

2019

Internet and Telecommunications Companies' Provision of Customer Information to the Government

Gbenga Ayodeji Osinowo
Walden University

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

 Part of the [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

Gbenga Ayodeji Osinowo

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. George Larkin, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Gregory Campbell, Committee Member,
Public Policy and Administration Faculty

Dr. Michael Brewer, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Internet and Telecommunications Companies' Provision of Customer Information to the
Government

by

Gbenga Ayodeji Osinowo

MBA, Kennesaw State University, 2012

MPA, University of Lagos, Nigeria, 2002

MS, University of Ibadan, Nigeria, 1998

BS, Ogun State University, Nigeria, 1995

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Administration

Walden University

August 2019

Abstract

The strategy of the National Security Agency (NSA) surveillance program is to incorporate the private sector into the bulk data collection of customers information, yet there is little legislative and judicial oversight. As a result, internet and telecommunications companies participated, placing at risk protected privacy interests of their customers. Using policy feedback theory and narrative policy framework as the theoretical framework, the purpose of this qualitative, case study was to explore how the federal government gains compliance of the internet and telecommunications industry to engage in information sharing with NSA during post 9/11, 2001 terrorists' attack. Secondary data were collected about internet and telecommunications companies through document analysis, corporate records, and credible news sources. These data were compiled as raw data and developed into codes, which led to categories and eventually developed into themes. Findings indicate that private companies participated for three main reasons: first, an interest in preserving national security, second, they believed they had limited or no liability, and third, profit-making. At the same time, the participants expressed concerns that the government gained compliance via the use of coercion, influence, and persuasion. The positive social change implication of this study includes recommendations to public policy practitioners/evaluators that it is necessary to include private sector analysis in a comprehensive review of public policy because inter-dependencies of the private-public sector guarantees effective public policy implementation/ assessment.

Internet and Telecommunications Companies' Provision of Customer Information to the

Government

by

Gbenga Ayodeji Osinowo

MBA, Kennesaw State University, 2012

MPA, University of Lagos, Nigeria, 2002

MS, University of Ibadan, Nigeria, 1998

BS, Ogun State University, Nigeria, 1995

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Administration

Walden University

August 2019

Dedication

This dissertation is dedicated to my late parents, Prince Emmanuel Oyedeji Osinowo and Caroline Omotayo Osinowo. I know that you are both smiling in heaven to see the academic excellence your little son has achieved.

Acknowledgments

My profound gratitude goes to my family for their understanding during my academic quest. I want to thank my wife, Ibiwonke Olabisi Osinowo, for her understanding of my divided attention during the project and for serving as an occasional proofreader. I want to thank my daughter, Aderinsola Osinowo, and my son, Bernard Osinowo, for their understanding of my divided attention to their needs while I was concentrating on my studies.

I want to acknowledge the late Dr. Ian Birdsall who untimely passed away during my academic journey. I want to thank Dr. George Larkin who gladly steered the direction of the research to completion, and I also want to thank Dr. Gregory Campbell for his intellectual inputs to the success of the research. Finally, I would like to thank Dr. Michael Brewer for accepting to be part of this project without any hesitations and for his eagerness to see the findings of the research.

Table of Contents

List of Tables	liv
List of Figures	lv
Chapter 1: Introduction the Study.....	1
Background to the Problem	2
Statement of the Problem.....	4
Purpose of the Study	5
Research Questions	6
Theoretical Framework.....	6
Nature of The Study.....	7
Operational Definitions.....	8
Assumptions, Limitations, Scope, and Delimitations.....	9
Assumptions.....	9
Limitations	9
Scope and Delimitations	10
Significance of the Study	10
Summary.....	11
Chapter 2: Literature Review	13
Introduction.....	13
Literature Search Strategy.....	14
Theoretical Framework.....	15
Policy Feedback Theory	15

Narrative Policy Framework.....	18
Review of Literature.....	19
History of Surveillance Programs.....	19
Advocates for the NSA Surveillance Programs.....	20
Critics of the NSA Surveillance Programs.....	22
The Activities of the Tech Companies and Effects of the NSA Surveillance Programs.....	23
The Capabilities of NSA Surveillance Programs.....	25
Synthesis of The Literature.....	26
Summary and Conclusions.....	30
Chapter 3: Research Method.....	32
Introduction.....	32
The Role of the Researcher.....	32
Research Methodology.....	34
Research Design.....	35
Data Collection.....	38
Data Collection Techniques.....	39
Data Analysis Plan.....	41
Ethical Procedures.....	45
Summary.....	48
Chapter 4: Results.....	49
Introduction.....	49

Setting	50
Demographics	51
Data Collection	52
Data Analysis	66
Evidence of Trustworthiness.....	76
Results.....	78
Private Companies Cooperate With NSA.....	79
How Private Companies Cooperated With Surveillance	81
Summary.....	88
Chapter 5: Discussion, Conclusions, and Recommendations.....	89
Introduction.....	89
Interpretation of the Findings.....	90
Limitations of the Study.....	94
Recommendations.....	94
Implications.....	96
Conclusion	99
References.....	102
Appendix A: Letter of Introduction to the Identified Organization and Supporting Documents	112

List of Tables

Table 1. Coded Data	68
Table 2. Code to Themes	71
Table 3. Research Findings.....	87

Chapter 1: Introduction the Study

The purpose of this research was to investigate how and why Internet and telecommunications companies provide customer information to the government. I explored the activities of the private sector in the National Security Agency (NSA) surveillance programs. Snowden's revelations that the government was secretly collecting bulk data about Americans without adequate legislative and judicial oversight has damaged the surveillance activities of the government. The private sector served as conduits to the government surveillance programs that led to the discovery that AT&T enhanced the ability of the NSA to spy on their customers' Internet traffic ("AT&T Helped NSA," 2015). I explored whether the private sector willingly cooperated with the government or whether they were forced to partake in the NSA surveillance programs.

This research might provide insights into the activities of the private sector collaboration with the government on the NSA surveillance programs from the private sector perspective. The research has the potential for social change in the sanctity of communications and how people perceive the government using and having access to communications. The private sector's handling data might reveal the need for changes and the way people evaluate public policy using the surveillance programs as the unit of analysis. The research might provide insights into the influence of the private sector in the implementation of public policy that might provide the basis for more scrutiny of the tech companies' activities regarding customers' data management.

The major sections in Chapter 1 include the background of the study on why it is essential to study the activities of the private sector in the NSA surveillance programs.

The problem statement includes the motives of the private companies to secretly partake in the NSA surveillance program. The purpose of the study is presented, and the research questions are provided. The theoretical framework was the policy feedback theory and narrative policy framework. The nature of the study was a qualitative case. I introduce the operational definitions, assumptions, limitations, scope, and delimitations. The significance of the study is presented to fill a gap to either include or exclude the private sector in a holistic evaluation of public policies. The final section is a summary on the main points of the chapter and with a transition to Chapter 2.

Background to the Problem

The nature of the NSA surveillance programs requires the government to collect data on people to prevent terrorist attacks; however, some fear that the government has the capabilities or has been secretly collecting data on people in the United States without adequate legislative and judicial oversight. The U.S. Government can conduct surveillance of people via the approval of the Foreign Intelligence Surveillance Court (FISA Court). However, the unconventional nature of the threats posed by terrorists with disregard to conventional warfare, like 911 where terrorists attacked the World Trade Center, led to the need to gather information regarding terrorist threats. This has created a situation whereby the actions of the NSA have been considered as illegitimate because they did not seek the approval of the FISA Court in all cases. The advancement in technology for surveillance purposes might have rendered the legal oversight of the NSA programs by the FISA Court to be obsolete, whereby the digital footprint of the people can be easily acquired or traced.

The extent, frequency, mode, and ease to which the government can perform surveillance on people in the United States due to asymmetrical warfare and technological advancement have shown the influence of the private sector as conduits of government surveillance capabilities. However, few studies have been conducted on the influence of the private sector in the NSA surveillance programs regarding their involvement, capacity, and the ability of the tech companies to influence the NSA surveillance programs. Bauerlein and Jeffrey (2016) contended that tech companies and the NSA should be equally responsible for the problems associated with NSA surveillance programs because they provided “back doors” to the NSA to have access to their networks. Gross (2006) highlighted the dilemma faced by the tech companies in turning over customers’ information that resulted in some companies like AT&T and BellSouth complying while Qwest and “Baby Bell” did not. However, Van der Velden (2015) explained that the NSA could access customers’ data from “leaky technology” via technologies that can come close to the machines that customers use to acquire their information without the NSA going through the tech companies. The purpose of this research was to understand the activities and gauge the influence of the private sector in the NSA surveillance programs to provide a better understanding of how the programs work. This study is needed to understand how the federal government gained compliance of the private sector to execute public policy and why the private sector abided by the dictates of the government even when it is against their core values.

Statement of the Problem

The purpose of this research was to determine the motive for private companies to secretly participate in NSA surveillance programs without adequate judicial and legislative oversight. Snowden's revelations regarding the NSA secretly collecting metadata of telephone records of U.S. citizens without judicial and legislative oversight had economic, political, and social consequences with U. S. allies' security of the program (Landau, 2014). Daniel and Benjamin (2014) posited that the revelations will hurt the United States' relationship with allies, and it will discourage U.S. technology firms from cooperating with the government. Thibodeau (2013) confirmed the backlash to the NSA surveillance program in the form of U.S. cloud-based companies potentially losing 10% to 20% of their foreign market, valued up to \$35 billion, because of the fear that they provided customers' data to the U.S. government. However, Gellman and Soltan (2014) confirmed that the NSA has the capabilities to store and retrieve data of phone records of the people up to 1 month. Greenwald and MacAskill (2013) also confirmed the ability of NSA to collect Internet data such as search history, e-mail contents, and live chats via a program called Prism. Katyal and Caplan (2008) posited that the scope of the NSA surveillance program infringes on the personal liberties of the people because they did not seek the approval of the FISA Court in some instances. Leahy (2006) also opposed the program because the FISA Court was instituted to check the excess powers of the president to guide against precedents. On the other hand, Yoo (2014) defended the program because the metadata only had the calling records with no contents of the phone records, and e-mail intercepts were of non-U. S. citizens. Gonzales (2006) also affirmed

that the program is lawful because it is the president's constitutional authority to execute war, which is required to keep the United States safe. However, there is a gap in the existing literature on the influence and extent of the private sectors in the NSA's surveillance program and why the private companies willingly or unwillingly cooperated with the government on the NSA surveillance program.

It is pertinent to study the motive of the private companies that secretly participated in the NSA surveillance programs without adequate judicial and legislative oversight. These companies are distancing themselves from the NSA surveillance program, considering the backlash from personal liberties advocates and support from security advocates after Snowden's revelations that exposed the private sector for gathering bulk data of their customers without adequate legislative and judicial oversight. Kerner (2014) stated the U.S. Government threatened Yahoo with a \$250,000 daily fine for noncompliance with the NSA data mining program. Mark (2013) stated that a complaint by a Verizon Wireless customer led to The American Civil Liberties Union (ACLU) filing a suit against the metadata collection program of the NSA. Apple filed a transparency request to stop the government's gag order against a FISA request of customers' records (Hustad, 2013). In this study, I investigated if the companies cooperated with the government because of profit, if they were forced by the government, or they believed in the activities of the NSA.

