entity that enacts law. Thus, through enacting the USA PATRIOT Act of 2001, national security became strengthened, and the investigative capabilities for the U.S. government (i.e., Coalition) expanded, thereby providing the opportunity to intercept terrorists. Similarly, Mr. Deutch did not explicitly mention the

Coalition; however, it is plausible to suggest that he was referring to it because he was addressing the Coalition during the hearing, and that is the function of the Coalition.

Ms. Lofgren stated:

> I was thinking back to September 11th, one of the worst days I have ever spent in the Congress, and remembering that that weekend, after the attack, that members of the White House, the intelligence community, Members of this Committee and our staff, sat right at that table. We sat around that table and worked together to craft the PATRIOT Act. And it is worth remembering that that original act was passed unanimously by the House Judiciary Committee, and it had the balance that we thought was important to protect the country, but also looking forward to protect the rights of Americans under the Constitution. (Administration's Use of FISA Authorities, 2013, p. 31)

Ms. Lofgren positioned Congress and the Coalition as the heroes in this passage. The Coalition was included in this passage as a hero since Ms. Lofgren identified the intelligence community as one of the entities that worked with Congress to craft the PATRIOT Act. Therefore, Ms. Lofgren contended that the PATRIOT Act was created as a joint effort by the Coalition and Congress to protect the country and protect constitutional rights.

Mr. Bachus stated:

> Let me start by saying I am satisfied, at least from what limited knowledge I have, that the motivation behind this was legitimate and necessary for our national security to start this process, establishment of a court. And that from your

> [Coalition] testimony you [Coalition] have not, apparently not abused individual rights, and you [Coalition] have been an effective tool for terrorism. (Administration's Use of FISA Authorities, 2013, p. 29)

It appeared Mr. Bachus attempted to situate the Coalition as the hero in this statement. It is reasonable to suggest that Mr. Bachus referred to the Coalition when this statement was made as he was addressing the Coalition and referring to the Coalition's testimony. Also, given the prior context of his statements, it is plausible to postulate that Mr. Bachus meant the Coalition used an effective tool for counterterrorism and that the tool was the NSA Surveillance Program. Additionally, it is reasonable to infer that Mr. Bachus was referring to the NSA Surveillance Program as the tool because that program was the topic for discussion and the chief matter in the Coalition's testimony. Also, Mr. Bachus stated that according to the Coalition's testimony, the Coalition had not abused individual rights. Thus, the Coalition used the NSA Surveillance Program to prevent or attempt to prevent a problem, terrorism.

Mr. Goodlatte stated, "However, Congress must ensure that the laws we have enacted are executed in a manner that is consistent with congressional intent and that *protects* [emphasis added] both our national security and our civil liberties" (Administration's Use of FISA Authorities, 2013, p. 3).

Mr. Goodlatte situated Congress as the hero in this statement. Mr. Goodlatte contended that Congress protects national security and civil liberties and thereby must enact laws to facilitate that endeavor. Thus, Congress solves or attempts to solve a problem by protecting national security and civil liberties through legislation.

Ms. Lofgren stated:

> But the concern is that the statute that we [Congress and Coalition] crafted so carefully may not be being adhered to as envisioned by us [Congress] and as reported to us [Congress]. And I just want to say this. I mean, yes, we have a system where there are checks and balances, but part of that is that the legislative branch needs to have understanding of what the executive branch and the judicial branch is doing, and we [Congress] can't do that without information. (Administration's Use of FISA Authorities, 2013, p. 31)

Ms. Lofgren situated Congress as the hero in this statement. While Ms. Lofgren was addressing the Coalition, she positioned Congress as attempting to fix a problem by obtaining information. Ms. Lofgren identified the potential problem as the Coalition not conducting operations as envisioned by Congress. Ms. Lofgren further explained that Congress could not fix the problem because they had received misinformation or that there may be a lack of information or both. Therefore, it was plausible to infer that Ms. Lofgren was arguing that if Congress can obtain more or accurate information, then Congress can fix the problem by redirecting the Coalition to operate in a manner that satisfies Congress.

Mr. Deutch stated:

> The American people have a right to know about this program and at the very least know that such a program is operating within our system of checks and balances. And I believe Congress has a constitutional obligation to *protect*[emphasis added] individual privacy rights, and I believe it is time to

> reexamine the PATRIOT Act, insert greater accountability into the FISA court, and ensure that our laws cannot be interpreted behind the backs of the American public. (Administration's Use of FISA Authorities, 2013, p. 52)

This statement provided by Mr. Deutch situated Congress as the hero. Mr. Deutch argued that Congress needs to protect privacy rights for the individual, and to do so, Congress must reexamine the PATRIOT Act. Thereby make greater accountability into the FISC and limit how the law may be interpreted. Thus, Congress is attempting to fix a problem by reexamining and changing the PATRIOT Act.

Mr. Nadler stated, "Ms. Martin, how can we—how can Congress solve the problem? We have a basic problem" (Administration's Use of FISA Authorities, 2013, p. 127)." Mr. Nadler situated Congress as the hero in this statement. Mr. Nadler positioned Congress as the hero by framing the question in a manner that lends to Congress possessing the ability to solve the problem. Although the problem is not explicitly mentioned, Mr. Nadler, however, expressed that there is indeed a problem. Therefore, the attempt is apparent by asking the question pertaining to how Congress can solve the problem.

Mr. Sensenbrenner stated:

> You know, I have been the author of the PATRIOT Act and the PATRIOT Act reauthorization of 2006. Mr. Conyers was correct in saying why the relevance standard was put in, and that was an attempt to limit what the intelligence community could be able to get pursuant to Section 215. (Administration's Use of FISA Authorities, 2013, p. 22)

Mr. Sensenbrenner situated Congress as the hero in this statement. Mr. Sensenbrenner argued that Congress created the relevance standard, which was an attempt to solve the problem by limiting the data the intelligence community would collect. Although Mr. Sensenbrenner was explicitly referring to himself in this passage, the hero was identified as Congress because Mr. Sensenbrenner was a member of Congress and was engaged in congressional duties.

Mr. Nadler stated:

> Now Mr. Snowden may have done a public service in giving some people standing by proving that they were harmed by this because anyone who is a Verizon subscriber arguably can now go into court and say that. How can we deal with these two problems that an Administration, any Administration can violate constitutional rights from here to kingdom come, subject to no court review because of either the state secrets doctrine or the standing problems because they don't admit what they are doing in the first place. It is secret. (Administration's Use of FISA Authorities, 2013, p. 127)

Mr. Nadler situated Edward Snowden as the hero in this statement. Mr. Nadler suggested that Snowden may have attempted to fix a problem by providing information pertaining to the NSA Surveillance Program. Mr. Nadler stated that there are two problems; the violation of constitutional rights and the doctrinal rights governing secrecy. Although Mr. Nadler did not explicitly mention the NSA Surveillance Program or that Snowden provided information, Mr. Nadler did, however, say that Snowden gave people standing by proving a problem. Moreover, it is reasonable to presume Mr. Nadler was referring to

the time that Snowden released information pertaining to the NSA Surveillance Program because that is how the people became privy to the fact that Verizon was sharing customer metadata with the government.

Mr. Holding stated:

> In a different professional capacity, I successfully used FISA warrants to investigate, disrupt, and prosecute terrorists and terrorist acts, and I can attest that not only are they effective, but there are very high burdens and hurdles to use FISA warrants. And they are significant. (Administration's Use of FISA Authorities, 2013, p. 54)

Mr. Holding situated himself as the hero in this statement and terrorists as the villain. Congress was not identified as the hero in this statement because Mr. Holding was referring to himself and the work he conducted while operating in a different official capacity apart from Congress. Mr. Holding identified that he used FISA warrants to prevent and prosecute terrorists. Terrorists and terrorist acts were identified as the problem in this statement based on the FBI's definition of domestic terrorists and foreign terrorists. Therefore, according to Mr. Holding, he prevented a problem from occurring and prosecuted those who caused a problem by using FISA warrants. The FISC was not identified as a hero in this statement as Mr. Holding was explicitly referring to the FISA warrants, which was not an individual or coalition and, therefore, does not meet the definition of a hero.

Villain Characters

Mr. Nadler stated:

> Let me ask the question. The fact—the fact that a secret court [FISC], unaccountable to public knowledge of what it is doing, for all practical purposes unaccountable to the Supreme Court, may join you [Coalition] in misusing or abusing the statute is of no comfort whatsoever. So to tell me that you [Coalition] go to the FISA court is irrelevant if the FISA court is doing the same abuse of the statute. (Administration's Use of FISA Authorities, 2013, p. 25)

Mr. Nadler framed the Coalition and the FISC as the villain in this statement due to the Coalition and the FISC abusing the statute. Thus, the Coalition was causing a problem by abusing the statute. It is reasonable to presume Mr. Nadler was referring to the Coalition as Mr. Nadler was addressing the Coalition at the time he made the statement.

Mr. Nadler also said:

> The problem, obviously, Mr. Cole, with what we are hearing from this panel and what we have heard generally about the relevant standard is that everything in the world is relevant. And that if we removed that word from the statute, you wouldn't consider or the FISA court wouldn't consider that it would affect your ability to collect metadata in any way whatsoever, which is to say you are disregarding the statute entirely. (Administration's Use of FISA Authorities, 2013, p. 23)

Mr. Nadler situated the Coalition and the FISC as the villains in this statement. Mr. Nadler stated that the problem is the Coalition and the FISC's disregard for the statute and thereby is operating outside the statute's bounds by including everything as relevant. Since Mr. Nadler was addressing Mr. Cole, it is reasonable to presume he was addressing

the Coalition. Furthermore, it is reasonable that Mr. Nadler was referring to the NSA Surveillance Program as this was the chief topic for this discussion and the fact that the relevant standard was included in the statute to limit the amount of metadata the NSA Surveillance Program collected.

Mr. Conyers stated:

> Now what we [Congress think we [Congress] have here is a situation in which if the Government [Coalition] cannot provide a clear public explanation for how its program [NSA Surveillance Program] is consistent with the statute, then it [NSA Surveillance Program] must stop collecting this information immediately. And so, this metadata problem to me has gotten quite far out of hand, even given the seriousness of the problems that surround it and created its need.
>
> (Administration's Use of FISA Authorities, 2013, p. 3)

Mr. Conyers situated the Coalition as the villain in this statement. Mr. Conyers argued that the problem is the metadata collection, and the potential problem is the Coalition's ability to describe how the NSA Surveillance Program was consistent with the USA PATRIOT Act. It is reasonable to suggest that Mr. Conyers was referring to the NSA Surveillance Program as that was the topic for discussion during this hearing and due to the fact that the NSA Surveillance Program collected and analyzed metadata. Additionally, it is plausible to infer that Mr. Conyers was referring to the Coalition when he explicitly mentioned government because Mr. Conyers was addressing the Coalition and needed an explanation from the Coalition as to how the NSA Surveillance Program was consistent with the statute. Lastly, Mr. Conyers affirmed the collection of metadata

(i.e., NSA Surveillance Program) is a problem in this statement, and the Coalition is causing this problem.

Mr. Conyers also said:

> But I maintain that the Fourth Amendment, to be free from unreasonable search and seizure, means that this metadata collected [NSA Surveillance Program] in such a super-aggregated fashion can amount to a Fourth Amendment violation before you do anything else. You [Coalition] have already violated the law, as far as I am concerned. And that is, in my view, the problem. (Administration's Use of FISA Authorities, 2013, p. 16)

Mr. Conyers positioned the Coalition as the villain in this statement by asserting that the Coalition caused the problem by using the NSA Surveillance Program to violate the law. It is reasonable to suggest Mr. Conyers was referring to the Coalition at the time he made this statement. Additionally, based on previous statements in the transcript, it is reasonable to infer the Coalition used the NSA Surveillance Program to collect the metadata, which was the chief topic for this discussion.

Mr. Sensenbrenner stated:

> But, Mr. Cole, with all due respect, the letter that I got from the department that you are the number-two person in says that you get the FISA court order because there are "reasonable grounds to believe that the data is relevant to an authorized investigation to protect against international terrorism," as Section 215 requires, even though most of the records in the dataset are not associated with terrorist activity. (Administration's Use of FISA Authorities, 2013, p. 23)

Mr. Sensenbrenner situated the Coalition as the villain in this statement. Mr. Sensenbrenner positioned the Coalition as the villain because the Coalition was collecting records that were not associated with terrorist activity. Prior, Mr. Sensenbrenner identified the collection of records not associated with terrorist activity as problematic. Therefore, it is reasonable to believe that Mr. Sensenbrenner still held to the proposition that the collection of records not associated with terrorist activity was still problematic. Thus, the Coalition was causing or attempting to cause a problem by collecting records not associated with terrorist activity. Lastly, it is plausible to infer that Mr. Sensenbrenner was referring to the Coalition as he was addressing Mr. Cole, who represented the Coalition.

Mr. Nadler stated:

> The abuse of the statute, the abuse of civil liberties, the abuse of privacy is not only misuse, but miscollection [*sic*]. If you [Coalition] are collecting information about my telephone when you [Coalition] shouldn't be doing that, that is an abuse, even if you [Coalition] just simply file that and never use it. (Administration's Use of FISA Authorities, 2013, p. 25)

Mr. Nadler framed the Coalition as the villain in this statement and the problem as the abuse of civil liberties. It is reasonable to suggest he was referring to the Coalition because he was addressing the Coalition during the hearing and the fact that the Coalition was using the NSA Surveillance Program to collect telephony information. The abuse of civil liberties was stemming from the NSA Surveillance Program. To place the excerpt into context, it is reasonable to suggest that Mr. Nadler was referring to the NSA

Surveillance Program collecting metadata from citizens not associated with terrorist activity. The reason to suggest this is grounded in previous statements made by Mr. Nadler in the transcript. Therefore, the problem is the Coalition using the NSA Surveillance Program to collect metadata not associated with terrorist activity, thereby abusing one's civil liberties.

Mr. Forbes stated:

> They feel like more than any Nation in history, this is an Administration that has used enormous power of Government agents [Coalition] to oppress and harass U.S. citizens like they have seen with the IRS. And now they see this Administration using this unprecedented amount of data collection, first in their campaigns and then in Government, on amounts of data to use for the aforementioned goals. (Administration’s Use of FISA Authorities, 2013, p. 33)

Mr. Forbes situated the Coalition as the villain in this statement. It is reasonable to suggest that the term government agents include those that comprise the Coalition. It is also reasonable to suggest Mr. Forbes was villainizing the Coalition predicated on previous statements he made when drawing correlations between the Coalition and the Internal Revenue Service (IRS). The reason for suggesting Mr. Forbes was referring to the NSA Surveillance Program is due to the fact that the program collected data on citizens. Thus, at the Obama Administration's direction, the Coalition was causing a problem by using the NSA Surveillance Program to oppress and harass U.S. citizens. Lastly, it is worth noting that the Obama Administration is also positioned as a villain in this statement as the Coalition was acting on the Administration's behest.