Purpose of the Study

The purpose of this study was to understand how the federal government gained compliance of the private sectors to execute public policy and why the private sector

abided by the dictates of the government even if it was against their core values. The results of the study can be used to explain the interplay of the private and the public sectors in public policy by providing a better understanding of the dynamics of private/public sector's involvement in the public policy process. I conducted a qualitative case study of the NSA Surveillance Program whereby congressional hearings, agency records, corporate records, and news sources served as sources of data. Inferences were drawn from these sources of data to determine the opinions and actions of these organizations in the private sectors that were involved in the bulk data transfer of customers' information to the government via the NSA surveillance program. The information would help to understand whether the instrument of coercion, persuasion, or collaboration was applied to gain compliance.

Research Questions

1. Why did the private Internet and telecommunications companies cooperate with the NSA surveillance programs activities?
2. How did the private Internet and telecommunications companies cooperate with the government NSA surveillance programs?

Theoretical Framework

The theoretical basis for this study was the policy feedback theory and narrative policy frameworks. Sabatier and Weible (2014) explained that the policy feedback theory is about politics-policy interactions and the impacts of policy design on society. Its origin is on the premise that historical political/policy precedents determine the new politics/politics of the present. In the narrative policy framework, the emphasis is on

adopting and rejecting policy output across space and time. According to the narrative policy framework, policymaking is an attempt to appeal to audience beliefs rather than to provide a balanced view on policy issues. I used the two theories to analyze private sector activities in the NSA surveillance programs. Policy feedback theory was used to understand NSA policy commitment due to political pressures made in the past, which led to the creation of FISA Court that was established to curb the excesses of the executive branch of government. The narrative policy framework was used to analyze the divergent views regarding the benefits/ drawbacks of the NSA surveillance program. I used these frameworks to explain how the proponents and opponents of the NSA surveillance program are marketing or persuading people in the United States to appeal to their audience beliefs.

The data obtained were used to analyze the themes of individual liberty and security of the country to reflect policy feedback theory politics-policy interactions. I explored the impact of NSA surveillance program in United States and how these opposing views are marketing their perspectives about the NSA surveillance to justify their positions. I will provide a detailed explanation of policy feedback theory and narrative policy framework in Chapter 2.

Nature of The Study

This was a qualitative research, and it was the most appropriate for the research because the information gathered from the sources of data was used to understand the NSA surveillance programs. The data were analyzed to understand why and how these private companies participated with the government to secretly gather information about

their customers. A qualitative case study approach is applied to focus on a single unit of study within a complex context (Rudestam & Newton, 2015). I chose a case study approach because I intended to provide an extensive study of the NSA surveillance programs, which is a single unit in the government complex espionage universe. The complexities of the NSA surveillance programs include the ability of the NSA to get phone records of the people (Gellman & Soltan, 2014). The ability of the NSA to retrieve Internet records like search history and e-mail contents (Greenwald & MacAskill, 2013) provided the basis for a study of the NSA surveillance programs within the context of the inherent complexities of the programs. However, due to the sensitivity of the study with security and legal implications, secondary data were applied to gather information from credible sources such as congressional hearings, corporate records, and news sources. Data analysis was done via coding and reducing the codes into themes and patterns to answer the research questions, and Chapter 3 will provide further clarifications on the use of case study approach.

Operational Definitions

Edward Snowden: A former employee(contractor) of the Central Intelligence Agency who illegally leaked classified information about the NSA surveillance programs (Berman, 2016).

FISA Court: The FISA Court is the federal court that is authorized to oversee and approve surveillance requests in the United States (Jones,2013).

Meta data: Data that provides more information about an item and split into categories of who, what, where, when, and how and leads to other materials. Hence, it is

a comprehensive information that comes and leads to many materials and sources (Woolcott, 2014).

MYSTIC: NSA surveillance voice interception program with retrospective retrieval capability (Gellman & Soltan, 2014).

Prism: NSA surveillance program that has the capabilities to collect Internet data, such as search history, e-mail contents, and live chats (Greenwald & MacAskill, 2013).

Assumptions, Limitations, Scope, and Delimitations

Assumptions

I assumed that I would get adequate data from congressional hearings, agency records, and news sources regarding the NSA surveillance programs because the NSA surveillance programs controversies are generating awareness and inquiries from all stakeholders. I also assumed that secondary data would help to understand the involvement of the private sector in the NSA surveillance programs because it would be used to understand and determine the extent of the private sector participation in the programs.

Limitations

The compilation of relevant data was difficult because it included multiple sources of information. However, the concentration on the private sector participation in the NSA surveillance programs allowed me the ability to extract the relevant information from the aggregate data. The sensitive nature of the NSA surveillance programs that has legal and political implications made it difficult to get adequate information regarding the research. However, inferences were drawn from the sources of information to understand

the operations, extent, frequency, and methods of the NSA surveillance programs and relate it to the private sector involvement. The case study approach did not provide a quantitative analysis of the NSA surveillance programs. Hence, the case study approach only provided an in-depth understanding of NSA surveillance programs from the perspective of the private sector involvement in the programs. Reflexivity, which is the conscious effort to explain a person's biases, values, and experiences at the outset of research, guaranteed the dependability of the research to minimize the influence of value judgment.

Scope and Delimitations

The purpose of the research was to understand the activities of the private sector in the NSA surveillance programs of the government by examining the motives of the private companies in the program that secretly gathered bulk data of their customers without adequate legislative and judicial oversight. Understanding the motive of the private sector in the NSA surveillance programs might help to understand the extent of collaboration between the public and the private sector in public policy. The boundaries of the research were the study of congressional hearings, agency records, and news sources to understand the activities of the private sector in the NSA surveillance programs. The outcome of the research might be transferable to other public policies of the government to understand the influence of the private sector in public policy.

Significance of the Study

Although numerous articles have been written about the NSA surveillance program, there is a gap in the literature on the influence and extent of the private sectors

in the NSA surveillance program and why the private companies willingly or unwillingly cooperated with the government on the NSA surveillance program. This research might explain whether to include or exclude the private sector in a holistic evaluation of public policies. The results of the study might determine whether the private sector influences public policy outcome or private sector only abide by the dictates of the government in executing public policy. The study of the private sector participation in the NSA surveillance program might provide insights into the relationship between the private and public sector in public policy. Laureate International Universities (n.d.) defined positive social change as “a deliberating process of creating and applying ideas, strategies, and actions to promote the worth, dignity, and development of individuals, communities, organizations, institutions, cultures, and societies” (p. 2). The study’s positive social change implications include providing useful knowledge to public policy practitioners/observers on how to incorporate private-public analysis for a comprehensive public policy review. Also, it might also prevent unnecessary or inadequate appraisal of public policy by incorporating or excluding private-public sector collaboration for a comprehensive evaluation of public policy for better public policy performance.

Summary

The leaks by Snowden regarding the NSA surveillance programs have caused controversy. Advocates for more security opine that the programs are needed to keep the United States safe; however, advocates for individual liberty posit that the activities of the NSA programs have to be curtailed to protect individual liberty. The leaks about the NSA surveillance programs have shown the private sectors as conduits to which the

government collects data, which has warranted the need to research the role of the private sector in the NSA surveillance programs. Therefore, I intended to understand the motive of the private companies in the NSA surveillance programs, with a view of understanding the role of the private sector in public policy that might explain whether the private sector should be included or excluded in public policy analysis.

In Chapter 2, I will provide more details about policy feedback theory and narrative policy framework that served as the guide for the research. I will also outline existing literature about the NSA surveillance programs.

Chapter 2: Literature Review

Introduction

The revelations of Snowden that the U.S. Government was secretly collecting data of the people without adequate judicial and legislative oversight has created problems for the private organizations involved in the NSA surveillance programs because they operated contrary to their core value of protecting customers' privacy. The surveillance programs have warranted the need to understand the motive of the private companies involved in the programs that secretly collected bulk data of their customers and provided it to the government without their consent, nor adequate judicial and legislative oversight. The results of this study might help to understand how the federal government gained compliance of the private sector to execute public policy. I explored why the private sector agreed to the directives of the government even when it is against their core values.

Scholars have established the relevance of understanding the motive of the private companies in the NSA surveillance programs because the revelations about the activities of the NSA programs have led to contending schools of thoughts to justify or nullify the need for the programs. Researchers have explained the economic, political, and social negative consequences of the NSA surveillance programs and the extent to which the government has the capabilities to retrieve and store data without citizen knowledge. Scholars also attempted to provide a rationale for the private companies in providing their customers' information to the government due to the immunity granted that made the companies comply with the directives; however, scholars have not provided a motive

behind the private sector participation. Researchers have outlined the views of the NSA surveillance programs, the negative consequences of the program, and the capacity of the programs and the extent to data were examined. These studies formed the basis upon which I used to understand the motive of the private sector to participate in the NSA surveillance programs from the private sector perspective with the intent to understand why they collaborated with the government without adequate legislative and judicial oversight.

The major sections of this chapter include the literature search strategy that I employed to get information regarding the NSA surveillance programs and an account of the theoretical framework of policy feedback theory and narrative policy framework that served as a guide to understand how to conduct the NSA surveillance programs research. The third section of this chapter is about the NSA surveillance programs using current literature, while the final section would be the summary and conclusions of the chapter.

Literature Search Strategy

The search strategy that I used for literature search included the use of keywords *Edward Snowden*, *NSA surveillance*, and *Prism*. The primary database for the research included the Thoreau Multi-Database Search. I made use of Academic Search Complete link that contains peer-reviewed journals, conference papers, newspapers, and magazines. The contemporaneous nature of the NSA surveillance programs made it imperative to access newspapers and conference papers to keep me updated with current trends in NSA surveillance programs. I also used Google Scholar Database to get articles about the NSA surveillance programs.

Theoretical Framework

The theoretical frameworks I used to guide the research were the policy feedback theory and narrative policy framework. Theory is needed to understand any research because it is used to describe abstract phenomena that occur under similar conditions. I chose the policy feedback theory to understand previous public policy commitments that allowed the NSA surveillance programs to be subjected to the oversight of the FISA Court, and the narrative policy framework was used to analyze divergent views of security and protection of individual liberty regarding NSA surveillance program.

The policy feedback theory is intended to link policy with long-term effects on society. Sabatier and Weible (2014) traced its origin to scholars like Schattschneider (1935), who posited that new policies create new politics. Esping-Anderson (1990) used a historical analysis of welfare states to posit that the content and makeup of policies determine political behavior. Skocpol (1992) explained that policies created at an earlier time (Time 1) could reshape state capacities, social groups, political goals, and capabilities at a later time (Time 2), and it could affect policy created at a later time (Time 2). On the other hand, Sabatier and Weible explained the narrative policy framework as the combination of the study of politics, coalitions, and policy change with policy narratives and storytelling in politics, and then traced its origin to McBeth, Jones, and Shanahan.