Mr. Poe stated:

> Question, people who have had their—the law NSA violated. I think Snowden, I don't like him at all, but we would have never known what happened if he hadn't have told us. Do they have a recourse against the Government [Coalition] for improperly seizure of their records? Is there a recourse? (Administration's Use of FISA Authorities, 2013, p. 43)

Mr. Poe framed the Coalition as the villain in this statement because the NSA was a component of the Coalition and the problem was violating the law. Within the statement, it is reasonable to suggest that Mr. Poe was revealing that the NSA violated the law by improperly seizing records.

Mr. Labrador stated:

> And I understand that. I believe that this argument, before my time has expired, but I think that determination has to occur before you [Coalition] collect the data, not after you [Coalition] collect the data. And I think that is what is wrong with what you guys [Coalition] are doing at this time. (Administration's Use of FISA Authorities, 2013, p. 48)

Mr. Labrador situated the Coalition as the villain in this statement. Mr. Labrador identified that the problem was collecting data before determining whether one's data was relevant or associated with terrorist activity. It is reasonable to suggest that is what Mr. Labrador was referring to when he said "determination has to occur before you collect the data," because this is what Mr. Labrador contended before this statement in the transcript.

Additionally, it is reasonable to submit that Mr. Labrador was referring to the Coalition as he addressed Mr. Cole directly during this conversation.

Mr. Gohmert stated, “But if you [Coalition] can gather the information that a private individual could and couple that with information that only the Federal Government [Coalition] we are now learning is gathering, then it really constitutes a grave threat to privacy” (Administration’s Use of FISA Authorities, 2013, p. 58). Mr. Gohmert positioned the Coalition as the villain in this statement because he was addressing the Coalition at the time this statement was made. Mr. Gohmert argued the Coalition is causing a problem by gathering information via the NSA Surveillance Program. It is reasonable to suggest he was referring to the NSA Surveillance Program because that was the program collecting data.

Ms. Jackson Lee stated:

> One, I maintain that we have too many contractors unknown and unbeknownst in the intelligence community. I thank them for their service, but they [Coalition] need to rein in this rampant proliferation of contracts, even though the Government [Coalition] tried to defend its satellites as this, and really have a profound staff that is here in the United States Government. (Administration’s Use of FISA Authorities, 2013, p. 133)

Ms. Jackson Lee positioned the Coalition as the villain in this statement since the intelligence community is a component of the Coalition and because she was addressing the coalition at the time this statement was made. The problem, per Ms. Jackson Lee, is

the number of contractors within the intelligence community. Therefore, the Coalition was causing or attempting to cause a problem by having too many contractors.

Mr Gohmert stated, “I have now seen the incredible abuse by the FISA court, in my opinion, and I am just wondering if we are better off going to a system where we don't require a FISA court: (Administration’s Use of FISA Authorities, 2013, p. 125). Mr. Gohmert framed the FISC as the villain in this statement. The problem, according to Mr. Gohmert, was that the FISC abused its authority. Based on prior statements, it is reasonable to presume Mr. Gohmert was referring the abuse as the FISC granting the authority for the Coalition to use the NSA Surveillance Program to collect metadata on U.S. citizens.

Mr. Goodlatte stated:

> Today, we are confronted with ongoing threats from terrorist organizations, some of which are well structured, but most of which are loosely organized, as well as threats from individuals who may subscribe to certain beliefs but do not belong to a specific terrorist group. (Administration’s Use of FISA Authorities, 2013, p. 2)

Mr. Goodlatte situated terrorists and individuals as the villains in this statement. Mr. Goodlatte contended terrorists and individuals who ascribe to terrorism ideologies threaten the United States. It is reasonable to infer that Mr. Goodlatte was referring to the United States predicated on the context in which Mr. Goodlatte spoke. Mr. Goodlatte did not identify the individuals as foreign or domestic; however, he mentioned that the individual might ascribe to particular radical beliefs that align with terrorism ideologies.

There is no specific reference to a hero in this statement as there is no individual or group identified as solving or attempting to solve a problem.

Mr. Goodlatte also said:

> The terrorist threat is real and ongoing. The Boston bombing reminded us all of that. I am confident that everyone in this room wishes that tragedy could have been prevented. We cannot prevent terrorist attacks unless we can first identify and then intercept the terrorist. (Administration's Use of FISA Authorities, 2013, p. 3)

Mr. Goodlatte positioned terrorists as the villain in this statement. There is no hero in this statement as it is not clear whether Mr. Goodlatte was referring to the Coalition as identifying and intercepting terrorists since the Coalition did not prevent the Boston bombing. Therefore, one could deduce from this statement that Mr. Goodlatte was situated the Coalition as the hero or villain. Thus, due to the lack of clarity in this statement, the Coalition cannot be identified as a hero or a villain and therefore nullifies itself.

Synthesizing Data

Four main themes emerged as a result of analyzing the data. The first theme was that members of the House Judiciary Committee situated Congress as a hero more often than any other component. The first theme became apparent after identifying the hero and villain characters in the transcript and comparing the subcategories. Second, members of the House Judiciary Committee situated the Coalition as the villain more than any other component. Similar to the first theme, after coding and comparing the subcategories, the

second theme became identified. The third theme revealed that members of the House Judiciary Committee defended the USA PATRIOT Act by asserting the Coalition operated outside the statute's legal confines. After revealing the first two themes, the third theme was identified after analyzing the content in greater depth. The logic toward identifying the third theme became especially apparent after members of the House Judiciary Committee situated Congress as the hero by creating the USA PATRIOT Act to fend off terrorism. The fourth theme seemingly revealed that Congress lacked an interest in the effectiveness of the NSA Surveillance Program by expressing a greater interest in the program's legality and constitutionality. The last theme was apparent after analyzing the transcript's content to obtain a comprehensive understanding of the hearing. The graphs below illustrate how many times Congress, the Coalition, and the FISC were referenced as heroes and villains, respectively.

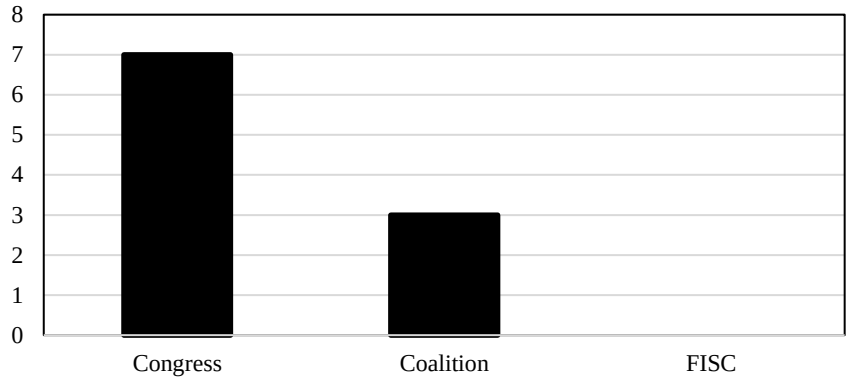

Figure 1. Hero characters.

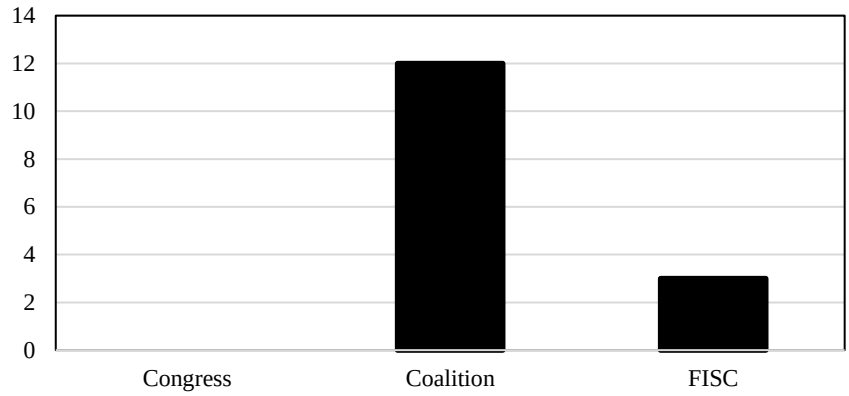

Figure 2. Villain characters.

Summary

This chapter covered the setting, demographics, data collection, data analysis, evidence of trustworthiness, and results of the study. After analyzing the data, four main themes emerged as a result of the study. The first theme was Congress was situated as a hero more than any other component. The second theme was the Coalition was positioned as a villain more than any other component. The third theme was Congress defended the USA PATRIOT Act and contended that the Coalition and the FISC operated outside the statute's bounds. The last theme seemingly revealed that Congress had a greater interest in how the NSA Surveillance Program functioned as opposed to how successful the program was regarding the detection/prevention of terrorism. An in-depth interpretation of these findings and themes, along with the study's limitations and recommendations for further research, are provided in Chapter 5.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this qualitative narrative case study was to describe how members of the House Judiciary Committee may have used rhetorical speech during the congressional hearing held on July 17, 2013, when speaking about the NSA Surveillance Program. The results of this study led to identifying how members of the House Judiciary Committee used rhetorical speech during the July 17, 2013, hearing to decide to prohibit the NSA Surveillance Program.

The methodology chosen for this topic was a dyadic qualitative case study and narrative inquiry that applied content analysis bounded by the NPF. I selected qualitative analysis due to its ability to help a researcher to critically evaluate a research question and express findings by way of holistically understanding phenomena (see Rudestam & Newton, 2015). The case study method was selected because it directs a focus on an organization, program, and event bounded by time (Rudestam & Newton, 2014). I used narrative inquiry to aid understanding of phenomena through the exploration and analysis of a story or events evolved through narration (see Ravitch & Carl, 2016). Therefore, I chose the coupled qualitative case study and narrative inquiry design to achieve an in-depth analysis of how, if at all, policymakers used rhetorical speech during a congressional hearing.

The key findings from this study revealed four themes. The first theme was that members of the House Judiciary Committee situated Congress as a hero more often than any other component. The second theme revealed that the House Judiciary Committee members demonized the Coalition by positioning the Coalition as the villain more than

any other component. The third theme was that members of the House Judiciary Committee defended the USA PATRIOT Act by asserting the Coalition operated outside the statute's legal confines. Due to the NSA Surveillance Program's questionable legal basis, the fourth and final theme seemingly revealed that Congress lacked interest regarding the program's effectiveness by expressing a greater interest in its legality and constitutionality.

Interpretation of Findings

As previously mentioned, the first theme was that members of the House Judiciary Committee situated Congress as the hero more than the Coalition or any other component (Administration's Use of FISA Authorities, 2013). This first theme seemingly revealed that the House Judiciary Committee absolved Congress of any wrongdoing for enacting the USA PATRIOT Act, which arguably provided the Coalition's legal framework to obtain authorization from the FISC to operate the NSA Surveillance Program. This theme became apparent when the conversation shifted from *analyzing* metadata to *collecting* metadata. According to the Coalition, the NSA Surveillance Program was legal under the USA PATRIOT Act (Administration's Use of FISA Authorities, 2013). Furthermore, the Coalition obtained approval from the FISC to collect the metadata for storage and only be accessed for counterterrorism matters (Administration's Use of FISA Authorities, 2013). However, Congress argued that the Coalition and the FISC violated the statute by collecting metadata not relevant to counterterrorism matters (Administration's Use of FISA Authorities, 2013). Thus, the

hearing created a distinction between collecting metadata and analyzing metadata for counterterrorism purposes.

Secondly, the committee members villainized the Coalition several times, whereas Congress was not identified as a villain (Administration's Use of FISA Authorities, 2013). Given this second theme, it is plausible to postulate that Congress did not acknowledge flaws that may have been inherent in the USA PATRIOT Act; instead, the blame was on the Coalition and the FISC for misinterpreting the statute. Thirdly, Congress defended the USA PATRIOT Act by asserting the Coalition operated outside the legal confines of what the statute allowed (Administration's Use of FISA Authorities, 2013). Congress also argued the FISC did not abide by the USA PATRIOT Act in authorizing the Coalition to utilize the NSA Surveillance Program to collect metadata on U.S. citizens not associated or relevant to terrorism (Administration's Use of FISA Authorities, 2013).

Fourthly, it appeared that Congress lacked interest in the NSA Surveillance Program's effectiveness regarding counterterrorism efforts. It is reasonable to presume this fourth theme because the discussion seemingly centered on the legality and constitutionality of collecting metadata on citizens not associated with terrorism, rather than collecting metadata on terrorists. Therefore, it is reasonable to conclude that Congress was more interested in learning how the NSA Surveillance Program functioned and how the Coalition would defend the legality and constitutionality of the NSA Surveillance Program.

Upon reviewing the NPF mesolevel hypotheses, it could be argued that the aforementioned themes align with two NPF hypotheses. For example, the first and second themes align with the devil-angel shift hypothesis (Weible & Sabatier, 2018). The devil-angel shift is when a legislator may situate themselves or their group as the hero and their opposition as the villain (Weible & Sabatier, 2018). Some studies have found that the winning individual/group in a policy debate will employ the "angel shift at statistically higher rates than the losing coalition" (Weible & Sabatier, 2018, p. 193). Additionally, the winning individual/group may also employ the devil shift at a higher rate than the losing coalition (Weible & Sabatier, 2018). The second hypothesis worth noting that aligned with themes three and four is the "issue containment as a narrative strategy" (Weible & Sabatier, 2018, p. 193). The issue containment strategy is employed by legislators who attempt to contain an issue by not addressing other variables associated with the problem (Weible & Sabatier, 2018). This strategy seemed to align with the rhetorical discourse exhibited in the transcript when the discussion focused on collecting metadata rather than preventing terrorism.

Perliger's (2012) seminal work found that after a terrorist attack, behavioral and rational thought patterns are adversely affected, which ultimately elicits an emotional response enacted through aggressive counterterrorism policy. Perhaps it is fair to say that Perliger's findings imply that behavioral and rational thought patterns are adversely affected after any devastating or significant event. Similarly, Weible and Sabatier (2018), and Shanahan et al. (2018) echoed the belief that an emotional response is the consequence of a significant event by affirming that people make irrational decisions

bounded by time and supported with limited information that is subjected to rhetorical speech. Given this information, it is plausible to suggest that Congress provided emotional responses during the congressional hearing after the NSA Surveillance Program's unauthorized disclosure.

This study's original gap was addressed and identified by positing that members of Congress leveraged rhetorical speech during the House Judiciary Committee hearing on July 17, 2013. Additionally, the purpose of this research was also addressed by describing how the themes aligned with the two NPF hypotheses. Therefore, given the results and synthesis of the data, it is reasonable to suggest that rhetorical speech from the hearing commandeered the trajectory of the dialogue during this hearing, and that rhetorical speech may have adversely affected rational judgment and decision making (Perliger, 2012; Shanahan et al., 2018; Weible & Sabatier, 2018).

Casarez (2016) and Berman (2016) posited that after the NSA Surveillance Program's unauthorized disclosure, U.S. intelligence/surveillance became the topic of interest for public and political discourse, which began to erode the public's trust in the U.S. government and confidence in their electronic communications. Perhaps this erosion of trust could be interpreted as being indicative of the House Judiciary Committee hearing that took place on July 17, 2013. Thus, it further may be argued that the rhetorical discourse, as demonstrated in this congressional hearing, perpetuated the public's distrust in the U.S. government and further affected succeeding congressional hearings.

Limitations of the Study

The veracity of this research is limited to its scope. As the data included identifying narrative characters at a congressional hearing, this research excluded press hearings, public speeches, media, social media, and other sources of potential data that may have enriched understanding regarding the effects of narration prohibiting the NSA Surveillance Program. Additionally, I was the only researcher gathering and analyzing the data; therefore, it was not feasible or practical for this study to include several congressional hearings or other data sources.

As the sole researcher for this study, dependability issues arose regarding content analysis and the identification of narrative characters in the congressional hearing transcript. Consequently, each excerpt from the congressional hearing transcript that applied to the particular narrative character's definition was displayed in this study. Additionally, an explanation was provided beneath each excerpt to articulate how each excerpt met the definition of the identified narrative character(s).

Recommendations

There are several recommendations for further research that align with this study. The first recommendation for additional research is to apply the NPF mesolevel content analysis to witnesses who provided testimony at a congressional hearing in addition to the members of Congress who attended that hearing. By applying the narratological lens to the witnesses and Congress members, it may be possible to identify how rhetorical speech differed between the witnesses and legislators. The additional data would contribute to the content analysis paradigm and enhance policy narrative learning

(Weible & Sabatier, 2018). The second recommendation for additional research is to apply the same theoretical framework and research design as provided in this dissertation to other congressional hearings that led toward enacting the USA FREEDOM Act of 2015. By examining additional congressional hearings that led toward banning the NSA Surveillance Program, it may be possible to determine if any rhetorical speech pattern analysis exists and thereby contribute to policy narrative learning (Weible & Sabatier, 2018).

The third recommendation for further research is to apply the same theoretical framework and research design to a congressional hearing that occurred after the terrorist attacks on September 11, 2001. By examining a congressional hearing that led toward drafting the USA PATRIOT Act of 2001, it may be possible to identify if rhetorical speech was present during that congressional hearing to learn how rhetorical speech may have been leveraged to enhance counterterrorism legislation. The fourth recommendation for further research is to take findings from the third recommendation and juxtapose those findings with this dissertation's results. By examining the rhetorical speech that led toward enhancing counterterrorism legislation and the rhetorical speech that led toward enhancing civil liberties, it may be possible to describe and perhaps illustrate how rhetorical speech fluctuates across a broad time continuum (Shanahan et al., 2018; Weible & Sabatier, 2018). All four recommendations would contribute to policy narrative learning, as described by Weible and Sabatier (2018). It is necessary to contribute to the policy narrative learning paradigm to refine and improve understanding regarding the use of rhetorical speech and its effects on policy.

Implications

This study has several implications for positive social change at various levels. However, the most direct impact regarding positive social change is toward the legislator. This study confirmed that the House Judiciary Committee members utilized rhetorical speech and how the legislators used rhetorical speech at the July 17, 2013, congressional hearing that led toward the USA FREEDOM Act of 2015. This study's findings may provoke legislators' interest in increasing their understanding regarding rhetorical speech and its effects on policy. Therefore, should the legislator increase their understanding of rhetorical speech and its effects on policy, s/he may recognize rhetorical speech in real-time and redirect the trajectory of the dialogue to keep policy debates impartial and free from emotional responses.

The domestic security dilemma is a recurring problem whereby counterterrorism programs are continuously in a state of flux as demands for increased civil liberties and national security compete (Field, 2017) – as demonstrated by the USA PATRIOT Act of 2001 and the USA FREEDOM Act of 2015 (Hu, 2018). One of the variables that contribute to the domestic security dilemma is the emotional response, which is often the consequence proceeding a significant event or terrorist attack (Perliger, 2012). These emotional responses are then further subjected to rhetorical speech, which may commandeer the policy debate trajectory (Weible & Sabatier, 2018). Policymakers use rhetorical speech to garner public support, and politicians may choose to divide groups on a moral basis by strategically leveraging narration (Weible & Sabatier, 2018). Consequently, since rhetorical speech influences legislation, should it be left unchecked,

it may adversely commandeer rational logic and decision making (Perliger, 2012; Pilecki, 2017; Weible & Sabatier, 2018). Therefore, in an effort for legislators to suspend their bias and perceive a policy solution from a neutral posture, it is necessary to understand rhetorical speech's power and recognize it when rhetorical speech surfaces during a policy debate. Should legislators accomplish this feat, this may lead to serving as a remedy for the domestic security dilemma. Thus, the implications for this are systemic positive social change as policy at the congressional level affects all United States citizens.

Additionally, this study's implications contribute to the scholarly literature concerning the NPF and content analysis application. Weible et al. (2016) argued the importance of congruency among narratological studies in terms of character definitions and means of utility regarding content analysis. Therefore, this dissertation was clear and thorough, explaining the research design, data collection, and content analysis. This study may serve as an example for other scholars to resemble while utilizing the NPF as their theoretical framework and employing content analysis.

Conclusion

Several notable public officials argued the NSA Surveillance Program was a valuable tool for the Intelligence Community (Obama Administration, 2013). Former NSA Director Michael Rogers expressed concern that the elimination of bulk metadata collection would adversely affect the NSA's ability to detect imminent terrorist threats (NSA, 2015). Moreover, Rogers confirmed that ending bulk collection would diminish the NSA's operational aptitude and that there was no replacement for the benefit of bulk

metadata collection (NSA, 2015). Supporting Rogers' position on bulk metadata collection, Mukasey (2015) and Yoo (2014) argued that the NSA Surveillance Program was a vital tool for the Intelligence Community that was legal and constitutional. Contrastingly, those who opposed the NSA Surveillance Program defended civil liberties by arguing the program violated the Constitution, did not apply to the third-party doctrine as outlined in the Supreme Court ruling on *Smith v. Maryland*, and it fostered an environment of distrust among the government and the governed (Donohue, 2014; Liu et al., 2015; Rapisarda, 2015; Shamsi & Abdo, 2011; Thompson, 2014).

Given these complex variables concerning the constitutionality and legality of the NSA Surveillance Program and given the complex nature of this study, one thing is for certain – that legislators used rhetorical speech during the July 17, 2013, congressional hearing leading to the USA FREEDOM Act of 2015. Weible and Sabatier (2018), Pilecki (2017), and Perliger (2012) identified that rhetorical speech might adversely affect rational thought and decision making. Consequently, adverse rational thought and decision making may lead to an ineffective policy decision (Perliger, 2012). Likewise, if policymakers do not recognize rhetorical speech when it surfaces during a policy debate, the dialogue may be situated on an unfavorable trajectory indicative of irrational thought. When considering the grave circumstances regarding the effectiveness of counterterrorism legislation, the consequences may become dire. Therefore, it is imperative to understand how rhetorical speech is utilized and how to identify rhetorical speech when it manifests.

References

Administration's Use of FISA Authorities: *Hearing before the House Judiciary Committee, House of Representatives* (Serial 113-45), 113th Cong. (2013). Retrieved from https://www.govinfo.gov

Barnett, R. (2015). Why the NSA data seizures are unconstitutional. *Harvard Journal of Law & Public Policy, 38,* 3–20. Retrieved from https://www.harvard-jlpp.com/

Bendix, W., & Quirk, P. (2016). Deliberating surveillance policy: Congress, the FBI, and the abuse of national security letters. *Journal of Policy History*, *18*(3), 447-469. doi:10.1017/S0898030616000178

Berman, E. (2014). Regulating domestic intelligence collection. *Washington & Lee Law Review,* 71(1), 3–91. Retrieved from lawreview.journals.wlu.io/

Berman, E. (2016). The two faces of the Foreign Intelligence Surveillance Court. *Indiana Law Journal*, 91(4), 1191–1250. Retrieved from https://www.law.indiana.edu/student-life/journals/

Burkholder, G. J., Cox, K. A., & Crawford, L. M., (2016). *Scholar-practitioner's guide to research design*. Baltimore, MD: Laureate Publishing

Casarez, N. B. (2016). The synergy of privacy and speech. *University of Pennsylvania Journal of Constitutional Law*, 3, 813. Retrieved from https://www.law.upenn.edu/journals/conlaw/

Congressional Digest. (2015) The pros and cons of the NSA's domestic surveillance program. Retrieved from https://congressionaldigest.com/

Denzin, N. K., & Lincoln, Y. S. (2013). *The landscape of qualitative research* (4th ed.). Thousand Oaks, CA: SAGE

Donohue, L. K. (2014). Bulk metadata collection: Statutory and constitutional considerations. *Harvard Journal of Law & Public Policy, 37*(3), 757–900. Retrieved from https://www.harvard-jlpp.com/

Federal Bureau of Investigation: Hearing before the Committee on the Judiciary, House, 113th Cong. 1 (2014). Retrieved from https://www.govinfo.gov/

Federal Bureau of Investigation. (n.d.). *Terrorism*. Retrieved from https://www.fbi.gov/investigate/terrorism

Field, A. (2017). The dynamics of terrorism and counterterrorism: Understanding the domestic security dilemma. *Studies in Conflict & Terrorism, 40*(6), 470–483. doi:10.1080/1057610X.2016.1221253

Forsyth, B. (2015). Banning bulk: Passage of the USA FREEDOM Act of 2015 and ending bulk collection. *Washington and Lee Law Review*, (3), 1307. Retrieved from http://lawreview.journals.wlu.io/

Galicki, A. (2015). End of Smith v. Maryland: The NSA's bulk telephony metadata program and the fourth amendment in the cyber age. *American Criminal Law Review*, (2), 375. Retrieved from https://www.law.georgetown.edu/american-criminal-law-review/

Government Publishing Office. (n.d.). About us. Retrieved from https://www.govinfo.gov/about

Hu, M. (2018). Bulk biometric metadata collection. *North Carolina Law Review, 96,*1425–1474. Retrieved from https://scholarlycommons.law.wlu.edu/wlufac/577/

Jackson, R. (2005). Security, democracy, and the rhetoric of counterterrorism. *Democracy & Security*, 1(2), 147–171. doi:10.1080/17419160500322517

Jaffer, J. (2010). The mosaic theory. *Social Research, 77*(3), 873–882. Retrieved from https://www.socres.org/

Jones, M. D., & McBeth, M. K. (2010). A narrative policy framework: Clear enough to be wrong. *Policy Studies Journal, 38*(2), 329. doi:10.1111/j.1541-0072.2010.00364.x

Jones, M. D., Shanahan, E. A, & McBeth, M. K. (2011). *The science of stories: Applications of the Narrative Policy Framework in public policy analysis*. New York, NY: Palgrave Macmillan

Judiciary Committee. (2015). USA FFREEDOM Act of 2015. Retrieved from https://judiciary.house.gov/issue/usa-freedom-act/

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: The power of reflexivity. *International Journal of Interdisciplinary Educational Studies, 13*(1), 19–31. doi:10.18848/2327-011X/CGP/v13i01/19-31

Lichtman, M. (2014). *Qualitative research in education* (4th ed.). Thousand Oaks, CA: SAGE

Liu, E. C., Nolan, A., & Thompson II, R. M. (2014). *Overview of Constitutional challenges to NSA collection activities and recent developments*. Washington, DC: Congressional Research Service

Martin, W. E., & Bridgmon, K. D., (2016). *Quantitative and statistical research methods*. San Francisco, CA: Jossey-Bass

Mukasey, M. B. (2015). Safe and surveilled: Former US Attorney General Michael B. Mukasey on the NSA, wiretapping, and prism [Symposium address]. *National Security Law Journal, 3*(2), 196. Retrieved from https://www.nslj.org/wp-content/uploads/3_NatlSecLJ_196-209_Mukasey.pdf

National Security Agency: Hearing before the Committee on Intelligence, Senate, 114th Cong. 1 (2015). Retrieved from https://www.govinfo.gov/

Noffke, S. &Somekh, B. (2009). *The SAGE handbook of educational action research*. Thousand Oaks, CA: SAGE

Obama Administration. (2013). Bulk collection of telephony metadata under Section 215 of the USA PATRIOT Act of 2001. Retrieved from https://fas.org/irp/nsa/bulk-215.pdf

Office of the Inspector General. (2009). National Security Agency. Central Security Service (Report No. ST-09-0002). Retrieved from https://apps.washingtonpost.com/g/page/world/national-security-agency-inspector-general-draft-report/277/

Ombres, D. (2015). NSA domestic surveillance from the PATRIOT Act to the FREEDOM Act: The underlying history, constitutional basis, and the efforts at

reform. *Seton Hall Legislative Journal, 39*(1). Retrieved from https://scholarship.shu.edu/shlj/

Osinowo, G. A. (2019). *Internet and telecommunications companies' provision of customer information to the government* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 22583301)

Oversight of the Federal Bureau of Investigation: Hearing before the Committee on the Judiciary, Senate, 113th Cong. (2013). Retrieve from https://www.govinfo.gov/

Oversight of the Foreign Intelligence Surveillance Act: Hearing before the Committee on the Judiciary, House, 116th Cong. (2019). Retrieved from https://www.govinfo.gov/

Perliger, A. (2012). How democracies respond to terrorism: regime characteristics, symbolic power, and counterterrorism. *Security Studies*, 21(3), 490–528. doi:10.1080/09636412.2012.706505

Pilecki, A. (2017). The moral dimensions of the terrorist category construction in presidential rhetoric and their use in legitimizing counterterrorism policy. *Qualitative Psychology*, (1), 23. doi:10.1037/qup0000037

Pillar, P. R. (2004). Counterterrorism after Al Qaeda. *Washington Quarterly*, 27(3), 101–113. Retrieved from https://twq.elliott.gwu.edu/

Pokalova, E. (2015). Legislative responses to terrorism: what drives states to adopt new counterterrorism legislation? *Terrorism & Political Violence*, 27(3), 474–496. doi:10.1080/09546553.2013.809339

Pozen, D. E. (2005). The mosaic theory, national security, and the Freedom of

Information Act. *Yale Law Journal*, (3), 628. Retrieved from https://www.yalelawjournal.org/

Ramos, M.C. (1989). Some ethical implications of qualitative research. *Research in Nursing & Health*, 12, 57-63. doi:10.1002/nur.4770120109

Rapisarda, M. (2015). Privacy, technology, and surveillance: NSA bulk collection and the end of the Smith v. Maryland era. *Gonzaga Law Review, 51*(1), 122–158. Retrieved from https://gonzagalawreview.com/