Policy Feedback Theory

Policy feedback theory is about historical institutionalism. According to policy feedback theory, people establish a policy and allocate resources to a program in the past,

and it defines the current structure of the present and it places an advantage of a group over another. Sabatier and Weible (2014) used Mettler and Sorelle's streams of policy feedback inquiry to explain policy feedback theory. Sabatier and Weible explained that public policy created at Time 1(past) is influenced by four major streams of what is the meaning of citizenship, the form of government, power of groups, and policy agendas. The meaning of citizenship explains the rights, duties, and obligations that the government enforces in society, and the citizens' response to the policy might influence the membership and attitudes in the political community. The form of government opines that policies established in the past shape public officials and their perception of what is considered legitimate from the domain of the government. In the power of groups, public policy or new legislation influences the likelihood of the formation of new groups in response to the needs or nuances of the new legislation. Policy agendas and problem definition are when public policy enacted in the past leads to how society comprehends social problems; this generates public attention and governmental action because it shapes the future conflict that might emanate from the policy. It might lead to coalitions within the groups with one group having an advantage over another.

Policy feedback theory presupposes that a public policy enacted in the past defines the meaning of citizenship in response to the nuances of the policy. It defines the form of government and power of groups that exist after the establishment of the policy, which leads to policy agenda and problem definition that will determine or influence current public policy. Goss (2010) offered a multilevel model of feedback theory to explain how public policy influences civil society via its contents, and it leads to

advocacy groups that affect individual levels and its civic engagement. Goss opined that the effects of public policy at the organizational level should not be viewed separately from the individual level because the effects of public policy on civic society trickle down to individuals who partake in groups, and individuals in the groups exact influences on one another, which serves as feedback that influences policy design.

I chose the policy feedback theory in the research to understand how the past policy of the NSA surveillance programs is influencing the current politics and policy of the NSA surveillance programs. The theory relates to the NSA surveillance programs because it explains how policy commitment of the past, which led to the creation of FISA court, is having an impact on the current NSA surveillance programs debate. Politics-policy interactions led to a creation of standard through FISA Court that guides the activities of the NSA regarding the use of wiretaps, and the commitments to that standard make it costly to deviate from getting warrants from FISA Court for wiretaps. The establishment of FISA court in the past (Time 1) has shaped the state capacity for surveillance. Also, it has created social groups like those that are advocating for more security and those that are advocating for the protection of privacy with different political goals and capabilities in the current (Time 2) that will shape the future policy on surveillance. Therefore, the study of the activities of the private sector involvement in the NSA surveillance program were analyzed based on the general principle of independent ideas of policy feedback theory that the impacts of policy precedents influence the politics of NSA surveillance programs. The policy feedback theory was used to understand how and why the Internet and telecommunications companies provided their

customers' information, without adequate legislative and judicial oversight, when past policies have identified the need for FISA Court to provide oversight.

Narrative Policy Framework

The narrative policy framework is used to influence policymaking by appealing to the audience's belief rather than presenting a clear presentation of balanced facts.

Sabatier and Weible (2014) explained four core elements of narrative policy framework.

The first element is the setting, which has to do with policy problems based on policy contexts. It must also possess a character of a victim who was harmed and a villain who wants to harm; it must possess a plot to establish relationships between the characters, and it should possess morals to provide a policy solution. The narrative policy framework is used to reinforce or oppose policy measures, and it equates to marketing or persuasion based on appealing to the audience's beliefs rather than on facts. Shanahan, Mcbeth, and Hathaway (2011) explained that media policy narratives influence public opinion when read to audiences with similar opinions.

I chose to use the narrative policy framework in the research to understand the divergent ideological views regarding the NSA surveillance programs when advocates promote the need to secure the United States against terrorists' attacks, while opponents emphasize the need to protect personal privacy and individual liberty. The divergent views are marketing their positions/arguments to influence the public's preference regarding the NSA surveillance program. I used the narrative policy framework to identify how the divergent views held on the NSA surveillance programs and to understand why the Internet and telecommunications companies provided their

customers' information to the government without adequate legislative and judicial oversight. Yoo (2014) attempted to persuade people in the United States that the NSA surveillance programs should be seen as legal because the unconventional nature of the war against al Qaeda would not always require FISA Court warrant. That position is playing on the U.S. audiences' belief that the country needs all measures to prevent another 9/11 terrorist attack, and the FISA Court might create a bottleneck that will prevent swift actions against the terrorists.

Review of Literature

The literature review plays a role in research because it lays the foundation upon which new ideas originate. Burkholder (2010) explained that the ability to critique a study provides the strengths and limitations of the study, which helps to discover new ideas regarding the study. Therefore, it is pertinent to trace the origin of the NSA surveillance programs to generate new ideas.

History of Surveillance Programs

The NSA was established in 1952 as an independent agency under the Department of Defense, with the responsibility of providing signal intelligence and information security for the U.S. Government (Schindler, 2010). Pearlman (2010) provided a mixed record of success of the NSA surveillance programs that was successful during the Korean war when it was able to penetrate the North Korean army radio traffic, while it was unsuccessful to penetrate the Soviet Union. Kirkus Reviews (2009) also claimed that the NSA was able to break all codes of the North Korean military within 30 days. However, President Eisenhower heard about the death of Stalin over the newswire

services and not via the intelligence community, which showed how the NSA was unsuccessful with the Soviet Union. Schindler (2010) suggested that United States could not penetrate the Soviet Union because of the Soviet spy, Bill Weisband, who compromised the NSA in 1948 by leaking the operations of the NSA to the Soviets. However, Kirkus identified the shift in the NSA from breaking codes and communications interceptions to eavesdropping on citizens without a warrant. Due to the revelations by Snowden regarding the activities of the NSA surveillance programs, there is a need to understand the operations and effects of the programs on people in the United States. Scholars who have studied the NSA surveillance programs have looked at the topic from two ideological perspectives: adequate security of the country and the protection of privacy. Researchers have focused on the negative consequences of the NSA surveillance programs, the capacity of the NSA surveillance programs, and the actions of the private companies in the NSA surveillance programs. Most of these researchers have approached the NSA surveillance programs from their ideological point of views and with conclusions often based on normative values and insufficient scientific methodology. However, these studies have inadequate scientific methodology, and the validity of their conclusions are less sacrosanct due to the influence of value judgment.

Advocates for the NSA Surveillance Programs

The advocates for the NSA surveillance are using legal, political, and constitutional viewpoints to support the NSA surveillance programs. Yoo (2014) provided the legal justification for the NSA surveillance program on the need to provide adequate security for people in the United States against terrorists. Yoo emphasized that

the NSA surveillance program was not illegal because the government only collected telephone records or metadata but did not receive the content of the phone records without judicial approval. Yoo explained that bulk data information is necessary for the unconventional warfare in which the enemy combatants do not represent a territorial sovereignty, population, or proper identification. It becomes necessary for the government to respond to the unconventional warfare via the constitutional power of the president as the commander-in-chief to execute war in cases of military hostilities. The activities of the NSA do not violate the Fourth Amendment (the right of the people to be secure against unreasonable searches without a warrant) because the president has the wartime authority to protect the United States. Yoo opined that the judiciary is inexperienced in conducting foreign intelligence, and the FISA cannot catch up with the terrorists who change their e-mail addresses and telephone numbers. Yoo opined that the NSA surveillance program is legal because of the “third party doctrine,” where the customers willingly provided their information to the telecommunications companies and the FISA court only requires probable cause of criminal activities to get metadata. The FISA court should be needed only when the contents of the telephone conversations are needed to make an arrest and for trial, and most of the data collected are that of non-U.S. citizens or residents that do not receive Fourth Amendment protection. Gonzales (2006) opined that the program is necessary and lawful because it provided the United States the avenue to collect the necessary information on Qaeda’s plan against the country, and it gives the president the constitutional authority to executive war, thereby securing the safety of the United States.

Critics of the NSA Surveillance Programs

The critics of the NSA programs also use legal, political, and constitutional measures to fight against the programs. Anderson (2014) not only criticized the operations of the illegality of the NSA surveillance program for collecting bulk data on Americans, but also criticized the provisions of the Foreign Intelligence Surveillance Act Amendment Act (FAA) enacted in 2008 and renewed in 2012. After the revelations of Snowden, the activities of the FAA were insufficient to protect privacy and individual liberties. Anderson posited that Congress did not adequately protect the Fourth Amendment because the law violates privacy and reduces the powers of the FISA court as it abolished the methodological distinction between wiretapping lines and intercepting radio waves which does not differentiate between domestic and international surveillance. The new provision provides surveillance in three scenarios that include targets that are non-U.S. citizens believed to be outside the United States, while the data collection agency is U.S, based. The targets are U.S citizens who reside outside of the United States, but the targeting agency collects data in the United States. The targets are U.S. citizens outside of the United States, while the targeting agency collects data from outside the United States. Anderson posited that these provisions do not provide adequate judicial oversight. Anderson proposed that the Congress should narrow the scope of the NSA surveillance program by strengthening the courts, the Congress, and independent watchdog agencies to supervise the activities of the FISA and to provide clarity on what constitutes reasonable suspicion.

Leahy (2006) argued that the Congress did not authorize the presidential order of President George Bush to confirm the legality of the surveillance programs because the president has the power to execute wars but not to write them. Leahy further argued that the wiretappings during President George Bush's administration that did not pass through the FISA Court were illegal. Leahy stated that the FISA court was established due to the historical precedent of the illegal wiretap of Dr. Martin Luther King Jr. and President Nixon's illegality during the Watergate scandal. Katyal and Caplan (2008) posited that the NSA surveillance programs infringed on the personal liberties of the people when they did not seek the approval of the FISA court for wiretaps. Austin (2015) claimed that the NSA surveillance went beyond privacy rights and it was against the rule of law. Austin faulted the idea that approval via FISA court is enough because a program that is lawful via statutory authority might still violate the rule of law.

The Activities of the Tech Companies and Effects of the NSA Surveillance Programs

The revelations by Snowden showed that the private tech companies participated in the NSA surveillance programs, and some companies have signified that they were compelled to execute the government directive. Rash (2013) stated that the tech companies did not disclose the extent of collaboration with the government because the governmental order also compelled them to maintain secrecy. However, Facebook admitted that they provided the government with customer records and the content of their Facebook communications, and Microsoft and Apple also admitted that they also received a governmental order to provide customer information. The United Business Media LLC (2006) wrote about class action lawsuit involving Mark Klein, a former

employee of AT&T, when he stated that he was required to connect fiber optic circuits to their customers' private Internet-based data to a device that diverted the same data to a room controlled by the NSA. I stopped reviewing here due to time constraints.