Ravitch, S. M., & Carl, N. M. (2016). *Qualitative research: Bridging the conceptual, theoretical, and methodological*. Thousand Oaks, CA: SAGE

Ravitch, S. M., & Riggan, M. (2012). *Reason and rigor: How conceptual frameworks guide research.* Thousand Oaks, CA: SAGE

Reilly, B. C. (2015). Doing more with more: The efficacy of big data in the intelligence community. *American Intelligence Journal*, 32(1), 18–24. Retrieved from https://www.jstor.org/journal/amerintej

Rudestam, K. E., & Newton, R. R. (2015). *Surviving your dissertation* (4th ed.). Thousand Oaks, CA: SAGE

Rule, P. (2011). Bakhtin and Freire: Dialogue, dialectic and boundary learning. *Educational Philosophy and Theory, 43*(9), 924-942. doi:10.1111/j.1469-5812.2009.00606.x

Sanders, M. L. (2016). *The USA PATRIOT Act of 2001 and punctuated equilibrium* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 1825665158)

Shamsi, H., & Abdo, A. (2011). Privacy and surveillance post-9/11. Retrieved from https://www.americanbar.org

Shanahan, E. A., Jones, M. D., & McBeth, M. K. (2018). How to conduct a Narrative Policy Framework study. *Social Science Journal*. doi:10.1016/j.soscij.2017.12.002

Shanahan, E. A., Jones, M. D., & McBeth, M. K. (2011). Policy narratives and policy processes. *Policy Studies Journal, 39*(3), 535-561. Retrieved from http://www.ipsonet.org/publications/journals/psj

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, 22(2), 63–75. doi:10.3233/EFI-2004-22201

Shor, E., Baccini, L., Tsai, C.-T., Lin, T.-H., & Chen, T. C. (2018). Counterterrorist legislation and respect for civil liberties: An inevitable collision? *Studies in Conflict & Terrorism*, 41(5), 339–364. doi:10.1080/1057610X.2017.1314653

Stransky, S. G. (2016). The Fourth Amendment and bulk telephone metadata: An overview of recent case law. *St. Louis University Public Law Review, 35*(1), 3–45. Retrieved from https://scholarship.law.slu.edu/plr/

Tang, S. (2009). 'The security dilemma: A conceptual analysis. *Security Studies*. 18:3, 587-623. doi: 10.1080/09636410903133050

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). *Digital crime and digital terrorism* (3rd ed.). Upper Saddle River, NJ: Pearson

Terchek, R., & Conte, T. (2001). *Theories of democracy*. Lanham, MD: Rowman & Littlefield.

Thompson, R. M. (2014). *The Fourth Amendment Third-Party Doctrine.* Washington, DC: Congressional Research Service

Thurairajah, K. (2019). Uncloaking the researcher: Boundaries in qualitative research. *Qualitative Sociology Review*, (1), 132. doi:10.18778/1733-8077.15.1.06

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. 114-23, § 1861, 129 Stat. 268 (2015). Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/2048

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (2001). Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3162

Weible, C. M., Olofsson, K. L., Costie, D. P., Katz, J. M., & Heikkila, T. (2016).Enhancing precision and clarity in the study of policy narratives: Ananalysis of climate and air issues in Delhi, India. *Review of Policy Research*, 33(4), 420–441. doi:10.1111/ropr.12181

Weible, C. M., & Sabatier, P. A. (2018). *Theories of the Policy Process* (4th ed.). New York, NY: Westview Press

White House. 2015. Statement by the President on the USA FREEDOM Act of 2015. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act

Young, M. D. (2011). Electronic surveillance in an era of modern technology and

evolving threats to national security. *Stanford Law & Policy Review*, 22(1), 11–39. Retrieved from https://law.stanford.edu/stanford-law-policy-review-slpr/

Yoo, J. (2014). The legality of the National Security Agency's bulk data surveillance programs. *Harvard Journal of Law & Public Policy*, *37*(3), 901–930. Retrieved from https://www.harvard-jlpp.com/

Appendix A: USA PATRIOT Act of 2001 Summary

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 - **Title I: Enhancing Domestic Security Against Terrorism** - Establishes in the Treasury the Counterterrorism Fund.
(Sec. 102) Expresses the sense of Congress that: (1) the civil rights and liberties of all Americans, including Arab Americans, must be protected, and that every effort must be taken to preserve their safety; (2) any acts of violence or discrimination against any Americans be condemned; and (3) the Nation is called upon to recognize the patriotism of fellow citizens from all ethnic, racial, and religious backgrounds.

(Sec. 103) Authorizes appropriations for the Federal Bureau of Investigation's (FBI) Technical Support Center.

(Sec. 104) Authorizes the Attorney General to request the Secretary of Defense to provide assistance in support of Department of Justice (DOJ) activities relating to the enforcement of Federal criminal code (code) provisions regarding the use of weapons of mass destruction during an emergency situation involving a weapon (currently, chemical weapon) of mass destruction.

(Sec. 105) Requires the Director of the U.S. Secret Service to take actions to develop a national network of electronic crime task forces throughout the United States to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

(Sec. 106) Modifies provisions relating to presidential authority under the International Emergency Powers Act to: (1) authorize the President, when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, to confiscate any property subject to U.S. jurisdiction of a foreign person, organization, or country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks (the rights to which shall vest in such agency or person as the President may designate); and (2) provide that, in any judicial review of a determination made under such provisions, if the determination was based on classified information such information may be submitted to the reviewing court ex parte and in camera.

Title II: Enhanced Surveillance Procedures - Amends the Federal criminal code to authorize the interception of wire, oral, and electronic communications for the production of evidence of: (1) specified chemical weapons or terrorism offenses; and (2) computer fraud and abuse.

(Sec. 203) Amends rule 6 of the Federal Rules of Criminal Procedure (FRCrP) to permit the sharing of grand jury information that involves foreign intelligence or counterintelligence with Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials (such officials), subject to specified requirements.

Authorizes an investigative or law enforcement officer, or an attorney for the Government, who, by authorized means, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom to disclose such contents to such officials to the extent that such contents include foreign intelligence or counterintelligence.

Directs the Attorney General to establish procedures for the disclosure of information (pursuant to the code and the FRCrP) that identifies a United States person, as defined in the Foreign Intelligence Surveillance Act of 1978 (FISA).

Authorizes the disclosure of foreign intelligence or counterintelligence obtained as part of a criminal investigation to such officials.

(Sec. 204) Clarifies that nothing in code provisions regarding pen registers shall be deemed to affect the acquisition by the Government of specified foreign intelligence information, and that procedures under FISA shall be the exclusive means by which electronic surveillance and the interception of domestic wire and oral (current law) and electronic communications may be conducted.

(Sec. 205) Authorizes the Director of the FBI to expedite the employment of personnel as translators to support counter-terrorism investigations and operations without regard to applicable Federal personnel requirements. Requires: (1) the Director to establish such security requirements as necessary for such personnel; and (2) the Attorney General to report to the House and Senate Judiciary Committees regarding translators.

(Sec. 206) Grants roving surveillance authority under FISA after requiring a court order approving an electronic surveillance to direct any person to furnish necessary information, facilities, or technical assistance in circumstances where the Court finds that the actions of the surveillance target may have the effect of thwarting the identification of a specified person.

(Sec. 207) Increases the duration of FISA surveillance permitted for non-U.S. persons who are agents of a foreign power.

(Sec. 208) Increases (from seven to 11) the number of district court judges designated to hear applications for and grant orders approving electronic surveillance. Requires that no fewer than three reside within 20 miles of the District of Columbia.

(Sec. 209) Permits the seizure of voice-mail messages under a warrant.

(Sec. 210) Expands the scope of subpoenas for records of electronic communications to include the length and types of service utilized, temporarily assigned network addresses, and the means and source of payment (including any credit card or bank account number).

(Sec. 211) Amends the Communications Act of 1934 to permit specified disclosures to Government entities, except for records revealing cable subscriber selection of video programming from a cable operator.

(Sec. 212) Permits electronic communication and remote computing service providers to make emergency disclosures to a governmental entity of customer electronic communications to protect life and limb.

(Sec. 213) Authorizes Federal district courts to allow a delay of required notices of the execution of a warrant if immediate notice may have an adverse result and under other specified circumstances.

(Sec. 214) Prohibits use of a pen register or trap and trace devices in any investigation to protect against international terrorism or clandestine intelligence activities that is conducted solely on the basis of activities protected by the first amendment to the U.S. Constitution.

(Sec. 215) Authorizes the Director of the FBI (or designee) to apply for a court order requiring production of certain business records for foreign intelligence and international terrorism investigations. Requires the Attorney General to report to the House and Senate Intelligence and Judiciary Committees semi-annually.

(Sec. 216) Amends the code to: (1) require a trap and trace device to restrict recoding or decoding so as not to include the contents of a wire or electronic communication; (2) apply a court order for a pen register or trap and trace devices to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of the order; (3) require specified records kept on any pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public; and (4) allow a trap and trace device to identify the source (but not the contents) of a wire or electronic communication.

(Sec. 217) Makes it lawful to intercept the wire or electronic communication of a computer trespasser in certain circumstances.

(Sec. 218) Amends FISA to require an application for an electronic surveillance order or search warrant to certify that a significant purpose (currently, the sole or main purpose) of the surveillance is to obtain foreign intelligence information.

(Sec. 219) Amends rule 41 of the FRCrP to permit Federal magistrate judges in any district in which terrorism-related activities may have occurred to issue search warrants for searches within or outside the district.

(Sec. 220) Provides for nationwide service of search warrants for electronic evidence.

(Sec. 221) Amends the Trade Sanctions Reform and Export Enhancement Act of 2000 to extend trade sanctions to the territory of Afghanistan controlled by the Taliban.

(Sec. 222) Specifies that: (1) nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance; and (2) a provider of such service, and a landlord, custodian, or other person who furnishes such facilities or technical assistance, shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance.

(Sec. 223) Amends the Federal criminal code to provide for administrative discipline of Federal officers or employees who violate prohibitions against unauthorized disclosures of information gathered under this Act. Provides for civil actions against the United States for damages by any person aggrieved by such violations.

(Sec. 224) Terminates this title on December 31, 2005, except with respect to any particular foreign intelligence investigation beginning before that date, or any particular offense or potential offense that began or occurred before it.

(Sec. 225) Amends the Foreign Intelligence Surveillance Act of 1978 to prohibit a cause of action in any court against a provider of a wire or electronic communication service, landlord, custodian, or any other person that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under such Act (for example, with respect to a wiretap).

Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 - International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001- Sunsets this Act after the first day of FY 2005 if Congress enacts a specified joint resolution to that effect.

Subtitle A: International Counter Money Laundering and Related Measures - Amends Federal law governing monetary transactions to prescribe procedural guidelines under which the Secretary of the Treasury (the Secretary) may require domestic financial institutions and agencies to take specified measures if the Secretary finds that reasonable grounds exist for concluding that jurisdictions, financia1 institutions, types of accounts, or transactions operating outside or within the United States, are of primary money laundering concern. Includes mandatory disclosure of specified information relating to certain correspondent accounts.

(Sec. 312) Mandates establishment of due diligence mechanisms to detect and report money laundering transactions through private banking accounts and correspondent accounts.

(Sec. 313) Prohibits U.S. correspondent accounts with foreign shell banks.

(Sec. 313) Prohibits U.S. correspondent accounts with foreign shell banks.

(Sec. 314) Instructs the Secretary to adopt regulations to encourage further cooperation among financial institutions, their regulatory authorities, and law enforcement authorities, with the specific purpose of encouraging regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected (based on credible evidence) of engaging in terrorist acts or money laundering activities. Authorizes such regulations to create procedures for cooperation and information sharing on matters specifically related to the finances of terrorist groups as well as their relationships with international narcotics traffickers.

Requires the Secretary to distribute annually to financial institutions a detailed analysis identifying patterns of suspicious activity and other investigative insights derived from suspicious activity reports and investigations by Federal, State, and local law enforcement agencies.

(Sec. 315) Amends Federal criminal law to include foreign corruption offenses as money laundering crimes.

(Sec. 316) Establishes the right of property owners to contest confiscation of property under law relating to confiscation of assets of suspected terrorists.

(Sec. 317) Establishes Federal jurisdiction over: (1) foreign money launderers (including their assets held in the United States); and (2) money that is laundered through a foreign bank.

(Sec. 319) Authorizes the forfeiture of money laundering funds from interbank accounts. Requires a covered financial institution, upon request of the appropriate Federal banking agency, to make available within 120 hours all pertinent information related to anti-money laundering compliance by the institution or its customer. Grants the Secretary summons and subpoena powers over foreign banks that maintain a correspondent bank in the United States. Requires a covered financial institution to terminate within ten business days any correspondent relationship with a foreign bank after receipt of written notice that the foreign bank has failed to comply with certain judicial proceedings. Sets forth civil penalties for failure to terminate such relationship.

(Sec. 321) Subjects to record and report requirements for monetary instrument transactions: (1) any credit union; and (2) any futures commission merchant, commodity trading advisor, and commodity pool operator registered, or required to register, under the Commodity Exchange Act.

(Sec. 323) Authorizes Federal application for restraining orders to preserve the availability of property subject to a foreign forfeiture or confiscation judgment.

(Sec. 325) Authorizes the Secretary to issue regulations to ensure that concentration accounts of financial institutions are not used to prevent association of the identity of an individual customer with the movement of funds of which the customer is the direct or beneficial owner.

(Sec. 326) Directs the Secretary to issue regulations prescribing minimum standards for financial institutions regarding customer identity in connection with the opening of accounts.

Requires the Secretary to report to Congress on: (1) the most timely and effective way to require foreign nationals to provide domestic financial institutions and agencies with appropriate and accurate information; (2) whether to require foreign nationals to obtain an identification number (similar to a Social Security or tax identification number) before opening an account with a domestic financial institution; and (3) a system for domestic financial institutions and agencies to review Government agency information to verify the identities of such foreign nationals.

(Sec. 327) Amends the Bank Holding Company Act of 1956 and the Federal Deposit Insurance Act to require consideration of the effectiveness of a company or companies in combating money laundering during reviews of proposed bank shares acquisitions or mergers.

(Sec. 328) Directs the Secretary take reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the United States and other countries, with the information to remain with the transfer from its origination until the point of disbursement. Requires annual progress reports to specified congressional committees.

(Sec. 329) Prescribes criminal penalties for Federal officials or employees who seek or accept bribes in connection with administration of this title.

(Sec. 330) Urges U.S. negotiations for international cooperation in investigations of money laundering, financial crimes, and the finances of terrorist groups, including record sharing by foreign banks with U.S. law enforcement officials and domestic financial institution supervisors.