Daniel and Benjamin (2014) explained the consequences of Snowden's revelations about the NSA surveillance program like the Brazilian President, Rousseff, claiming that the United States of America violated her fundamental human rights and civil liberties. They informed that Snowden's revelation had damaged U.S relations with its allies which have angered and surprised allies' public, and it has affected the United States' moral high ground on cybersecurity and internet governance. President Obama instituted an independent group of experts to examine the damage, and the panel recommended the end of the bulk collection of telephone metadata, and to restrict the surveillance of foreign leaders. The panel also suggested that the telephone providers but not the government should store the metadata of the customers. However, Snowden's revelations have threatened the U.S technology companies with their critics claiming they voluntarily provided customer information to the government. These companies have started to encrypt their services to distance themselves from the government. The dilemma for the NSA is either to continue to keep their operations secret and hope there will no longer be any leaks, or not to continue their operations in secret and become more transparent to avoid leaks. Landau (2014) explained the negative consequence of Snowden's revelations about metadata and the PRISM programs of the NSA surveillance programs which detailed how the U.S is spying on foreign countries and their leaders. She stated that U.S companies providing cloud services are worried that they will lose

many customers due to NSA surveillance programs, and European Parliament President Martin Schulz warned that if Snowden's revelations are correct, it will negatively affect E.U-U.S relations.

The Capabilities of NSA Surveillance Programs

The NSA surveillance programs have shown that the government has enormous capabilities to collect peoples' data. Greenwald and MacAskill (2013) explained that the NSA surveillance program called Prism program can access servers of companies like Google, Apple, and Facebook. This program allows the government the ability to retrieve materials such as search history, the content of an e-mail, file transfers, and live chats from the companies directly. They stated that this program allows the NSA to retrieve information from participants that live outside the United States and Americans who are communicating with people outside the United States. They also explained that this program compelled companies to provide the information to the government, and they also have the capabilities to obtain targeted information without having to request from the service providers. Microsoft joined the program in 2007, Yahoo in 2008, Facebook in 2009, YouTube in 2010, Skype and AOL in 2011, and Apple in 2012 which shows how far reaching the operations of the NSA surveillance Prism program. Gellman and Soltan (2014) asserted that the NSA has the capabilities to record 100% of a foreign country's telephone calls, rewind, and review conversation for a 30-day period. They informed that the voice interception program with retrospective retrieval capability is called MYSTIC, and it started in the year 2009 with a 30-day rolling buffer which allows it to clear the oldest calls when the new ones arrive.

Synthesis of The Literature

The NSA surveillance program is generating controversies between the proponents and opponents of the program. Proponents of the NSA surveillance like, Yoo (2014), justified the legality of the program based on the desire to keep America safe after the 9/11 terrorist attack in the United States, which showed the unconventional nature of the warfare that does not represent territorial sovereignty, population, and identity. It becomes imperative for the government to create a metadata upon which all telephone activities willingly provided to the private companies, (third party doctrine) can be monitored because of the rapidly changing tactics of the terrorists who regularly change their telephone numbers and email addresses. Metadata is an essential instrument needed to monitor the activities of the terrorists, but the government should seek the approval of the Foreign Intelligence Surveillance Court when the contents of the metadata are needed to be monitored for trial and prosecution. Gonzales (2006) also supported the NSA program on the basis that the president has the constitutional power to execute the NSA surveillance program during the wartime period.

On the other hand, scholars like Anderson (2014) opined that the NSA surveillance program is illegal because it was illegally creating metadata of the people without the approval of the FISA court. Anderson stated that metadata undermines the privacy and individual liberties as promulgated by the Fourth Amendment (right of the people to be secure against unreasonable searches without a warrant) as written in the United States Constitution. Anderson posited that the Foreign Intelligence Surveillance Act (2012) did not secure privacy because there is no distinction between wiretapping

lines and intercepting radio waves and is subject to limited judicial scrutiny. Anderson disagreed with the inadequate supervision of the new provisions of the Act that allows for surveillance in three scenarios. He opined that target of non-U.S citizens believed to be outside the United States, while the data collection agency is U.S based. The target of U.S citizens outside the U.S but targeting agency collects data in U.S. And the target of U.S citizens outside the U.S and targeting agency outside the U.S. Anderson recommended that the government should narrow the scope of the surveillance program by strengthening the ability of the Congress, courts, and establish independent watchdog agency, to supervise the operations of the foreign intelligence Surveillance Act.

Leahy (2006) criticized the NSA surveillance programs based on the fact that it went against the historical precedent of not passing through FISA court which was instituted to curb the excesses of the executive branch of government. Katyal and Caplan (2008) believed that NSA surveillance programs infringed on personal liberties. Austin (2015) went further to opine that it is against the rule of law.

Irrespective of the differing schools of thought regarding the NSA surveillance programs, it must be noted that both schools of thought agreed that there is the need to have a surveillance program to keep America safe, but the extent of the surveillance program is the difference between the divergent opinions. Rash (2013) suggested that the companies were compelled by the government to keep the NSA surveillance programs as secret. The United Business Media LLC (2006) gave an example of when an AT&T employee was compelled to divert customers' data to the NSA which confirmed that these companies participated in the NSA surveillance programs. However, in the light of

Snowden's revelations, the NSA surveillance program is having negative effects on United States relationship with allies. Daniel and Benjamin (2014) explained that the negative consequences of Snowden's revelations which have surprised and angered the publics of allied countries has made the United States lose moral high ground in cybersecurity and Internet governance. U.S technology companies have been accused by critics that they willingly collaborated with the government to provide customers' information, and this has resulted in them to encrypt their services to show that they did not voluntarily cooperate with the government to provide customer information. Landau (2014) explained that the NSA surveillance programs are damaging to the United States Cloud-based companies. However, Greenwald and MacAskill (2013) explained the capacity of the NSA surveillance programs via PRISM, can access the servers of the private companies.

Gellman and Soltan (2014) also explained the capacity of NSA surveillance program to record 100% of the foreign call via the program called MYSTIC, which signifies how enormous and far-reaching of the NSA surveillance programs are. Based on the analyses of the literature, one can understand that the private companies play a pivotal role in the provision of the government with customer information. However, there is a gap in the existing literature that explains the role of the private sector in the NSA surveillance program because all the companies that were involved in the NSA surveillance programs started to openly distance themselves from the program after the revelations of Snowden. The gap in the identified literature is that they have not

explained the role of the private companies as the conduit for providing customer information to the government.

This research would attempt to understand the motive of the private companies in the NSA surveillance programs, whether they were coerced to cooperate with the government, or they cooperated for financial motivation, or they voluntarily cooperated with the programs because they believed in the programs and decided to keep the programs secret. I hope that the findings in the proposed research might explain the role of the private sector in public policy. Whether to incorporate the involvement of the private sector in the comprehensive evaluation of public policy because of their enormous influence on public policy, or they are just instruments of enforcement of public policy by the government.

The literature has shown that the private companies participated in the NSA surveillance programs, and the programs can access the data that the private companies possess. The literature has led to the need to answer the research questions of why did the private Internet and telecommunications companies cooperate with the NSA surveillance programs activities and how did the private internet and telecommunications companies cooperate with the government NSA surveillance programs? The literature review has shown that the private companies serve as conduits for the execution of the NSA surveillance programs, and these companies have customer information in their databases which gave the NSA the opportunity to be able to retrieve the information without the consent of their customers. The nature of the research questions has shown that the appropriate method of getting the answers to the research questions should be via

a qualitative research method because the inquiry seeks to understand how and why regarding the NSA surveillance programs. The qualitative research method would provide answers from multiple sources of information regarding the NSA surveillance programs from the private sector perspective, and a case study approach would be appropriate because it would provide direction to concentrate on the activities of the NSA surveillance programs solely.

Summary and Conclusions

The literature review showed contending views from two different ideological spectrums regarding the activities of the NSA surveillance programs. Advocates of the NSA surveillance programs believe that the program is legitimate and it is needed to keep American safe, while critics of the programs are of the opinion that it contravenes privacy rights when data of Americans are collected without adequate legislative and judicial oversight. The literature also explained the activities of the tech companies regarding their customer data and the NSA surveillance programs, the negative effects of the NSA surveillance programs to their companies and the country, and the capabilities of the NSA to be able to collect our data without our consent secretly. The literature has been able to confirm the existence of a secret NSA surveillance programs that have the capacity and indeed collected massive data of the people without adequate legislative and judicial oversight, and the private sector served as conduits when they provided the data to the NSA. However, the literature could not explain why the private companies participated in the NSA surveillance programs without adequate judicial legislative and judicial oversight when they understand that it is against their core values. This research might

fill in the gap to understand the role of the private companies as conduits for providing customer information to the government with a view to understanding the motive of the private companies in the NSA surveillance programs. It is hoped that the findings might explain the role of the private sector in public policy. A qualitative research method would be used to analyze the activities of the private sector in the NSA surveillance programs, and the case study approach would be used to provide an in-depth understanding of the program in Chapter 3

Chapter 3: Research Method

Introduction

The purpose of this study was to understand how the federal government gained compliance of the private sectors to agree to execute public policy and why the private sector abided by the dictates of the government even if it was against their core values. I explained the interplay of the private and the public sectors in public policy by providing a better understanding of the dynamic of private/public sector involvement in the public policy process. In this chapter, I explain how I executed the research. I outline the role of the researcher, the methodology employed, instrumentation for data collection, data analysis, ethical procedures, and a summary of the chapter.

The Role of the Researcher

The research questions of the research were the following:

1. Why did the private Internet and telecommunications companies cooperate with the NSA surveillance programs activities?
2. How did the private Internet and telecommunications companies cooperate with the Government NSA surveillance programs?

The central purpose of the study was to explore the motive of the private companies that participated in the NSA surveillance programs to understand why the private companies cooperated with the government when it was against their core values. Therefore, I intended to conduct the research via a qualitative method to understand the how and why of the research. The qualitative method is exploratory, and researchers use it to understand a phenomenon from the perspectives of those who directly participated or

who were affected by the phenomenon. Creswell (2009) stated, “qualitative research is a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem” (p. 232). I sought to understand the opinions of the telecommunications and Internet companies of the clandestine surveillance programs of the NSA by exploring their perspectives and opinions about the programs.

In conducting this research, I gathered qualitative data from congressional hearings, agency records, corporate records, and news sources. I also determined how to conduct the research approach, the sources of data, and methods of data collection. Hence, the outcome and the credibility of the research was dependent on my ability to successfully conduct qualitative research. My intention was to be professional and objective in the way information was gathered and interpreted from multiple sources. The sources of data were secondary, which makes it unlikely that I would influence the result because the data are already established and vetted. I am neutral in the debate regarding the NSA surveillance programs because I belong to neither school of thoughts that proposes more security for the country or for the protection of personal privacy. Although I currently work in the telecommunications industry, I conducted the research from the public policy perspective that does not provide any conflict with my profession, nor has anything to do with my work environment. I minimized biases via adherence to the tenets of qualitative research by applying scientific methodology to explore the activities of the private sector in the NSA surveillance programs.

Research Methodology

Creswell (2009) provided the characteristics of the qualitative research method to include a natural setting where the researcher gathers data and the researcher as a key instrument who personally collects data. The use of multiple sources of data like interviews, observations, and documents lead to inductive data analysis that involves building a pattern of data from the bottom up. The researcher learns from the participants involved in the research, whereby the theoretical lens is used to understand the object or phenomenon under research. The scholar uses interpretative inquiry based on the researcher's background, history, contexts, and prior understanding, and researcher develops a holistic account from different perspectives. The qualitative research method is designed to understand how and why of a research question because it uses research techniques like field notes, pilot studies, document analysis, observation strategies, interviewing, focus groups, questionnaires, and journaling to understanding phenomena. I chose qualitative research because I wished to understand how and why Internet and telecommunications companies provided customer information to the government.

Creswell (2013) explained that the sample size in qualitative research is determined not only to study a few sites or individuals but to also collect extensive data about each site or individual. Miles, Huberman, and Saldana (2014) stated that qualitative researchers often use small sample sizes based on context and in-depth analysis that is purposive rather than random. The sample size in a qualitative research should be small and purposive because the data gathered are not used to generalize but to elucidate information from the human subjects who have lived through or are associated with a

phenomenon. The necessary sample size to generate meaningful qualitative data can be determined by defining the aspect of a phenomenon a researcher wants to investigate and the need to define the conceptual framework that will help to explain or qualify the basic process of the study (Miles et al., 2014). The sources of data for this study included document analysis of congressional hearings, agency records, corporate records, and news sources from the perspective of the private sector about the NSA surveillance programs. The multiple sources of data provided meaningful and in-depth data that explained the corporate organizations' opinions regarding the NSA surveillance programs.

Research Design

A case study provides a detailed explanation of the development or analysis of an event/events, person/group of persons, or situation/situations over a period. Yin (2014) explained that case studies are preferred strategies to understanding how or why of a research questions, and when a researcher has little control over the events and with focus on contemporaneous events with real-life consequences. Yin explained that research questions with how and why provides operational links that can be traced over time rather than mere frequencies or incidence. Case studies are used to investigate such questions because they are more exploratory in understanding the history and intricacies of such research inquiries. Yin stated that case studies are preferred when investigating contemporary events that the researcher cannot manipulate because it relies on multiple sources of information such as documents, artifacts, interviews, and observations. I chose a case study for the study of NSA surveillance programs because it involves the use of

research question of how and why the Internet and telecommunications provide customer information to the government. I cannot easily manipulate the research findings because it involves multiple sources of data that includes congressional hearings, agency records, corporate records, and news sources. Finally, the NSA surveillance program is a contemporaneous topic with real-life implications on the manner in which communications are handled in the United States.

I chose a case study design because it provided an in-depth understanding of the programs. The case study was not used as a teaching mechanism to explain or serve a particular purpose towards the understanding of a particular phenomenon, but it was used to gather information about the NSA surveillance programs. Creswell (2013) outlined the defining features of a case study to include an identification of a case. An in-depth understanding of a case, a description of a case, issues might be organized in chronology by the researcher, and the researcher's conclusion are informed by the overall meaning derived from the case. An inquiry into the activities of the NSA surveillance programs should be studied via the use of a case study approach because I identified the NSA surveillance programs as a specific case. It is unique, as I wished to describe an in-depth understanding of the programs, organized the case from the era of President George Bush's administration, and to provide an informed conclusion based on the overall information gotten from the conduct of the research. The quality of the data sources is paramount to the success of the research. Congressional hearings from legislative oversight, agency records on the formal corporate opinion about the programs, and the news sources provided investigative data about the NSA surveillance programs.

Yin (2014) explained that an explanatory, single case study with competing explanations of the same set of events could be applied to other situations. The study of the NSA surveillance programs, which was a single case study with competing viewpoints, was used to understand the NSA surveillance programs' private-public governmental policy that might serve as a blueprint for a broad understanding of all private-public governmental policies.

I applied purposeful sampling strategy, whereby the information that was acquired from the multiple sources was geared towards understanding the private sector involvement in the NSA surveillance programs. The type of sampling used was based on the maximum variation, whereby diverse variations of information sources and conclusions were selected based on characteristics that signifies the influence/involvement of the Internet and telecommunications companies in the NSA surveillance programs. The criteria I employed to determine the sources of information were maximum variation to reflect diverse aspects of the NSA surveillance programs like Prism and MYSTIC programs and diverse points of view to reflect the corporate decisions of the Internet and telecommunications companies. Congressional reports were used to get the official position of the Internet and telecommunications companies. The official corporate records were also designed to provide a reliable source of information, while news sources were designed to provide investigative information regarding the NSA surveillance programs. The point of data saturation was determined when data collected from multiple sources were trending towards the same or similar conclusions. I stopped reviewing here due to time constraints.

Data Collection

The instrument of data collection was designed to be in three phases, and the first phase was to be via the minutes of congressional hearings, and other public documents. The information acquired from congressional hearings (such as, House Judiciary Committee Report and Senate Judiciary Committee Report) was to lay the data foundation for the research because these are legally binding documents through which the private sector executives were mandated or subpoenaed to provide official positions about their companies regarding the NSA surveillance programs. The second phase of data collection designed was to be the official corporate records of some of the identified companies and published records of the identified organizations. The data obtained from the corporate records (such as, press releases and official statements by executives of identified companies) was designed to be used to complement the congressional hearings to capture other NSA surveillance programs activities that might not be the focus of congressional hearings. The third and final phase of the data collection designed was credible news sources that might provide investigative data of the private sector involvement in the NSA surveillance programs.

The data were designed to be based on drawing inferences from multiple sources of data examined by myself to answer four specific questions from the contents of multiple sources of data. The first question was to understand the official positions of the identified organizations about the NSA surveillance programs; why these organizations hold such views; how these organizations got involved in the NSA surveillance programs; and what these organizations perceived as the strengths and weaknesses of

their operations in the NSA surveillance programs. These four specific questions were designed to provide a proper understanding of the NSA surveillance programs by forming the bases upon which the research questions of the dissertation are answered. The first question would provide the background of the identified organization regarding the NSA surveillance programs which will in turn help to understand the private sector involvement in the NSA surveillance programs. The second question would help me to understand why these organizations hold their official positions which would help to provide a diverse variation of information of the private sector involvement in the NSA surveillance programs. The third question would help me identify whether these organizations willingly got involved in the NSA surveillance programs or they were coerced by the government to partake in the programs. While the fourth question would help me to understand the specific strengths or weaknesses of the NSA surveillance programs from the identified organizations' perspective which will, in turn, reflect the diverse aspects of the programs and diverse points of view that influenced corporate decisions. These four specific questions were designed to form my focal attention during data mining from the multiple sources of data of congressional hearings, corporate records, agency records, and credible news sources.

Data Collection Techniques

The data collection technique was based on finding ways to search/ gain access to where the information is located, how to conduct a good qualitative research sampling, how to record and keep data, and the anticipated ethical issues (Creswell, 2013). The data collection technique would commence by identifying congressional hearings that has to

do with the NSA surveillance programs, and to gain access to government gazette which might require a letter of introduction (Appendix A) to the Congress and other governmental agencies with the information. The second phase was to identify the private companies that were involved in NSA surveillance programs, and which might also require a letter of introduction if there is need be to visit their physical locations. The third phase was the need to identify news sources that might provide more data about the NSA surveillance programs and access to the data is incumbent upon my dexterity as a researcher to use the search engines and the library. Getting necessary news sources of information about the NSA surveillance programs included the search for keywords such as *metadata* and *Prism*. However, it must be noted that the use of the library would play a pivotal role in all data sources identification/access and analysis, but my ability as a qualitative research expert would ameliorate the concern of identifying the necessary data. Hence, the quality of the data would be ensured by the use of credible documents prepared for other purposes such as congressional hearings, agency records, and corporate records. While the reliability and validity of the data were guaranteed via the ability to ascertain that the prepared documents can be inspected and verified by those interested in the research, and they can interpret the data and compare it to the extent of the creativity of the research findings (Patton, 2002).

Data Analysis Plan

Data analysis is vital to the success of any research because it presents the outcome of the investigation to answer the research question. Creswell (2013) explained that data analysis involves preparing and organizing data, reduce them into themes via the process of coding and condensing the codes, and presenting the data in figures, table or discussion. Data analysis strategy is a detailed plan of action or policy to achieve the overall aim of preparing, organizing and interpreting the data which seeks to answer the research question. The data analysis strategy for the research would be based on creating and identifying codes, reducing the codes to themes and patterns, making contrasts and comparison between the multiple sources of data as explained in the data collection section. Then create a point of view and display the data in tabular form, before the researcher presents the data in the form of discussion.

The research would be based on the pre-coding structure for data analysis to answer the research question accurately. Miles et al. (2014) posited that incorporating conceptual framework, and research questions will lead to good data and well-founded conclusion because the expectations of the research participants will be defined in advance. The research participants in the research are provided by the multiple sources of secondary data. The first phase of data analysis is that I shall pre-coded the themes of security and individual liberty based on the literature review thoroughly explained in Chapter 2. The policy feedback and narrative framework would serve as the guide to identify both themes which would help to relate the themes to the research questions and to define the expectations of the research. The second phase of data analysis would

proceed with I manually analyzing the data collected from multiple data sources such as congressional hearings, agency records, corporate records and news sources and organize them on both themes of security and personal liberty. However, it was designed that if any discrepant cases are observed in the analyses, they would be coded and related to the research questions with a view to defining subthemes or new themes that were not envisaged at the beginning of the research.

I will link statements, write-ups, and contents from all the multiple sources of data, and analyze them with the pre-coded themes of security and individual liberty. The quest for security led to the need for the NSA surveillance programs, while the need to protect individual liberty led to the need to understand the motive of the private companies for their involvement in the NSA surveillance programs. The identified specific question of understanding the official positions of the identified organizations about the NSA surveillance programs. Why these organizations hold such views; how these organizations got involved in the NSA surveillance programs; and what these organizations perceived as the strengths and weaknesses of their operations in the NSA surveillance programs would be used to elicit information from all the multiple sources of data. These four specific and consistent questions that I have identified will be used to draw patterns and comparison from all multiple sources of data, and form common themes of security and individual liberty, and any other new themes that emanated from data analysis of the multiple sources of data.

The data gathered were designed to be presented in two phases of tabular format and written analysis of the data. The tabular format was to comprise two tables, and table

one will start with the research questions in the first column, security as a theme in the second column, individual liberty as a theme in the third column, while other columns might exist depending on if new themes are discovered. The rows would state the data to correspond with the themes and the sources of the data. The second table would have the themes in the first column, types of companies in the second column, methods of surveillance in the third columns, while the last column would state the sources of data. The first table would provide a comprehensive picture of the themes, the reasons why the companies decided to partake in the NSA surveillance programs, and how they participated in the program. While the second table would show all the discovered themes, types of business and the sources of data. I believed that the tabular format would provide a holistic overview of all the data which will enhance a better analysis to properly understand how and why the private sector cooperated in the NSA surveillance programs. The second phase was written analysis and interpretation of the data that were discovered in the tabular format to address the research statement of the problem which is to understand the motive of internet and telecommunications companies to cooperate with the NSA surveillance programs without adequate legislative and judicial oversight.

The credibility of the research was designed to be based on validation strategies, whereby internal validity would be achieved by defining my past experiences and values to clarify biases, prejudices, experiences, and orientation at the outset of the research that might color the interpretation of the findings. The reflexivity approach in which my past experiences and values which might explain my views regarding the NSA surveillance programs would be stated at the outset of the research. I was born in Nigeria, a

developing country where individual liberty is not adequately guaranteed by the constitution, and a country that is a victim of incessant terrorists' attacks from organizations like, Boko Haram. My past experiences with infringement on individual liberty and destruction by terrorist organizations provide a balanced view of the activities of the NSA surveillance programs. The balanced view would curb or minimize personal biases in the research because I do not belong to any school of thought, and this, in turn, should provide a more objective interpretation of the findings. Furthermore, external validity would be achieved via the use of triangulation because multiple sources of data would provide cross verification of data whereby themes would be identified from different sources.