Subtitle B: Bank Secrecy Act Amendments and Related Improvements - Amends Federal law known as the Bank Secrecy Act to revise requirements for civil liability immunity for voluntary financial institution disclosure of suspicious activities. Authorizes the inclusion of suspicions of illegal activity in written employment references.

(Sec. 352) Authorizes the Secretary to exempt from minimum standards for anti-money laundering programs any financial institution not subject to certain regulations governing financial recordkeeping and reporting of currency and foreign transactions.

(Sec. 353) Establishes civil penalties for violations of geographic targeting orders and structuring transactions to evade certain recordkeeping requirements. Lengthens the effective period of geographic targeting orders from 60 to 180 days.

(Sec. 355) Amends the Federal Deposit Insurance Act to permit written employment references to contain suspicions of involvement in illegal activity.

(Sec. 356) Instructs the Secretary to: (1) promulgate regulations requiring registered securities brokers and dealers, futures commission merchants, commodity trading advisors, and commodity pool operators, to file reports of suspicious financial transactions; (2) report to Congress on the role of the Internal Revenue Service in the administration of the Bank Secrecy Act; and (3) share monetary instruments transactions records upon request of a U.S. intelligence agency for use in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.

(Sec. 358) Amends the Right to Financial Privacy Act to permit the transfer of financial records to other agencies or departments upon certification that the records are relevant to intelligence or counterintelligence activities related to international terrorism.

(Sec. 359) Subjects to mandatory records and reports on monetary instruments transactions any licensed sender of money or any other person who engages as a business in the transmission of funds, including through an informal value transfer banking system or network (e.g., hawala) of people facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.

(Sec. 360) Authorizes the Secretary to instruct the United States Executive Director of each international financial institution to use his or her voice and vote to: (1) support the use of funds for a country (and its institutions) which contributes to U.S. efforts against international terrorism; and (2) require an auditing of disbursements to ensure that no funds are paid to persons who commit or support terrorism.

(Sec. 361) Makes the existing Financial Crimes Enforcement Network a bureau in the Department of the Treasury.

(Sec. 362) Directs the Secretary to establish a highly secure network in the Network that allows financial institutions to file certain reports and receive alerts and other information regarding suspicious activities warranting immediate and enhanced scrutiny.

(Sec. 363) Increases to $1 million the maximum civil penalties (currently $10,000) and criminal fines (currently $250,000) for money laundering. Sets a minimum civil penalty and criminal fine of double the amount of the illegal transaction.

(Sec. 364) Amends the Federal Reserve Act to provide for uniform protection authority for Federal Reserve facilities, including law enforcement officers authorized to carry firearms and make warrantless arrests.

(Sec. 365) Amends Federal law to require reports relating to coins and currency of more than $10,000 received in a nonfinancial trade or business.

(Sec. 366) Directs the Secretary to study and report to Congress on: (1) the possible expansion of the currency transaction reporting requirements exemption system; and (2) methods for improving financial institution utilization of the system as a way of reducing the submission of currency transaction reports that have little or no value for law enforcement purposes.

Subtitle C: Currency Crimes - Establishes as a bulk cash smuggling felony the knowing concealment and attempted transport (or transfer) across U.S. borders of currency and monetary instruments in excess of $10,000, with intent to evade specified currency reporting requirements.

(Sec. 372) Changes from discretionary to mandatory a court's authority to order, as part of a criminal sentence, forfeiture of all property involved in certain currency reporting offenses. Leaves a court discretion to order civil forfeitures in money laundering cases.

(Sec. 373) Amends the Federal criminal code to revise the prohibition of unlicensed (currently, illegal) money transmitting businesses.

(Sec. 374) Increases the criminal penalties for counterfeiting domestic and foreign currency and obligations.

(Sec. 376) Amends the Federal criminal code to extend the prohibition against the laundering of money instruments to specified proceeds of terrorism.

(Sec. 377) Grants the United States extraterritorial jurisdiction where: (1) an offense committed outside the United States involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within U.S. jurisdiction; and (2) the person committing the offense transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within U.S. jurisdiction any article used to assist in the commission of the offense or the proceeds of such offense or property derived from it.

Title IV: Protecting the Border - **Subtitle A: Protecting the Northern Border** - Authorizes the Attorney General to waive certain Immigration and Naturalization Service (INS) personnel caps with respect to ensuring security needs on the Northern border.

(Sec. 402) Authorizes appropriations to: (1) triple the number of Border Patrol, Customs Service, and INS personnel (and support facilities) at points of entry and along the Northern border; and (2) INS and Customs for related border monitoring technology and equipment.

(Sec. 403) Amends the Immigration and Nationality Act to require the Attorney General and the Federal Bureau of Investigation (FBI) to provide the Department of State and INS with access to specified criminal history extracts in order to determine whether or not a visa or admissions applicant has a criminal history. Directs the FBI to provide periodic extract updates. Provides for confidentiality.

Directs the Attorney General and the Secretary of State to develop a technology standard to identify visa and admissions applicants, which shall be the basis for an electronic system of law enforcement and intelligence sharing system available to consular, law enforcement, intelligence, and Federal border inspection personnel.

(Sec. 404) Amends the Department of Justice Appropriations Act, 2001 to eliminate certain INS overtime restrictions.

(Sec. 405) Directs the Attorney General to report on the feasibility of enhancing the Integrated Automated Fingerprint Identification System and other identification systems to better identify foreign individuals in connection with U.S. or foreign criminal investigations before issuance of a visa to, or permitting such person's entry or exit from, the United States. Authorizes appropriations.

Subtitle B: Enhanced Immigration Provisions - Amends the Immigration and Nationality Act to broaden the scope of aliens ineligible for admission or deportable due to terrorist activities to include an alien who: (1) is a representative of a political, social, or similar group whose political endorsement of terrorist acts undermines U.S. antiterrorist efforts; (2) has used a position of prominence to endorse terrorist activity, or to persuade others to support such activity in a way that undermines U.S. antiterrorist efforts (or the child or spouse of such an alien under specified circumstances); or (3) has been associated with a terrorist organization and intends to engage in threatening activities while in the United States.

(Sec. 411) Includes within the definition of "terrorist activity" the use of any weapon or dangerous device.

Redefines "engage in terrorist activity" to mean, in an individual capacity or as a member of an organization, to: (1) commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity; (2) prepare or plan a terrorist activity; (3) gather information on potential targets for terrorist activity; (4) solicit funds or other things of value for a terrorist activity or a terrorist organization (with an exception for lack of knowledge); (5) solicit any individual to engage in prohibited conduct or for terrorist organization membership (with an exception for lack of knowledge); or (6) commit an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training for the commission of a terrorist activity; to any individual who the actor knows or reasonably should know has committed or plans to commit a terrorist activity; or to a terrorist organization (with an exception for lack of knowledge).

Defines "terrorist organization" as a group: (1) designated under the Immigration and Nationality Act or by the Secretary of State; or (2) a group of two or more individuals, whether related or not, which engages in terrorist-related activities.

Provides for the retroactive application of amendments under this Act. Stipulates that an alien shall not be considered inadmissible or deportable because of a relationship to an organization that was not designated as a terrorist organization prior to enactment of this Act. States that the amendments under this section shall apply to all aliens in exclusion or deportation proceedings on or after the date of enactment of this Act.

Directs the Secretary of State to notify specified congressional leaders seven days prior to designating an organization as a terrorist organization. Provides for organization redesignation or revocation.

(Sec. 412) Provides for mandatory detention until removal from the United States (regardless of any relief from removal) of an alien certified by the Attorney General as a suspected terrorist or threat to national security. Requires release of such alien after seven days if removal proceedings have not commenced, or the alien has not been charged with a criminal offense. Authorizes detention for additional periods of up to six months of an alien not likely to be deported in the reasonably foreseeable future only if release will threaten U.S. national security or the safety of the community or any person. Limits judicial review to habeas corpus proceedings in the U.S. Supreme Court, the U.S. Court of Appeals for the District of Columbia, or any district court with jurisdiction to entertain a habeas corpus petition. Restricts to the U.S. Court of Appeals for the District of Columbia the right of appeal of any final order by a circuit or district judge.

(Sec. 413) Authorizes the Secretary of State, on a reciprocal basis, to share criminal- and terrorist-related visa lookout information with foreign governments.

(Sec. 414) Declares the sense of Congress that the Attorney General should: (1) fully implement the integrated entry and exit data system for airports, seaports, and land border ports of entry with all deliberate speed; and (2) begin immediately establishing the Integrated Entry and Exit Data System Task Force. Authorizes appropriations.

Requires the Attorney General and the Secretary of State, in developing the integrated entry and exit data system, to focus on the use of biometric technology and the development of tamper-resistant documents readable at ports of entry.

(Sec. 415) Amends the Immigration and Naturalization Service Data Management Improvement Act of 2000 to include the Office of Homeland Security in the Integrated Entry and Exit Data System Task Force.

(Sec. 416) Directs the Attorney General to implement fully and expand the foreign student monitoring program to include other approved educational institutions like air flight, language training, or vocational schools.

(Sec. 417) Requires audits and reports on implementation of the mandate for machine readable passports.

(Sec. 418) Directs the Secretary of State to: (1) review how consular officers issue visas to determine if consular shopping is a problem; and (2) if it is a problem, take steps to address it, and report on them to Congress.

Subtitle C: Preservation of Immigration Benefits for Victims of Terrorism - Authorizes the Attorney General to provide permanent resident status through the special immigrant program to an alien (and spouse, child, or grandparent under specified circumstances) who was the beneficiary of a petition filed on or before September 11, 2001, to grant the alien permanent residence as an employer-sponsored immigrant or of an application for labor certification if the petition or application was rendered null because of the disability of the beneficiary or loss of employment due to physical damage to, or destruction of, the business of the petitioner or applicant as a direct result of the terrorist attacks on September 11, 2001 (September attacks), or because of the death of the petitioner or applicant as a direct result of such attacks.

(Sec. 422) States that an alien who was legally in a nonimmigrant status and was disabled as a direct result of the September attacks may remain in the United States until his or her normal status termination date or September, 11, 2002. Includes in such extension the spouse or child of such an alien or of an alien who was killed in such attacks. Authorizes employment during such period.

Extends specified immigration-related deadlines and other filing requirements for an alien (and spouse and child) who was directly prevented from meeting such requirements as a result of the September attacks respecting: (1) nonimmigrant status and status revision; (2) diversity immigrants; (3) immigrant visas; (4) parolees; and (5) voluntary departure.

(Sec. 423) Waives, under specified circumstances, the requirement that an alien spouse (and child) of a U.S. citizen must have been married for at least two years prior to such citizen's death in order to maintain immediate relative status if such citizen died as a direct result of the September attacks. Provides for: (1) continued family-sponsored immigrant eligibility for the spouse, child, or unmarried son or daughter of a permanent resident who died as a direct result of such attacks; and (2) continued eligibility for adjustment of status for the spouse and child of an employment-based immigrant who died similarly.

(Sec. 424) Amends the Immigration and Nationality Act to extend the visa categorization of "child" for aliens with petitions filed on or before September 11, 2001, for aliens whose 21st birthday is in September 2001 (90 days), or after September 2001 (45 days).

(Sec. 425) Authorizes the Attorney General to provide temporary administrative relief to an alien who, as of September, 10, 2001, was lawfully in the United States and was the spouse, parent, or child of an individual who died or was disabled as a direct result of the September attacks.

(Sec. 426) Directs the Attorney General to establish evidentiary guidelines for death, disability, and loss of employment or destruction of business in connection with the provisions of this subtitle.

(Sec. 427) Prohibits benefits to terrorists or their family members.

Title V: Removing Obstacles to Investigating Terrorism - Authorizes the Attorney General to pay rewards from available funds pursuant to public advertisements for assistance to DOJ to combat terrorism and defend the Nation against terrorist acts, in accordance with procedures and regulations established or issued by the Attorney General, subject to specified conditions, including a prohibition against any such reward of $250,000 or more from being made or offered without the personal approval of either the Attorney General or the President.

(Sec. 502) Amends the State Department Basic Authorities Act of 1956 to modify the Department of State rewards program to authorize rewards for information leading to: (1) the dismantling of a terrorist organization in whole or significant part; and (2) the identification or location of an individual who holds a key leadership position in a terrorist organization. Raises the limit on rewards if the Secretary State determines that a larger sum is necessary to combat terrorism or defend the Nation against terrorist acts.

(Sec. 503) Amends the DNA Analysis Backlog Elimination Act of 2000 to qualify a Federal terrorism offense for collection of DNA for identification.

(Sec. 504) Amends FISA to authorize consultation among Federal law enforcement officers regarding information acquired from an electronic surveillance or physical search in terrorism and related investigations or protective measures.

(Sec. 505) Allows the FBI to request telephone toll and transactional records, financial records, and consumer reports in any investigation to protect against international terrorism or clandestine intelligence activities only if the investigation is not conducted solely on the basis of activities protected by the first amendment to the U.S. Constitution.

(Sec. 506) Revises U.S. Secret Service jurisdiction with respect to fraud and related activity in connection with computers. Grants the FBI primary authority to investigate specified fraud and computer related activity for cases involving espionage, foreign counter-intelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or restricted data, except for offenses affecting Secret Service duties.

(Sec. 507) Amends the General Education Provisions Act and the National Education Statistics Act of 1994 to provide for disclosure of educational records to the Attorney General in a terrorism investigation or prosecution.

Title VI: Providing for Victims of Terrorism, Public Safety Officers, and Their Families - Subtitle A: Aid to Families of Public Safety Officers - Provides for expedited payments for: (1) public safety officers involved in the prevention, investigation, rescue, or recovery efforts related to a terrorist attack; and (2) heroic public safety officers. Increases Public Safety Officers Benefit Program payments.

Subtitle B: Amendments to the Victims of Crime Act of 1984 - Amends the Victims of Crime Act of 1984 to: (1) revise provisions regarding the allocation of funds for compensation and assistance, location of compensable crime, and the relationship of crime victim compensation to means-tested Federal benefit programs and to the September 11th victim compensation fund; and (2) establish an antiterrorism emergency reserve in the Victims of Crime Fund.

Title VII: Increased Information Sharing for Critical Infrastructure Protection - Amends the Omnibus Crime Control and Safe Streets Act of 1968 to extend Bureau of Justice Assistance regional information sharing system grants to systems that enhance the investigation and prosecution abilities of participating Federal, State, and local law enforcement agencies in addressing multi-jurisdictional terrorist conspiracies and activities. Authorizes appropriations.

Title VIII: Strengthening the Criminal Laws Against Terrorism - Amends the Federal criminal code to prohibit specific terrorist acts or otherwise destructive, disruptive, or violent acts against mass transportation vehicles, ferries, providers, employees, passengers, or operating systems.