External validity was ensured via external reviewer contribution, and peer debriefing sessions as two colleagues of the researcher have agreed to participate. The reliability of the data was ensured by accurate documentation of data from all the multiple data sources as and when available, and ensured that only data from credible sources are documented. The dependability of the research data would be established via accurate citing the sources of data which will provide an audit trail for anybody that wants to examine the research findings. The confirmability of the research is going to be guaranteed by the choice of credible sources of data to establish that the data are reliable, and accurate citing the sources of data would provide an audit trail. The use of reflexivity approach would also ensure the confirmability of the research because I am aware of my biases, values, and experiences and I would deliberately use the

consciousness as a guide to ensure the accurate interpretation of data and minimize the use of value judgment.

Ethical Procedures

The procedures to which data were collected and protected are pivotal to the overall success of research, and I intend to abide by Walden University educational standard. Walden University Institutional Review Board, Section 3, IRB application form identified 10 potential risks and three benefits that must be explained before any proposed research is approved. An examination of the 10 potential risks of the proposed study suggests:

- Unintended disclosure of confidential information does not apply to the proposed research because all the data will be gotten from congressional hearings, agency records, corporate records and news sources.
- Psychological stress greater than what one would experience in daily life constitutes minimal risk does not apply because the sources of data are public documents.
- Attention to personal information is irrelevant to the study because the sources of data are public documents that do not include personal information.
- The proposed research does not permit for unwanted solicitation, intrusion, or observation in public places because the sources of data are public documents.

- Social or economic loss constitutes a minimal risk in the proposed research because the sources of data are public documents.
- The perceived coercion to participate due to any existing or expected relationship between the participant and the researcher is not applicable to the proposed research because it does not involve interviewing any individual.
- Misunderstanding as a result of experimental deception is not applicable because the sources of data are public documents that were not written specifically for the proposed research.
- Minor negative effects on the participants' or stakeholders' health are not applicable to the proposed research because the sources of data are public documents.
- Major negative effects on participants' or stakeholders' health are not applicable to the proposed research because the sources of data have no health implications.

Based on the analysis of the proposed research, which implies no risks because the sources of data are public documents, it becomes imperative to influence the IRB to grant permission to the study.

It must be noted that any research that involves the NSA surveillance program would receive scrutiny from the IRB because of the sensitive nature of the topic on the security of United States. I was able to gain approval of the IRB based on the research plan and I adhered to Walden University IRB application guidelines and sound

qualitative research standard. Walden University IRB Section 3, Questions 17, 18, and 19 require steps to minimize risks and to protect participants, describe anticipated benefits of the research to the participants, and the anticipated benefits to the society. I explained to the IRB that the research does not involve any individual participation that might lead to any exposure, but the sources of data will be public documents that do not affect any individual.

I also explained the anticipated benefits of the research to the society, which provides the ability of the society to have a holistic evaluation of public policy. The study would explain the activities of the private sector in public policy, whether they have a direct influence on public policy in terms of collaboration and cooperation, or they were compelled to carry out the directives of the public sector. This would, in turn, provide the society the ability to evaluate public policies by accommodating the activities of all collaborators. I would exhibit the personal ability and competence to conduct a sound qualitative research. Simon (2011) explained that validity in qualitative research could be achieved by the trustworthiness of the research, and reliability can be achieved via dependability of the research findings. I explained and exhibited to the IRB my intellectual and proven integrity to conduct a qualitative research that will be trustworthy and dependable due to my experience to conduct qualitative research. I put into practice the knowledge acquired at Walden University, and the intellectual competence acquired via scholarly articles on qualitative research studies to research the NSA surveillance programs.

Summary

This chapter was an explanation of the role of the researcher as the research instrument to conduct a good qualitative research via a case study analysis of the NSA surveillance programs. The data collection would be via credible existing data such as, congressional hearings, agency records, corporate records, and new sources on NSA surveillance programs. The data collection technique would be to identify and have access to public documents that will shed light upon the NSA surveillance programs. Data analysis would be to reduce data into themes via the process of coding and condense the codes for better understanding and interpretation of the collected data. The internal validity of the research would be attained by using my past experiences and values to clarify my biases by using the reflexivity approach to explain the biases at the outset of the research. The external validity would be attained through external reviewer contribution and peer debriefing sessions. The reliability of the research would be ensured via accurate documentation of data from credible sources, while dependability would be achieved by accurate citing of sources of data to provide an audit trail. Finally, the ethical protection of sources of data would be achieved through the use of public documents to conform with the Walden University academic standard, and the overall process would lead to Chapter 4 that will explain the outcomes and results of the conducted research.

Chapter 4: Results

Introduction

In this study, I sought to understand how the federal government gained compliance of the private sectors to agree to execute public policy and why the private sector abided by the dictates of the government even if it was against their core values. I explained the involvement of the private sector in the public policy process by using the NSA surveillance programs as a reference point to understand the private/public sector collaboration in public policy process. The research questions were the following:

1. Why did the private Internet and telecommunications companies cooperate with the NSA surveillance programs activities?
2. How did the private Internet and telecommunications companies cooperate with the Government NSA surveillance programs?

In the first section in this chapter, I explain the changes that occurred in the data gathering phase of the research. I also include the demographics section that describes the influence of two major events: 9/11 and Snowden's 2013 revelations on NSA surveillance programs. The third section is the data collection, which includes how the raw data were compiled, followed by the data analysis section that describes how the data were coded into themes. The evidence of trustworthiness is the next section, followed by the results of the study and the identified themes. The final section is the summary that provides answers to the research questions and a transition to Chapter 5.

Setting

The data were primarily secondary data, which meant that all information regarding the NSA surveillance programs already existed. I was able to harvest data from multiple sources to understand the public sector involvement in the NSA surveillance programs. I intended to gather data in three phases, as stated in Chapter 3, to include the congressional hearings as the primary sources of data because of the legally binding powers of the legislature. However, I found that the executive branch of the U.S. Government secretly granted the technology companies immunity that prevented them from fully cooperating with the Congress to provide the envisaged information regarding the NSA surveillance programs. Zetter (2013) revealed that the Justice Department agreed to grant immunity to participating companies from criminal liability for participating in the surveillance programs. Masnick (2013) reported that Congress provided blanket immunity to companies that helped in the NSA surveillance programs.

Intelligence officers misinformed the Congress to protect the private companies regarding their involvement in the NSA surveillance programs. Sledge (2014) reported that the NSA did not collect information on millions of people in the United States. Greenberg (2013) also apologized for providing an erroneous statement to Senator Ron Wyden. All cover ups and misinformation by the government made it difficult for me to rely on congressional reports as the primary source of data as envisaged in Chapter 3. The setting for the secondary sources of data changed to equal preference to all sources of data of congressional hearings, corporate records, and credible news sources regarding the NSA surveillance programs.

Demographics

The private companies that were researched regarding the NSA surveillance programs were divided into two blocks. The first block was the telecommunications companies that comprised Verizon Wireless, AT&T, Sprint, and T-Mobile. These are the four major telecommunications companies in the United States, and I sought data about these companies regarding their involvement in the NSA surveillance programs. The second block was four companies categorized as the Internet companies that comprised Yahoo, Google, Facebook, and Microsoft. These Internet companies are major software companies that were involved in the NSA surveillance programs.

I further categorized the data into two phases. In the first phase, I identified companies' NSA surveillance activities after the 9/11 terrorists attack in the United States. The second phase was termed as post-Snowden's revelations phase of June 2013. *Harvard Law Review* (2018) stated that current events influenced the activities of the private companies regarding their NSA surveillance programs' involvement because the aftermaths of 9/11 attack and Snowden's revelations influenced corporate decision making. The private companies started to distance themselves from the NSA surveillance programs after the backlash from individual liberties advocates. I decided to identify the timeframe of the private companies' NSA surveillance programs activities after 9/11 and after Snowden's revelations to gauge the reasons why they cooperated with the government and how they cooperated with the government. However, the private companies' activities in these identified two phases were not based on when the information was released to the public, but the time when such activities relating to the

NSA surveillance programs were conducted, thereby providing a chronological timeframe that helped to answer the research questions.

Data Collection

The raw data were divided into two blocks of telecommunications and Internet companies, with an emphasis on understanding the identified companies' activities with regards to the NSA surveillance programs. The nature of the research that was based on secondary data made it imperative to show the evidence of raw data. The raw data are presented below, stating the sources of the data and the relationship of the private companies to the NSA surveillance programs. I created the raw data from a pool of multiple articles about the relationship of the private companies with the NSA. I used the four questions of understanding the official positions of the identified organizations about the NSA surveillance programs, why these organizations held such views, how these organizations got involved in the NSA surveillance programs, and what these organizations perceived as the strengths and weaknesses of their operations in the NSA surveillance programs. I developed the raw data to identify articles, statements, and quotations to draw patterns and comparisons from all of the sources of data that were eventually used to develop codes, categories, and themes.

1. Verizon Wireless- Bankston (2013) stated that Stratton, who was the Verizon Enterprise Solutions President, appreciated that it is important for technology firms to “grandstand a bit, and wave their arms and protest loudly so as not to offend the sensibility of their customers.” Stratton suggested that national security was more important than privacy

concerns. Nakashima and Horwitz (2013) provided a link to the newly declassified documents that showed that Verizon Wireless was compelled to provide metadata of their customers phone records (Appendix A). Condon (2013) reported that the Senate Majority Leader, Reid, stated that Verizon Wireless's decision to provide customers data was done according to congressionally approved law. Reid told reporters, "Right now I think everyone should just calm down and understand that this isn't anything that is brand new, it's been going on for some seven years, and we have tried to often to try to make it better and work, and we will continue to do that." Kavets (2013) reported Verizon Wireless's response to the allegation that it's providing metadata of customers to the government on an on-going basis for 3 months. Milch, Verizon's general counsel, wrote that "Verizon continually takes steps to safeguard its customers' privacy. Nevertheless, the law authorizes the federal courts to order a company to provide information in certain circumstances, and if Verizon were to receive such an order, we would be required to comply." Severin (2014) reported that the German government terminated a contract with Verizon Wireless based on the revelations of Snowden because mass surveillance was conducted in Germany, and it was alleged that the NSA eavesdropped on the mobile phone of German Chancellor, Angela Merkel. Hesseldahl (2014) reported that Verizon Wireless challenged the legality of the NSA's phone data collection program and lost. The court rejected

the argument saying the Supreme Court had ruled in 1979 in favor of the program (Appendix A). The ACLU (2007) expressed their disappointment towards Verizon Wireless when it revealed that it has been turning over customer data without warrants since 2005. Bellows, Executive Director Maine ACLU, stated, “We are outraged that Verizon would breach the privacy of its customers and ignore the constitution by handing over customer records without their knowledge, Verizon must be held accountable for its participation in the illegal spying program.” Fitchard (2014) reported that Verizon Wireless released its first transparency report stating the numbers of Subpoenas, wiretap requests, and warrants it received the previous year.

2. AT&T- Wolf (2006) reported the argument between the Senate Judiciary Committee Chairman Arlen Specter and AT&T CEO Edward Whitacre. The senator asked if AT&T provide customer information to any law enforcement agency. Whitacre refused to explain their company’s involvement in any NSA surveillance by repeatedly saying “We follow the law.” Angwin and Larson (2015) revealed how cooperative AT&T was in the NSA surveillance programs. Angwin and Larson reviewed the documents leaked by Snowden and discovered that the relationship between the NSA and AT&T was considered unique and extraordinarily productive. Angwin and Larson described it as “highly collaborative.” Another lauded the company’s “extreme willingness to help.” The

documents dated 2003-2013 claimed that AT&T gave NSA access to billions on their network and provided technical assistance in wiretapping Internet communications. A document showed the NSA's top-secret budget in 2013 for AT&T partnership was more than twice of Verizon. AT&T installed surveillance equipment in at least 17 of its Internet hubs on U.S. soil. Its engineers are first to try out new surveillance technologies, and a document reminds NSA officials to be polite when visiting AT&T facilities, noting: "This is a partnership, not a contractual relationship." Angwin and Larson were able to identify AT&T as the company behind the Fairview program, and Verizon Wireless was behind the program called Stombrew. Angwin and Larson discovered that the Fairview program forwarded 400 billion Internet metadata records to the NSA while the Stombrew program had not commenced operations. Angwin and Larson also discovered that in 2011, AT&T started to hand over 1.1 billion domestic cellphone calling records a day to the NSA, and the NSA spent \$188.9 million on Fairview program, twice the amount spent on the Stombrew program. Angwin and Larson also reported a statement credited to a retired AT&T technician Mark Klein who claimed that 3 years earlier, he had seen a secret room in a company building in San Francisco where the NSA had installed equipment. Klein also claimed that AT&T was providing the NSA with access to Internet traffic from other telecommunications companies known as "peering," which is a

cooperative arrangement between companies whereby customers of other companies could end up on AT&T network. AT&T spokesman, Brad Burns, replied to the allegations as “We do not voluntarily provide information to any investigating authorities other than if a person’s life is in danger and time is of the essence.” Hatmaker (2018) corroborated the position that AT&T collaborated with the NSA on the surveillance programs. The evidence includes NSA classified documents, public records, and interviews with several former AT&T former employees to identify the eight AT&T facility containing the network equipment that transports large quantities of internet traffic across the U.S and the world. They identified the physical infrastructures with addresses that are used as “peering sites” located in Atlanta, Chicago, Dallas, Los-Angeles, New York City, San Francisco, Seattle, and Washington D.C. Hatmaker also provided a link to the New York Times articles by Charles Savage and James Risen and the ProPublica which first revealed the Fairview program of AT&T. Gallagher and Moltke (2018), provided a detailed map of the AT&T site that helps the NSA and reported that AT&T currently boasts 19,500 “points of presence” (An access point that connects to the internet, located inside a facility that contains routers, servers, and other networking equipment) in 149 countries where internet traffic is exchanged. In response to the revelations, Baker (2018), reported what AT&T Director of Corporate Communications Jim Greer said AT&T was

“Like all companies, we required by law to provide information to government and law enforcement entities by complying with court orders, subpoenas, lawful discovery requests, and other legal requirements.” Jones (2018) reported a secret AT&T program called Project Hemisphere that searches trillions of phone records, analyzes cell data to find where a person is making a call location, the location of the receiver and possibly the details of the call. He reported that when The New York Times reported the program in 2013, it was labeled a partnership with the government as a counter-narcotic tool. However, it was later discovered that it was used to fight against Medicaid fraud to homicides, and “The Daily Beast” reported that it was developed by AT&T and sold to the U.S government for millions of dollars. AT&T document showed that no warrant was required but law enforcement only required to use it in a non-publicized investigation. The report also alleged that AT&T keeps data way back 2008 whereas Verizon keeps data for only one year and Sprint for 18 months. The report also stated that New York Times reported that AT&T has trillions of phone records and more extensive than any other companies and allegedly makes as much as \$1 million annually from different police departments that access Project Hemisphere. Lipp (2016) further corroborated the use of Project Hemisphere by providing a link which showed it was used in at least 28 of DEA centers across the country, and the centers are staffed by federal agents and local law

enforcement, while AT&T employees analyzed on behalf of law enforcement clients. AT&T recommends that information gotten from the program should serve as leads before they are used as routine police work, and a statement of work from 2014 shows AT&T wants to keep Project Hemisphere. Lenzner (2013) informed that NSA pays AT&T, Verizon and Sprint several hundred million dollars a year for access to international calls into the U.S. The leaked inspector general's report stated that AT&T charges \$325 for each activation fee and an additional \$10 daily to monitor the account, while Verizon charges \$775 per tapping an account for the first month and \$500 monthly thereafter. A separate Washington Post reported that NSA pays telcos roughly \$300 million annually to access information, but it is surprising to know that the government pays these companies to maintain watch over their customers even if it constitutes a small fraction of their overall revenues.

3. Sprint- Nakashima (2014), reported that Sprint Corporation was the only telecommunications company to demand legal access to the legal rationale behind the NSA surveillance program requests in 2010 before the revelations of Edward Snowden in June 2013 (Appendix A). However, the company dropped the legal challenge after being shown the legal basis for the surveillance programs. "Sprint believes that substantive legal grounding should be provided when the government requests customer information from carriers," Spokesman for Sprint John Taylor said in a

statement. “Sprint has a long-standing commitment to protecting our customers’ privacy and challenge an order for customer information that we don’t think complies with the law.” Newman (2014) reported Sprint being sued by the United States Government for overcharging federal agencies for wiretapping services. The government asserted that Sprint overcharged for \$21 million worth of services (see Appendix A).

However, Robertson (2015) reported that Sprint settled the government overcharging suit for \$15.5 million.

4. T-Mobile- Whittaker (2018), reported that T-Mobile experienced an uptick in government data demands in its 2017 transparency report in August 14th, 2018 revealing 12% increase in government demands compared to the previous year. He also reported that Google started to publish transparency report indicating government data demands in 2010, but other tech companies started to publish transparency report in 2013 after the revelations of Edward Snowden to counter the backlash from privacy advocacy groups.
5. Yahoo- Menn (2016), reported Yahoo secretly built a custom software program to search its customers’ incoming emails for specific information needed by the National Security Agency. It was done by scanning hundreds of millions of Yahoo mail accounts at the behest of the NSA or FBI by searching for a set of characters either in the body of an email or an attachment. It was alleged that Yahoo’s cooperation with NSA led to

the resignation of Chief Information Officer Alex Stamos in June 2015 because of the decision of Yahoo's Chief Executive Marissa Mayer decision to obey the directive. Yahoo brief response to Reuter's question regarding the report is "Yahoo is a law-abiding company, and complies with the laws of the United States." Toor (2016) reported that Yahoo called on the U.S government to explain why it compelled the company to scan millions of its users' email account in response to Reuter's bombshell revelation. The letter signed by Yahoo's general counsel, Ron Bell addressed to James Clapper, the director of national intelligence called on the government to clarify the "national security orders they issue to internet companies to obtain user data." (see a copy of the letter in Appendix A).

6. Google- Miller (2013) reported Google's Director for Law Enforcement and Information Security Richard Salgado called on the U.S government to improve privacy laws and warns of the threat to open internet and the United States economy. In his testimony before the Senate Judiciary Subcommittee on privacy, technology, and law. He cited studies like one from Forrester and posited that the cloud computing industry could lose \$180 billion, 25% of its revenue by 2016. He warned that countries like Brazil are considering so-called data localization laws, which would require that all data related to Brazilian companies and citizens be stored in Brazil. This he believes "has gained considerable traction since the

revelation of the Prism program,” and companies like Google “could be barred from doing business in one of the world’s most significant markets.” Zetter (2013) reported that the National Security Agency uses the cookies that companies force on users to pinpoint targets they want to hack, according to Edward Snowden’s leaked document. They especially focus on Google’s ubiquitous “PREF” cookie which includes unique numeric codes that can identify the user’s browser to websites. These codes help NSA to hone in on specific machines they want to attack, and they also use these cookies to identify and single out a specific individual’s communications among the massive amount of data it collects through Internet tap. However, the article did not specify how the NSA obtains the Google PREF cookies, whether they hack into Google or they were provided access to the cookies by Google. Marquis-Boire, Greenwald, and Lee (2015) reported the National Security Agency’s most powerful tool of mass surveillance to be XKEYSCORE program. This program makes tracking someone’s internet usage as easy as entering an email address and provides no built-in technology to prevent abuse. The program sweeps internet searches, emails, documents, usernames and passwords, and other private communications. The program gets a constant flow of communications of internet traffic from fiber optic cables with over 700 servers that store from collection sites, and store data for 3 to 5 days and metadata for 30 to 45 days. XKEYSCORE program can be

used to hack computer networks around the world which can be done by typing a few words in Google. Hudson (2013) quoted Google's Executive Chairman Eric Schmidt in his book *The New Digital Age* which portrayed the battle for internet privacy as a "long, important struggle" when he depicted the emergence of Big Data Surveillance tactics as a threat to a free society. "Government operating surveillance platforms will surely violate restrictions placed on them (by legislation or legal ruling) eventually," He wrote in a chapter on the future of terrorism, "The potential for misuse of this power is terrifyingly high, to say nothing of the dangers introduced by human error, data-driven false positives and simple curiosity." Then after Edward Snowden's revelation about the PRISM program, he changed the tone and tweeted on June 7, 2013, that "Google does not have a 'backdoor' for the government to access private user data." Hence, it suggests at minimum Google cooperated with the government within legal boundaries or at maximum offer little resistance to the magnitude of the NSA surveillance programs. The fact that he knew about the NSA surveillance programs before Edward Snowden's revelation makes his book prophetic.

7. Facebook- Simpson and Brown (2013) reported how NSA uses Facebook and other social media profiles to create maps of social connections as part of the revelations by Edward Snowden. New York Times revealed that the surveillance began after a policy change in the year 2010, because prior to

that, “chaining” was only limited to foreign citizens. The new policy allows the analyst to use social media, geo-location information, insurance and tax records, plus other public and private sources to enhance analysis of phone and email records. Snowden showed how analyst use software to create diagrams where a person was at certain times, their traveling companions, their social networks, and email correspondence. Leswing (2016) confirmed how NSA Prism program was used to hack a New Zealand pro-democracy advocate Tony Fullman who was suspected of plotting a violent revolution. The documents provided by Snowden showed a leaked slide which suggests that the NSA was able to directly access Fullman’s Facebook account and get his personal information. However, Facebook CEO Mark Zuckerberg wrote in 2013 that “Facebook is not and has never been part of any program to give U.S or any other government direct access to our servers.” Armasu (2018) reported Facebook defense against the lawsuit by Max Schrem against NSA mass surveillance of European Union citizens on the basis of protection of privacy. However, Facebook defense of the U.S mass surveillance in the lawsuit in Irish court is based on preserving “national security.” However, Nicks (2014), reported that Facebook CEO Mark Zuckerberg wrote a post when he called President Obama “I’ve called President Obama to express my frustration over the damage the government is creating for all of our future. Unfortunately, it seems like it will take a very long time for full

reform,” He continued to say “The internet is our shared space. It helps us connect. It spreads opportunity,” he writes. “This is why I’ve been so confused and frustrated by the repeated reports of the behavior of the U.S. government. When our engineers work tirelessly to improve security, we imagine we’re protecting you against criminals, not our government.”