(Sec. 802) Amends the Federal criminal code to: (1) revise the definition of "international terrorism" to include activities that appear to be intended to affect the conduct of government by mass destruction; and (2) define "domestic terrorism" as activities that occur primarily within U.S. jurisdiction, that involve criminal acts dangerous to human life, and that appear to be intended to intimidate or coerce a civilian population, to influence government policy by intimidation or coercion, or to affect government conduct by mass destruction, assassination, or kidnapping.

(Sec. 803) Prohibits harboring any person knowing or having reasonable grounds to believe that such person has committed or to be about to commit a terrorism offense.

(Sec. 804) Establishes Federal jurisdiction over crimes committed at U.S. facilities abroad.

(Sec. 805) Applies the prohibitions against providing material support for terrorism to offenses outside of the United States.

(Sec. 806) Subjects to civil forfeiture all assets, foreign or domestic, of terrorist organizations.

(Sec. 808) Expands: (1) the offenses over which the Attorney General shall have primary investigative jurisdiction under provisions governing acts of terrorism transcending national boundaries; and (2) the offenses included within the definition of the Federal crime of terrorism.

(Sec. 809) Provides that there shall be no statute of limitations for certain terrorism offenses if the commission of such an offense resulted in, or created a foreseeable risk of, death or serious bodily injury to another person.

(Sec. 810) Provides for alternative maximum penalties for specified terrorism crimes.

(Sec. 811) Makes: (1) the penalties for attempts and conspiracies the same as those for terrorism offenses; (2) the supervised release terms for offenses with terrorism predicates any term of years or life; and (3) specified terrorism crimes Racketeer Influenced and Corrupt Organizations statute predicates.

(Sec. 814) Revises prohibitions and penalties regarding fraud and related activity in connection with computers to include specified cyber-terrorism offenses.

(Sec. 816) Directs the Attorney General to establish regional computer forensic laboratories, and to support existing laboratories, to develop specified cyber-security capabilities.

(Sec. 817) Prescribes penalties for knowing possession in certain circumstances of biological agents, toxins, or delivery systems, especially by certain restricted persons.

Title IX: Improved Intelligence - Amends the National Security Act of 1947 to require the Director of Central Intelligence (DCI) to establish requirements and priorities for foreign intelligence collected under the Foreign Intelligence Surveillance Act of 1978 and to provide assistance to the Attorney General (AG) to ensure that information derived from electronic surveillance or physical searches is disseminated for efficient and effective foreign intelligence purposes. Requires the inclusion of international terrorist activities within the scope of foreign intelligence under such Act.

(Sec. 903) Expresses the sense of Congress that officers and employees of the intelligence community should establish and maintain intelligence relationships to acquire information on terrorists and terrorist organizations.

(Sec. 904) Authorizes deferral of the submission to Congress of certain reports on intelligence and intelligence-related matters until: (1) February 1, 2002; or (2) a date after February 1, 2002, if the official involved certifies that preparation and submission on February 1, 2002, will impede the work of officers or employees engaged in counterterrorism activities. Requires congressional notification of any such deferral.

(Sec. 905) Requires the AG or the head of any other Federal department or agency with law enforcement responsibilities to expeditiously disclose to the DCI any foreign intelligence acquired in the course of a criminal investigation.

(Sec. 906) Requires the AG, DCI, and Secretary of the Treasury to jointly report to Congress on the feasibility and desirability of reconfiguring the Foreign Asset Tracking Center and the Office of Foreign Assets Control to provide for the analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations.

(Sec. 907) Requires the DCI to report to the appropriate congressional committees on the establishment and maintenance of the National Virtual Translation Center for timely and accurate translation of foreign intelligence for elements of the intelligence community.

(Sec. 908) Requires the AG to provide a program of training to Government officials regarding the identification and use of foreign intelligence.

Title X: Miscellaneous - Directs the Inspector General of the Department of Justice to designate one official to review allegations of abuse of civil rights, civil liberties, and racial and ethnic profiling by government employees and officials.

(Sec. 1002) Expresses the sense of Congress condemning acts of violence or discrimination against any American, including Sikh-Americans. Calls upon local and Federal law enforcement authorities to prosecute to the fullest extent of the law all those who commit crimes.

(Sec. 1004) Amends the Federal criminal code with respect to venue in money laundering cases to allow a prosecution for such an offense to be brought in: (1) any district in which the financial or monetary transaction is conducted; or (2) any district where a prosecution for the underlying specified unlawful activity could be brought, if the defendant participated in the transfer of the proceeds of the specified unlawful activity from that district to the district where the financial or monetary transaction is conducted.

States that: (1) a transfer of funds from one place to another, by wire or any other means, shall constitute a single, continuing transaction; and (2) any person who conducts any portion of the transaction may be charged in any district in which the transaction takes place.

Allows a prosecution for an attempt or conspiracy offense to be brought in the district where venue would lie for the completed offense, or in any other district where an act in furtherance of the attempt or conspiracy took place.

(Sec. 1005) First Responders Assistance Act - Directs the Attorney General to make grants to State and local governments to improve the ability of State and local law enforcement, fire department, and first responders to respond to and prevent acts of terrorism. Authorizes appropriations.

(Sec. 1006) Amends the Immigration and Nationality Act to make inadmissible into the United States any alien engaged in money laundering. Directs the Secretary of State to develop a money laundering watchlist which: (1) identifies individuals worldwide who are known or suspected of money laundering; and (2) is readily accessible to, and shall be checked by, a consular or other Federal official before the issuance of a visa or admission to the United States.

(Sec. 1007) Authorizes FY 2002 appropriations for regional antidrug training in Turkey by the Drug Enforcement Administration for police, as well as increased precursor chemical control efforts in South and Central Asia.

(Sec. 1008) Directs the Attorney General to conduct a feasibility study and report to Congress on the use of a biometric identifier scanning system with access to the FBI integrated automated fingerprint identification system at overseas consular posts and points of entry to the United States.

(Sec. 1009) Directs the FBI to study and report to Congress on the feasibility of providing to airlines access via computer to the names of passengers who are suspected of terrorist activity by Federal officials. Authorizes appropriations.

(Sec. 1010) Authorizes the use of Department of Defense funds to contract with local and State governments, during the period of Operation Enduring Freedom, for the performance of security functions at U.S. military installations.

(Sec. 1011) Crimes Against Charitable Americans Act of 2001 - Amends the Telemarketing and Consumer Fraud and Abuse Prevention Act to cover fraudulent charitable solicitations. Requires any person engaged in telemarketing for the solicitation of charitable contributions, donations, or gifts to disclose promptly and clearly the purpose of the telephone call.

(Sec. 1012) Amends the Federal transportation code to prohibit States from licensing any individual to operate a motor vehicle transporting hazardous material unless the Secretary of Transportation determines that such individual does not pose a security risk warranting denial of the license. Requires background checks of such license applicants by the Attorney General upon State request.

(Sec. 1013) Expresses the sense of the Senate on substantial new U.S. investment in bioterrorism preparedness and response.

(Sec. 1014) Directs the Office for State and Local Domestic Preparedness Support of the Office of Justice Programs to make grants to enhance State and local capability to prepare for and respond to terrorist acts. Authorizes appropriations for FY 2002 through 2007.

(Sec. 1015) Amends the Crime Identification Technology Act of 1998 to extend it through FY 2007 and provide for antiterrorism grants to States and localities. Authorizes appropriations.

(Sec. 1016) Critical Infrastructures Protection Act of 2001 - Declares it is U.S. policy: (1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and U.S. national security; (2) that actions necessary to achieve this policy be carried out in a public-private partnership involving corporate and non-governmental organizations; and (3) to have in place a comprehensive and effective program to ensure the continuity of essential Federal Government functions under all circumstances.

Establishes the National Infrastructure Simulation and Analysis Center to serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation.

Defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Authorizes appropriations.

■

Appendix B: USA FREEDOM Act of 2015 Summary

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 or the USA FREEDOM Act of 2015

TITLE I--FISA BUSINESS RECORDS REFORMS

(Sec. 101) Amends the Foreign Intelligence Surveillance Act of 1978 (FISA) to establish a new process to be followed when the Federal Bureau of Investigation (FBI) submits an application to a FISA court for an order requiring the production of business records or other tangible things for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. (The FBI currently uses such authority to request FISA orders requiring telephone companies to produce telephone call records to the National Security Agency.)

Prohibits the FBI from applying for a tangible thing production order unless a specific selection term is used as the basis for the production. Maintains limitations under current law that prohibit the FBI from applying for tangible thing production orders for threat assessments.

Establishes two separate frameworks for the production of tangible things with different standards that apply based on whether the FBI's application seeks:

- production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation to protect against international terrorism, in which case the specific selection term must specifically identify an individual, account, or personal device; or
- production of call detail records or other tangible things in any other manner, in which case the selection term must specifically identify an individual, a federal officer or employee, a group, an entity, an association, a corporation, a foreign power, an account, a physical or an electronic address, a personal device, or any other specific identifier but is prohibited from including, when not used as part of a specific identifier, a broad geographic region (including the United States, a city, county, state, zip code, or area code) or an electronic communication or remote computing service provider, unless the provider is itself a subject of an authorized investigation.

Defines "call detail record" as session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call. Excludes from such definition: (1) the contents of any communication; (2) the name, address, or financial information of a subscriber or customer; or (3) cell site location or global positioning system information.

Requires the FBI, in applications for ongoing production of call detail records for investigations to protect against international terrorism, to show: (1) reasonable grounds to believe that the call detail records are relevant to such investigation; and (2) a reasonable, articulable suspicion that the specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation for such terrorism.

Requires a judge approving such an ongoing release of call detail records for an investigation to protect against international terrorism to:

- limit such production to a period not to exceed 180 days but allow such orders to be extended upon application, with FISA court approval;
- permit the government to require the production of an initial set of call records using the reasonable, articulable suspicion standard that the term is associated with a foreign power or an agent of a foreign power and then a subsequent set of call records using session-identifying information or a telephone calling card number identified by the specific selection term that was used to produce the initial set of records (thus limiting the government to what is commonly referred to as two "hops" of call records); and
- direct the government to adopt minimization procedures requiring prompt destruction of produced call records that are not foreign intelligence information.

Allows a FISA court to approve other categories of FBI requests for the production of call detail records or tangible things (i.e., FBI call detail record and tangible thing applications that do not seek ongoing production of call detail records created before, on, or after the date of an application relating to an authorized investigation to protect against international terrorism) without subjecting the production to:

(1) the reasonable, articulable suspicion standard for an association with a foreign power or an agent of a foreign power; (2) the 180-day or the two-hop limitation; or (3) the special minimization procedures that require prompt destruction of produced records only if the order approves an ongoing production of call detail records for investigations to protect against international terrorism.

(Sec. 102) Authorizes the Attorney General to require the emergency production of tangible things without first obtaining a court order if the Attorney General: (1) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing production can be obtained with due diligence, (2) reasonably determines that a factual basis exists for the issuance of such a production order, (3) informs a FISA judge of the decision to require such production at the time the emergency decision is made, and (4) makes an application to a FISA judge within seven days after the Attorney General requires such emergency production.

Terminates the authority for such emergency production of tangible things when the information sought is obtained, when the application for the order is denied, or after the expiration of seven days from the time the Attorney General begins requiring such emergency production, whichever is earliest.

Prohibits information obtained or evidence derived from such an emergency production from being received in evidence or disclosed in any proceeding in or before any court, grand jury, agency, legislative committee, or other authority of the United States, any state, or any political subdivision if: (1) the subsequent application for court approval is denied, or (2) the production is terminated and no order is issued approving the production. Bars information concerning any U.S. person acquired from such production from being used or disclosed in any other manner by federal officers or employees without the consent of such person, except with approval of the Attorney General if the information indicates a threat of death or serious bodily harm.

(Sec. 103) Requires FISA court orders approving the production of tangible things to include each specific selection term used as the basis for such production. Prohibits FISA courts from authorizing the collection of tangible things without the use of a specific selection term.

(Sec. 104) Requires a FISA court, as a condition to approving an application for a tangible thing production order, to find that the minimization procedures submitted with the application meet applicable FISA standards. Authorizes the court to impose additional minimization procedures.

Allows a nondisclosure order imposed in connection with a tangible thing production order to be challenged immediately by filing a petition for judicial review. (Currently, such a tangible thing nondisclosure order cannot be challenged until one year after the issuance of the production order.) Removes a requirement that a judge considering a petition to modify or set aside a nondisclosure order treat as conclusive a certification by the Attorney General, the Deputy Attorney General, an Assistant Attorney General, or the FBI Director that disclosure may endanger national security or interfere with diplomatic relations.

(Sec. 105) Extends liability protections to persons who provide information, facilities, or technical assistance for the production of tangible things. (Currently, liability protections are limited to persons who produce such tangible things.)

(Sec. 106) Requires the government to compensate a person for reasonable expenses incurred in producing tangible things or providing technical assistance to the government to implement production procedures.

(Sec. 108) Amends the USA PATRIOT Improvement and Reauthorization Act of 2005 to require the Inspector General of the Department of Justice to audit the effectiveness and use of FISA authority to obtain production of tangible things from 2012 to 2014, including an examination of whether minimization procedures adopted by the Attorney General adequately protect the constitutional rights of U.S. persons. Directs the Inspector General of the Intelligence Community, for the same 2012-2014 period, to assess: (1) the importance of such information to the intelligence community; (2) the manner in which such information was collected, retained, analyzed, and disseminated; and (3) the adequacy of minimization procedures, including an assessment of any minimization procedures proposed by an element of the intelligence community that were modified or denied by the court.

Requires such Inspectors General to report to Congress regarding the results of such audit and assessment.

(Sec. 109) Requires amendments made by this Act to FISA's tangible thing requirements to take effect 180 days after enactment of this Act. Prohibits this Act from being construed to alter or eliminate the government's authority to obtain an order under the tangible things requirements of FISA as in effect prior to the effective date of such amendments during the period ending on such effective date.

(Sec. 110) Prohibits this Act from being construed to authorize the production of the contents of any electronic communication from an electronic communication service provider under such tangible thing requirements.

TITLE II--FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

(Sec. 201) Requires the government's FISA applications for orders approving pen registers or trap and trace devices to include a specific selection term as the basis for the use of the register or device. Prohibits broad geographic regions or an identification of an electronic communications service or a remote computing service from serving as such selection term.

(Sec. 202) Directs the Attorney General to ensure that appropriate privacy procedures are in place for the collection, retention, and use of nonpublicly available information concerning U.S. persons that is collected through a pen register or trap and trace device installed with FISA court approval.

TITLE III--FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

(Sec. 301) Limits the government's use of information obtained through an authorization by the Attorney General and the Director of National Intelligence (DNI) to target non-U.S. persons outside the United States if a FISA court later determines that certain targeting or minimization procedures certified to the court are unlawful.

Prohibits information obtained or evidence derived from an acquisition pursuant to a part of a targeting certification or a related minimization procedure that the court has identified as deficient concerning a U.S. person from being received in evidence or

otherwise disclosed in any proceeding in or before any court, grand jury, agency, legislative committee, or other authority of the United States, any state, or any political subdivision.

Bars information concerning any U.S. person acquired pursuant to a deficient part of a certification from being used or disclosed subsequently in any other manner by federal officers or employees without the consent of the U.S. person, except with approval of the Attorney General if the information indicates a threat of death or serious bodily harm.

Allows a FISA court, if the government corrects the deficiency, to permit the use or disclosure of information obtained before the date of the correction.

TITLE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

(Sec. 401) Directs the presiding judges of the FISA court and the FISA court of review to jointly designate at least five individuals to serve as amicus curiae to assist in the consideration of any application for an order or review that presents a novel or significant interpretation of the law, unless the court finds that such appointment is not appropriate.

Permits FISA courts to appoint an individual or organization to serve as amicus curiae in other instances, including to provide technical expertise. Requires such amicus curiae to provide: (1) legal arguments that advance protection of individual privacy and civil liberties, or (2) other legal arguments or information related to intelligence collection or communications technology.

Allows the FISA court of review to certify a question of law to be reviewed by the Supreme Court. Permits the Supreme Court to appoint FISA amicus curiae or other persons to provide briefings or other assistance upon such a certification.

(Sec. 402) Requires the DNI to: (1) conduct a declassification review of each decision, order, or opinion issued by the FISA court or the FISA court of review that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of "specific selection term" as defined in this Act; and (2) make such decisions, orders, or opinions publicly available to the greatest extent practicable, subject to permissible redactions.

Authorizes the DNI to waive such review and public availability requirements if: (1) a waiver is necessary to protect the national security of the United States or properly classified intelligence sources or methods, and (2) an unclassified statement prepared by the Attorney General is made publicly available to summarize the significant construction or interpretation of law.

TITLE V--NATIONAL SECURITY LETTER REFORM

(Sec. 501) Amends the federal criminal code, the Right to Financial Privacy Act of 1978, and the Fair Credit Reporting Act to require the FBI and other government agencies to use a specific selection term as the basis for national security letters that request information from wire or electronic communication service providers, financial institutions, or consumer reporting agencies. Requires the government to identify: (1) a person, entity, telephone number, or account for requests for telephone toll and transactional records; (2) a customer, entity, or account when requesting financial records for certain intelligence or protective functions; or (3) a consumer or account when requesting consumer reports for counterintelligence or counterterrorism purposes.

Revises standards under which the government can prohibit recipients of national security letters from disclosing to anyone that the government has sought or obtained access to the requested information.

(Sec. 502) Directs the Attorney General to adopt procedures for imposed nondisclosure requirements, including requirements under the National Security Act of 1947, to be reviewed at appropriate intervals and terminated if facts no longer support nondisclosure.

Removes a requirement that the court treat as conclusive a certification by the Attorney General, the Deputy Attorney General, an Assistant Attorney General, or the FBI Director that disclosure may endanger U.S. national security or interfere with diplomatic relations.

(Sec. 503) Allows national security letter recipients to challenge national security letter requests or nondisclosure requirements under modified procedures for filing a petition for judicial review.

TITLE VI--FISA TRANSPARENCY AND REPORTING REQUIREMENTS

(Sec. 601) Requires the Attorney General to expand an annual report to Congress regarding tangible thing applications to include a summary of compliance reviews and the total number of: (1) applications made for the daily production of call detail records created before, on, or after the date of an application relating to an authorized investigation to protect against international terrorism; and (2) orders approving such requests.

Directs the Attorney General to report to Congress annually regarding tangible things applications and orders in which the specific selection term does not specifically identify an individual, account, or personal device. Requires the report to indicate whether the court approving such orders has directed additional, particularized minimization procedures beyond those adopted by the Attorney General.

(Sec. 602) Directs the Administrative Office of the U.S. Courts to submit annually to Congress the number of: (1) FISA applications submitted and orders granted, modified, or denied under specified FISA authorities; and (2) appointments of an individual to serve as amicus curiae for FISA courts, including the name of each appointed individual, as well as any findings that such an appointment is not appropriate. Makes the report subject to a declassification review by the Attorney General and the DNI.

Directs the DNI to make available publicly a report that identifies, for the preceding 12-month period, the total number of: (1) FISA court orders issued for electronic surveillance, physical searches, the targeting of persons outside the United States, pen registers and trap and trace devices, call detail records, and other tangible things; and (2) national security letters issued.

Requires the DNI's reports to include the estimated number of: (1) targets of certain FISA orders, (2) search terms and queries concerning U.S. persons when the government retrieves information from electronic or wire communications obtained by targeting non-U.S. persons outside the United States, (3) unique identifiers used to communicate certain collected information, and (4) search terms concerning U.S. persons used to query a database of call detail records. Exempts certain queries by the FBI from such estimates.

(Sec. 603) Permits a person who is subject to a nondisclosure requirement accompanying a FISA order, directive, or national security letter to choose one of four methods to report publicly, on a semiannual or annual basis, the aggregate number of orders, directives, or letters with which the person was required to comply. Specifies the categories of orders, directives, and letters to be itemized or combined, the details authorized to be included with respect to contents or noncontents orders and the number of customer selectors targeted, and the ranges within which the number of orders, directives, or letters received may be reported aggregately in bands under each permitted method (i.e., reported in bands of 1000, 500, 250, or 100 depending on the chosen method).

Requires the information that may be included in certain aggregates to be delayed by 180 days, one year, or 540 days depending on the chosen reporting method and whether the nondisclosure requirements are contained in a new order or directive concerning a platform, product, or service for which the person did not previously receive an order or directive.

(Sec. 604) Expands the categories of FISA court decisions, orders, or opinions that the Attorney General is required to submit to Congress within 45 days after issuance of the decision to include: (1) a denial or modification of an application under FISA; and (2) a change of the application, or a novel application, of any FISA provision. (Currently, the Attorney General is only required to submit only decisions regarding a significant construction or interpretation of any FISA provision.)

(Sec. 605) Revises reporting requirements regarding electronic surveillance, physical searches, and tangible things to include the House Judiciary Committee as a recipient of such reports.

Requires the Attorney General to identify in an existing semiannual report each agency on behalf of which the government has applied for orders authorizing or approving the installation and use of pen registers or trap and trace devices under FISA.

TITLE VII--ENHANCED NATIONAL SECURITY PROVISIONS

(Sec. 701) Establishes procedures for a lawfully authorized targeting of a non-U.S. person previously believed to be located outside the United States to continue for a period not to exceed 72 hours from the time that the non-U.S. person is reasonably believed to be located inside the United States. Requires an element of the intelligence

community, as a condition to exercising such authority, to: (1) determine that a lapse in the targeting poses a threat of death or serious bodily harm; (2) notify the Attorney General; and (3) request, as soon as practicable, the employment of emergency electronic surveillance or emergency physical search under appropriate FISA standards.

(Sec. 702) Expands the definition of "agent of a foreign power" to include a non-U.S. person who: (1) acts in the United States for or on behalf of a foreign power engaged in clandestine intelligence activities in the United States contrary to U.S. interests or as an officer, employee, or member of a foreign power, irrespective of whether the person is inside the United States; or (2) knowingly aids, abets, or conspires with any person engaging in an international proliferation of weapons of mass destruction on behalf of a foreign power or conducting activities in preparation for such proliferation.

(Sec. 704) Increases from 15 to 20 years the maximum penalty of imprisonment for providing material support or resources to a foreign terrorist organization in cases where the support does not result in the death of any person.

(Sec. 705) Amends the USA PATRIOT Improvement and Reauthorization Act of 2005 and the Intelligence Reform and Terrorism Prevention Act of 2004 to extend until December 15, 2019, FISA authorities concerning: (1) the production of business records, including call detail records and other tangible things; (2) roving electronic surveillance orders; and (3) a revised definition of "agent of a foreign power" that includes any non-U.S. persons who engage in international terrorism or preparatory activities (commonly referred to as the "lone wolf" provision). (Currently, such provisions are scheduled to expire on June 1, 2015.)

TITLE VIII--SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A--Safety of Maritime Navigation

(Sec. 801) Amends the federal criminal code to provide that existing prohibitions against conduct that endangers the safe navigation of a ship: (1) shall apply to conduct that is committed against or on board a U.S. vessel or a vessel subject to U.S. jurisdiction, in U.S. territorial seas, or by a U.S. corporation or legal entity; and (2) shall not apply to activities of armed forces during an armed conflict or in the exercise of official duties.

Sets forth procedures regarding the delivery of a person who is suspected of committing a maritime navigation or fixed platform offense to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation.

Subjects property used or intended to be used to commit or to facilitate the commission of a maritime navigation offense to civil forfeiture.

(Sec. 802) Prohibits: (1) using in or on a ship or a maritime fixed platform any explosive or radioactive material, biological, chemical, or nuclear weapon, or other nuclear explosive device in a manner likely to cause death or serious injury or damage when the purpose is to intimidate a population or to compel a government or international organization to act or abstain from acting; (2) transporting on board a ship such material or device (or certain related material or technology) that is intended for such use, with specified exceptions; (3) transporting on board a ship a person known to have committed a maritime navigation offense intending to assist such person to evade prosecution; (4) injuring or killing any person in connection with such an offense; or (5) conspiring, attempting, or threatening to commit such an offense. Sets forth: (1) the circumstances in which the United States can exercise jurisdiction over such offenses, and (2) exceptions applicable to activities of the armed forces. Provides for civil forfeiture of property used to commit or to facilitate a violation.

(Sec. 805) Includes offenses involving violence against maritime navigation and maritime transport involving weapons of mass destruction within the definition of "federal crime of terrorism."

Subtitle B--Prevention of Nuclear Terrorism

(Sec. 811) Prohibits anyone, knowingly, unlawfully, and with intent to cause death, serious bodily injury, or substantial damage to property or the environment, from: (1) possessing radioactive material or making or possessing a nuclear explosive device or a radioactive material dispersal or radiation-emitting device; (2) using radioactive material or a device, using, damaging, or interfering with the operation of a nuclear facility in a manner that causes or increases the risk of the release of radioactive material, or causing radioactive contamination or exposure to radiation; or (3) threatening, attempting, or conspiring to commit such an offense. Sets forth: (1) the circumstances in which the United States can exercise jurisdiction over such offenses, and (2) exceptions applicable to activities of the armed forces.

Includes such offenses within the definition of "federal crime of terrorism."

(Sec. 812) Amends provisions prohibiting transactions involving nuclear materials to: (1) prohibit, intentionally and without lawful authority, carrying, sending, or moving nuclear material into or out of a country; and (2) establish an exception for activities of the armed forces.

■

Appendix C: Material Submitted for the House Judiciary Committee Hearing Record

Questions for the Record submitted to James Cole, United States Department of Justice; Robert S. Litt, Office of Director of National Intelligence; John C. Inglis, National Security Agency; and Stephanie Douglas, FBI National Security Branch*

Questions for the Record from Representative Steve Cohen (TN-09)

For: Mr. James Cole, United States Department of Justice;
Mr. John C. Inglis, National Security Agency;
Mr. Robert S. Litt, Office of Director of National Intelligence; and
Ms. Stephanie Douglas, National Security Branch, Federal Bureau of Investigation

FISA Court

Throughout the hearing, you assured the Committee that the surveillance programs that Members expressed concerns about are legal and proper, in large part because the Foreign Intelligence Surveillance Court, or FISA Court, has ruled that they are. However, it is critical the Members have a fuller understanding of how this court operates and who sits on the court since we entrust it to make such important decisions about the proper balance between national security and personal privacy.

1. In the last five years, how many of the FISA Court's decisions, orders, and opinions were made by only one judge acting alone?
2. How many of these decisions, orders and opinions were made by a three-judge panel?
3. How many of these decisions, orders and opinions were made by the court acting *en banc*?
4. How many cases were appealed to the Foreign Intelligence Surveillance Court of Review?
5. When the FISA Court acts as a three-judge panel or *en banc* or the Foreign Intelligence Surveillance Court of Review hears cases, is a simple majority sufficient to issue an order or decision?
6. How many dissents were issued by judges acting in a three-judge panel, *en banc*, or on the Foreign Intelligence Surveillance Court of Review?
7. Given the enormous power that the Government seeks when obtaining permission from the FISA Court, shouldn't there be a third party specifically assigned to argue against the Government so that the Court can hear the other side?
8. Wouldn't the public be more accepting of the programs you are defending if they could read at least a summary of the FISA Court's decisions? Would you support publishing unclassified summaries of these decisions?
9. Under current law, the FISA Court need only deliver to Congress those decisions, orders, and opinions that involve a "significant construction or interpretation" of law. Who determines what is a significant construction or interpretation of law and what will be transmitted to Congress?

*The Committee had not received a response to these questions at the time this hearing record was finalized and submitted for printing on December 12, 2013.

137

Privacy and Civil Liberties Oversight Board

Back in 2004, this Committee's Subcommittee on Commercial and Administrative Law spearheaded the effort to create the Privacy and Civil Liberties Oversight Board.

After some reorganization and confirmation of its chairman, it is now up and running and has held a number of hearings and have issued its semi-annual report.

1. To what extent have your agencies been working with the Board to ensure that intelligence programs do not unduly infringe on privacy and civil liberties?

2. Will you commit to working closely and cooperatively with the board going forward?

Response to Questions from the Hearing from Stewart A. Baker, Steptoe & Johnson, LLP

Oversight Hearing on the Administration's use of FISA Authorities
Committee on the Judiciary

United States House of Representatives

Held July 17, 2013

September 13, 2013 Response to Supplemental Question by Stewart A. Baker
Partner, Steptoe & Johnson LLP

Question:

> Mr. GOHMERT. . . . But I would like to ask the witnesses if you have any proposals, if you could provide them in writing to us, any alternatives, any major changes, because I think this justifies major changes.

Response:

It is becoming increasingly obvious from the nature of the documents that have been leaked that Mr. Snowden and some of those working with him are quite prepared to release material that harms U.S. security, even when the material reveals no misconduct. While it is always useful to periodically review oversight mechanisms like the FISA court, in the present climate, I would caution against radically changing how we provide oversight of foreign intelligence surveillance. To respond in knee-jerk fashion to revelations that may be more advocacy than journalism would make bad law and reward Mr. Snowden's illegal actions.

Response to Questions for the Record from Jameel Jaffer, American Civil Liberties Union (ACLU)

Answers to Questions for the Record of
The House Judiciary Committee

Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Laura W. Murphy
Director, Washington Legislative Office
American Civil Liberties Union

NSA Data Collection and Surveillance Oversight

July 17, 2013

QUESTION FROM REP. STEVE COHEN

Are there ways to enhance the role of the Privacy and Civil Liberties Oversight Board so as to ensure a better balance between legitimate national security needs on the one hand and privacy, civil liberties, and public transparency on the other?

Congress should enhance the PCLOB in at least four ways in order to ensure that the Board plays a meaningful role in overseeing the impact of government policies on privacy, civil liberties, and public transparency. First, Congress should grant the Board the authority to challenge the classification decisions of other agencies when it finds reason to believe classification powers have been abused to cover up wrongdoing, to prevent embarrassment, or to stifle legitimate public debate. Second, the Board should enjoy a set of enforcement powers that could be used to implement its recommendations. Third, Congress must ensure that the Board is given sufficient resources—in terms of both staff and budget—to pursue its mandate on an ongoing basis. And finally, assuming all three prior enhancements have been achieved, Congress should consider broadening the Board's mandate so that its oversight authority ranges to other areas of policymaking such as certain law enforcement programs that raise serious privacy and civil-liberties issues. In broadening the mandate, however, it is critically important not to dilute the time, attention and resources devoted to counterterrorism programs.

Response to Questions from the Hearing and for the Record from Kate Martin, Center for National Security Studies

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

Answers from Kate Martin to Members' questions from the hearing on July 17, 2013 and for the record.

Representative Goodlatte (p. 122):

"Let me turn to Ms. Martin, however, and your testimony includes a number of suggestions for increasing the visibility into the – increasing visibility into the FISA programs. Which of these would you prioritize as a way to both preserve our national security efforts while also giving the public a better understanding of how the programs work?

Since the hearing, the government has disclosed additional opinions by the FISC court and a White Paper concerning the 215 program, which disclosures are welcome and useful. Nevertheless, we still do not have a complete understanding of the FISA court's views on the law, nor of the executive's interpretation of the law. Accordingly, I would prioritize obtaining disclosure of the following information:

1. All FISA court opinions concerning the law, including those authorizing bulk collection of internet meta-data, and the government's pleadings containing legal arguments submitted to the court. Any operational details which are still a secret could be redacted from these documents.
2. In light of the government's disclosure of the 215 program, there should be a new declassification review and public release of the Inspectors Generals' report required by the FISA Amendments Act (Report on the President's Surveillance Program, Offices of the Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, July 10, 2009. Unclassified version available at http://www.justice.gov/oig/special/s0907.pdf). This report is crucial for understanding the legal history and scope of the current surveillance programs.
3. Equally important, this Committee should demand a *comprehensive public report* from the Executive Branch concerning government collection of information about Americans for national security or foreign intelligence purposes. The report should detail:
    - the overlapping authorities for collection of information about Americans' communications, e.g., national security letter authorities, pen register/trap and trace authorities, other FISA authorities;
    - the rules governing accessing, analyzing, data-mining, keeping, using or disseminating information concerning Americans' communications;

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 cnss@cnss.org

- in addition to existing authorities, the report should identify existing prohibitions, if any, on collecting or data-mining information on Americans, and all restrictions, if any, on sharing information with the White House, including the National Security Council, or foreign governments;
- which agencies may exercise which authorities and what information may be may be shared between each agency; and
- the scope of the collection of Americans' personal information, including the kinds of information, the amount of information collected and the approximate number of Americans whose information has been collected.

Representative Gohmert (p. 125-126):

"I have now seen the incredible abuse by the FISA court, in my opinion, and I am just wondering if we are better off going to a system where we don't require a FISA court. There is not this Star Chamber. What would be another alternative?"

. . .

"But I would ask the witnesses if you have any proposals, if you could provide that in writing to us, any alternatives, any major changes, because I think this justifies major changes."

Since its creation, the FISA court has issued particularized orders based on a finding of probable cause and those authorities do not raise the concerns you have articulated. I would urge the Congress, however, to examine carefully whether the new authorities, in particular the FISA Amendments Act, section 702 of the FISA, which do not require any particularity in collection activities, but are specifically intended to collect information on Americans, (even though they may not be technically "targeted") should be limited or repealed. Doing so would address some of the more problematic authorities of the FISA court. *As a first step, Congress should shorten the current sunset for those authorities from the current date of 2017 to align with the current mid 2015 sunset date for section 215.* In addition, Congress should amend section 215 to make clear that it does not authorize bulk collection of information on Americans.

There have been some proposals to provide for an "independent" advocate to participate in the secret proceedings before the FISA court. Such an advocate might prove helpful to the judges on the court, who do not have the benefit of briefing by two parties. (FISA court judges could perhaps be consulted on how helpful such a position would be.) But providing such an advocate would be no substitute for reinstating *public adversarial* judicial review. The essence of judicial review of the legality of the government's action is that such review is transparent, a court acts openly, and that the individual whose rights are at stake participates in the proceeding. The current proposals would not address either of these key requirements—transparency or adversarialness -- for restoring real judicial review.

Accordingly, this Committee should examine other ways to provide adversarial judicial review of individual instances of foreign intelligence surveillance. Such judicial review could like judicial review of searches and seizure done for law enforcement purposes, take place after the fact, when the surveillance is finished. While the original FISA contained a provision for such review, 50 U.S.C. 1806, that provision does not apply to all current collection authorities under FISA. Moreover, it has not proved sufficient to provide a real opportunity for a subject of surveillance to challenge the surveillance in an open and adversarial proceeding before a judge.

Representative Nadler (p. 127):

"Ms. Martin, how can we—how can Congress solve the problem? We have a basic problem. Every challenge to abuse of constitutional rights by the Bush administration and the Obama administration has been met in the same way. Either the use of the state secrets doctrine to say you can't go to a court on that. The subject matter of the discussion is a state secret. Therefore, move to dismiss the case ab initio. Or you have no standing because you cannot prove that you personally were harmed by this.

Now Mr. Snowden may have done a public service in giving some people standing by proving that they were harmed by this because anyone who is a Verizon subscriber arguable can no go into court and say that. How can we deal with these two problems that an administration, any administration can violate constitutional rights from here to kingdom come, subject to no court review because of either the state secrets doctrine or the standing problems because they don't admit what they are doing in the first place. It is secret.

It is secret what we are doing to you. Therefore, you have no standing because you can't prove what we are doing to you."

There are several steps the Congress could take to ameliorate the problem that individuals cannot challenge the government's actions against them in court, when the government refuses to acknowledge its activities and claims that the state secrets privilege or other doctrine prevents litigation.

First, the Congress should insist on public disclosure of information concerning the government's activities. In addition to public disclosure concerning the legal authorities and scope of surveillance programs generally, Congress should also require investigation of specific instances of surveillance, where there are credible allegations that individual rights have been violated, either by congressional committees, an inspector general or other body. That investigation could then inform additional public disclosures concerning questionable instances of government surveillance. And those disclosures in turn would facilitate judicial challenges by the affected individuals. In particular, the government would not be able to seek dismissal of such challenges on state secrets grounds, because the information relevant to pursuing the case would be public.

In addition, I would urge the Congress to examine the possibility of creating a statutory cause of action for violation of an individual's constitutional rights. Doing so would make it more difficult for the government to secure dismissal of a challenge on technical grounds, and help insure that the court considers the merits of whether the government has violated someone's rights.

Representative Cohen:

"Are there ways to enhance the role of the Privacy and Civil Liberties Oversight Board so as to ensure a better balance between legitimate national security needs on the one hand and privacy, civil liberties and public transparency on the other?"

Congress should ensure that the Privacy and Civil Liberties Oversight Board receives adequate funding to enable it to carry out its statutory mandate. At the same time, the Congress and the federal courts have the ultimate constitutional responsibility for ensuring privacy, civil liberties and public transparency while protecting the national security.

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

The Honorable Bob Goodlatte
Chair
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Goodlatte,

Thank you for the opportunity to testify before the Committee at its hearing on oversight of the Administration's Use of FISA Authorities, Wednesday, July 17, 2013. Enclosed please find written answers to the Members' questions asked during the hearing and for the record.

Sincerely,

Kate Martin
Director

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 cnss@cnss.org

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

Answers from Kate Martin to Members' questions from the hearing on July 17, 2013 and for the record.

Representative Goodlatte (p. 178-179):

"Let me turn to Ms. Martin, however, and your testimony includes a number of suggestions for increasing the visibility into the – increasing visibility into the FISA programs. Which of these would you prioritize as a way to both preserve our national security efforts while also giving the public a better understanding of how the programs work?

Since the hearing, the government has disclosed additional opinions by the FISC court and a White Paper concerning the 215 program, which disclosures are welcome and useful. Nevertheless, we still do not have a complete understanding of the FISA court's views on the law, nor of the executive's interpretation of the law. Accordingly, I would prioritize obtaining disclosure of the following information:

1. All FISA court opinions concerning the law, including those authorizing bulk collection of internet meta-data, and the government's pleadings containing legal arguments submitted to the court. Any operational details which are still a secret could be redacted from these documents.
2. In light of the government's disclosure of the 215 program, there should be a new declassification review and public release of the Inspectors Generals' report required by the FISA Amendments Act (Report on the President's Surveillance Program, Offices of the Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, July 10, 2009. Unclassified version available at http://www.justice.gov/oig/special/s0907.pdf). This report is crucial for understanding the legal history and scope of the current surveillance programs.
3. Equally important, this Committee should demand a *comprehensive public report* from the Executive Branch concerning government collection of information about Americans for national security or foreign intelligence purposes. The report should detail:

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 cnss@cnss.org

147

- the overlapping authorities for collection of information about Americans' communications, e.g., national security letter authorities, pen register/trap and trace authorities, other FISA authorities;
- the rules governing accessing, analyzing, data-mining, keeping, using or disseminating information concerning Americans' communications;
- in addition to existing authorities, the report should identify existing prohibitions, if any, on collecting or data-mining information on Americans, and all restrictions, if any, on sharing information with the White House, including the National Security Council, or foreign governments;
- which agencies may exercise which authorities and what information may be may be shared between each agency; and
- the scope of the collection of Americans' personal information, including the kinds of information, the amount of information collected and the approximate number of Americans whose information has been collected.

Representative Gohmert (p. 186 -87):

"I have now seen the incredible abuse by the FISA court, in my opinion, and I am just wondering if we are better off going to a system where we don't require a FISA court. There is not this Star Chamber. What would be another alternative?"

. . .

"But I would ask the witnesses if you have any proposals, if you could provide that in writing to us, any alternatives, any major changes, because I think this justifies major changes."

Since its creation, the FISA court has issued particularized orders based on a finding of probable cause and those authorities do not raise the concerns you have articulated. I would urge the Congress, however, to examine carefully whether the new authorities, in particular the FISA Amendments Act, section 702 of the FISA, which do not require any particularity in collection activities, but are specifically intended to collect information on Americans, (even though they may not be technically "targeted") should be limited or repealed. Doing so would address some of the more problematic authorities of the FISA court. *As a first step, Congress should shorten the current sunset for those authorities from the current date of 2017 to align with the current mid 2015 sunset date for section 215.* In addition, Congress should amend section 215 to make clear that it does not authorize bulk collection of information on Americans.

There have been some proposals to provide for an "independent" advocate to participate in the secret proceedings before the FISA court. Such an advocate might prove helpful to the judges on the court, who do not have the benefit of briefing by two parties. (FISA court judges could perhaps be consulted on how helpful such a position would be.) But providing such an advocate would be no substitute for reinstating *public adversarial* judicial review. The essence of judicial review of the legality of the government's action is that such review is transparent, a

court acts openly, and that the individual whose rights are at stake participates in the proceeding. The current proposals would not address either of these key requirements—transparency or adversarialness -- for restoring real judicial review.

Accordingly, this Committee should examine other ways to provide adversarial judicial review of individual instances of foreign intelligence surveillance. Such judicial review could like judicial review of searches and seizure done for law enforcement purposes, take place after the fact, when the surveillance is finished. While the original FISA contained a provision for such review, 50 U.S.C. 1806, that provision does not apply to all current collection authorities under FISA. Moreover, it has not proved sufficient to provide a real opportunity for a subject of surveillance to challenge the surveillance in an open and adversarial proceeding before a judge.

Representative Nadler (p. 191-192):

"*Ms. Martin, how can we—how can Congress solve the problem? We have a basic problem. Every challenge to abuse of constitutional rights by the Bush administration and the Obama administration has been met in the same way. Either the use of the state secrets doctrine to say you can't go to a court on that. The subject matter of the discussion is a state secret. Therefore, move to dismiss the case ab initio. Or you have no standing because you cannot prove that you personally were harmed by this.*

Now Mr. Snowden may have done a public service in giving some people standing by proving that they were harmed by this because anyone who is a Verizon subscriber arguable can no go into court and say that. How can we deal with these two problems that an administration, any administration can violate constitutional rights from here to kingdom come, subject to no court review because of either the state secrets doctrine or the standing problems because they don't admit what they are doing in the first place. It is secret.

It is secret what we are doing to you. Therefore, you have no standing because you can't prove what we are doing to you."

There are several steps the Congress could take to ameliorate the problem that individuals cannot challenge the government's actions against them in court, when the government refuses to acknowledge its activities and claims that the state secrets privilege or other doctrine prevents litigation.

First, the Congress should insist on public disclosure of information concerning the government's activities. In addition to public disclosure concerning the legal authorities and scope of surveillance programs generally, Congress should also require investigation of specific instances of surveillance, where there are credible allegations that individual rights have been violated, either by congressional committees, an inspector general or other body. That investigation could then inform additional public disclosures concerning questionable instances of government surveillance. And those disclosures in turn would facilitate judicial challenges by

the affected individuals. In particular, the government would not be able to seek dismissal of such challenges on state secrets grounds, because the information relevant to pursuing the case would be public.

In addition, I would urge the Congress to examine the possibility of creating a statutory cause of action for violation of an individual's constitutional rights. Doing so would make it more difficult for the government to secure dismissal of a challenge on technical grounds, and help insure that the court considers the merits of whether the government has violated someone's rights.

Representative Cohen:

"Are there ways to enhance the role of the Privacy and Civil Liberties Oversight Board so as to ensure a better balance between legitimate national security needs on the one hand and privacy, civil liberties and public transparency on the other?"

Congress should ensure that the Privacy and Civil Liberties Oversight Board receives adequate funding to enable it to carry out its statutory mandate. At the same time, the Congress and the federal courts have the ultimate constitutional responsibility for ensuring privacy, civil liberties and public transparency while protecting the national security.

Appendix D: Collaborative Institutional Training Initiative Certification

Completion Date 01-Sep-2020
Expiration Date N/A
Record ID 38114405

This is to certify that:

Michael Hall

Not valid for renewal of certification through CME. Do not use for TransCelerate mutual recognition (see Completion Report).

Has completed the following CITI Program course:

Student's (Curriculum Group)
Doctoral Student Researchers (Course Learner Group)
1 - Basic Course (Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?wdab10c2c-c0f8-4bcf-b488-335e37359394-38114405