Perhaps, in the bid to be transparent Bailey (2013) reported Facebook general counsel Ted Ulyot reveal the six months ending Dec.31,2012 the total number of user-data requests Facebook received from all government agencies.

8. Microsoft- Lowe (2013) reported Snowden’s revelation that was provided to The Guardian newspaper that Microsoft assisted the FBI and NSA in encryption bypass to access services which include Outlook.com, Hotmail, Skype, SkyDrive and more. The company allowed agencies to collect video and audio from conversations made via Skype. Techrights (2017) informed that Microsoft as one of the most cooperative software companies because they provided NSA with backdoors to their operating systems and receives payments for their surveillance collaboration. Solove (2016) reported a victory in court for Microsoft in a matter that involved a warrant in searching a certain email account controlled and maintained by Microsoft Corporation that had been stored in Ireland. The court sided with Microsoft and held that Stored Communications Act (SCA) which is

part of the Electronic Communications Privacy Act (ECPA) does not govern data stored beyond U.S borders.

The secondary data were employed for this research, and eight companies were selected as research participants. The nature of the research demanded that I should present the raw data because the data were pulled from numerous sources that align with the research objectives. Four telecommunications companies and four internet companies were researched to understand their involvement in NSA surveillance programs. The raw data were pulled from multiple sources such as NSA congressional hearings analysis, corporate records analysis, and investigative analysis from credible sources. Data were pulled from Walden University library, Google Scholar, and Google Internet search for articles that involved the private sector in NSA surveillance programs. The data were collected daily for a period of 6 weeks after the approval by the IRB on the 15th of August to 30th of September, 2018.

The data were collected for each company (participant) for a minimum of 3 days, whereby full concentration was devoted to any chosen company (participant) within a particular timeframe. The data for each company (participant) were recorded whenever relevant information was discovered during the search for data, and individual company's data were stored in separate folders stating the source, and the information that was collected. The only variation that occurred during data collection from the plan presented in Chapter 3 was that I had no preference for any source of data over the other. I was of the intention in Chapter 3 that the congressional reports will lay the data foundation for

the research, but I discovered during data collection that the government had provided the private companies immunity for their activities in the NSA surveillance programs.

There were limited congressional hearings that involved the NSA surveillance programs, and the immunity provided to the private companies shielded them from providing adequate information on the NSA surveillance programs. All sources of data carried equal weight provided they are credible and relevant to the research. One of the unusual circumstances encountered in the data collection stage was that I encountered numerous information regarding the NSA surveillance programs, which made it a bit difficult to easily discover which information is relevant to the research. I had to diligently read through many articles to be able to discover and record the data that are relevant to the research. Also, I discovered that there was no need to physically visit the locations of the identified companies because all the relevant data are in the library and internet searches, which made the letter of introduction designed in Appendix A not required for data collection.

Data Analysis

Coding is essential to qualitative research because it shows an analytical perspective from where a researcher intends to dissect data for a better analysis. Saldana (2013) explained a code in qualitative inquiry as a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and evocative attribute for a portion of language-based or visual data. Hence, coding is a link between data collection and data interpretation. I used Liamputtong and Ezzy's (2005) recommendation of formatting the

data into three columns of raw data, preliminary code, and final code for the preliminary stage of the data analysis.

Table 1

Coded Data

Raw Data	Preliminary Code	Final Code
<p>Bankston (2013) reported that John Stratton Verizon Enterprise Solutions President was quoted that it is important for technology firms to “grandstand a bit and wave their arms and protest loudly so as not to offend the sensibility of their customers.”</p> <p>Condon (2013) Senate Majority Leader Harry Reid statement regarding Verizon “Right now I think everyone should just calm down and understand that this isn’t anything that is brand new, it’s been going on for some seven years, and we have tried to often to try to make it better and work and we will continue to do that.”</p> <p>ACLU (2007) reported Shenna Bellows, Executive Director Maine ACLU said that Verizon must be held accountable for participating in the illegal spying program.</p> <p>Wolf (2006) reported the statement of AT&T CEO Edward Whitacre “We follow the law”. Angwin and Larson (2015) revealed documents that lauded AT&T as “highly collaborative” and “extreme willingness to help” and “This is a partnership, not a contractual relationship.”</p> <p>Hatmaker (2018) reported AT&T physical infrastructures used as “peering sites” via the Fairview program. Gallagher and Moltke (2018) provided a detailed map of the AT&T map of “points of presence.”</p> <p>Jones (2018), reported that AT&T developed a program called Project Hemisphere that searches trillions of phones records, analyzes cell data. Menn (2016) reported that Yahoo secretly built a custom software program to search its customers’ incoming emails for specific information needed by the National Security Agency.</p> <p>Zetter (2013) reported that the NSA uses Google’s ubiquitous “PREF” cookies that companies force on users to pinpoint targets they want to hack, according to Edward Snowden’s leaked document.</p> <p>Marquis-Boire, Greenwald, and Lee (2015) reported that NSA has a powerful tool of mass surveillance called XKEYSCORE program on Google to track email addresses, internet searches documents, usernames, and passwords.</p> <p>Simpson and Brown (2013), reported how NSA uses Facebook and other social media profiles to create maps of social connections.</p> <p>Leswing (2016) confirmed how Facebook was used to access a New Zealand pro-democracy advocate Tony Fullman.</p> <p>Armasu (2018) reported Facebook defense against a suit against the NSA surveillance in an Irish court which was based on preserving “national security.”</p> <p>Lowe (2013) reported that Microsoft assisted the FBI and NSA in encryption bypass to access services which include Outlook.com, Hotmail, Skype, SkyDrive and more.</p> <p>Techrights (2017), reported Microsoft as one of the most cooperative software companies because they provided NSA with backdoors to their operating systems and receives payments for their surveillance collaboration.</p>	Willingness to cooperate with the National Security Agency, and how they cooperated.	Collaboration
<p>Nakashima and Horwitz (2013), provided newly declassified documents of Verizon Wireless Secondary Order to partake in NSA surveillance (see Appendix A).</p> <p>Baker (2018), reported that AT&T Director of Corporate Communications Jim Greer said “Like all companies, we required by law to provide information to government and law enforcement entities by complying with court orders, subpoenas, lawful discovery requests, and other legal requirements.”</p> <p>Menn (2016), quoted Yahoo’s brief response to Reuter’s question regarding NSA surveillance programs “Yahoo is a law-abiding company, and complies with the laws of the United States.”</p>	Legal Demands	Mandated to comply
<p>Kavets (2013) reported Randy Milch, Verizon’s general counsel letter to employees “Verizon continually takes steps to safeguard its customer privacy.”</p> <p>Hasseldahl (2014), reported that Verizon Wireless challenged the legality of the NSA’s phone data collection and lost (see Appendix A to see court ruling).</p> <p>Fitchard (2014), reported that Verizon Wireless released its first transparency report stating the numbers of subpoenas and wiretap requests.</p> <p>Nakashima (2014), reported that Sprint Corporation was the only telecommunications company to demand a legal basis for NSA surveillance before the revelations of Edward Snowden (see Appendix A).</p> <p>A spokesman for Sprint John Taylor said in a statement “Sprint has a long-standing commitment to protecting our customers’ privacy and challenge an order for customer information that we don’t think complies with the law.”</p> <p>Whittaker (2018)</p>	Transparency	Resistance to the NSA requests

reported T-Mobile experienced an uptick in government data demands in its 2017 transparency report. Toor (2016) reported the displeasure of Yahoo regarding the NSA surveillance programs by asking the director of national intelligence James Clapper to clarify the need for the NSA surveillance programs requests (see Appendix A). Miller (2013) reported Google's Director for Law Enforcement and Information Security Richard Salgado called on the U.S government to improve privacy laws and warns of the threat to open internet and the United States economy. He believes that Edward Snowden's revelation "has gained considerable traction since the revelation of the Prism program," and companies like Google "could be barred from doing business in one of the world's most significant markets." Hudson (2013) quoted Google's Executive Chairman Eric Schmidt after Edward Snowden's revelation and posited that "Google does not have a 'backdoor' for the government to access private user data." Nick (2014), reported that Facebook CEO Mark Zuckerberg called President Obama to express his displeasure with the NSA after the revelations of Edward Snowden "I've called President Obama to express my frustration over the damage the government is creating for all of our future." Bailey (2013), reported Facebook general counsel Ted Ulyot reveal six months ending Dec.31,2012 the total number of user-data requests from governmental agencies in a bid to be transparent.

Severin (2014) reported that the German government canceled Verizon Wireless contract because of Edward Snowden's revelation. Jones (2018), AT&T developed a program called Project Hemisphere and sold to the U.S government for millions of dollars. Lipp (2016) shows that AT&T wants to keep Project Hemisphere. Lenzner (2013), informed that the NSA pays AT&T, Verizon and Sprint several hundred million dollars a year for access to international calls into the U.S. Newman (2014) reported Sprint being sued for \$21 million by U.S government for overcharging federal agencies for wiretapping services (see appendix A). While Robertson (2015) reported Sprint's settlement of \$15.5 million. Techrights (2017) reported Microsoft as one of the most cooperative software companies because they provided NSA with backdoors to their operating systems and receives payments for their surveillance collaboration. Solove (2016) reported a victory in court for Microsoft in a matter that involves a warrant to search a certain account controlled and maintained in Ireland.

Data Request

Data Order Processed

After the coding of the raw data, it became imperative to refine the coded data into categories and themes for proper interpretation to be able to answer the research questions better. Saldana (2013) recommended a transition from data to code, to category and eventually to themes. I designed the second table in line with Saldana's recommendation which comprises four columns of the raw data, final code, category, and the transition into themes.

Table 2

Code to Themes

Raw Data	Final Code	Category	Theme
<p>Bankston (2013) reported that John Stratton Verizon Enterprise Solutions President was quoted that it is important for technology firms to “grandstand a bit and wave their arms and protest loudly so as not to offend the sensibility of their customers.”</p> <p>Condon (2013) Senate Majority Leader Harry Reid statement regarding Verizon “Right now I think everyone should just calm down and understand that this isn’t anything that is brand new, it’s been going on for some seven years, and we have tried to often to try to make it better and work and we will continue to do that.”</p> <p>ACLU (2007) reported Shenna Bellows, Executive Director Maine ACLU said that Verizon must be held accountable for participating in the illegal spying program.</p> <p>Wolf (2006) reported the statement of AT&T CEO Edward Whitacre “We follow the law”. Angwin and Larson (2015) revealed documents that lauded AT&T as “highly collaborative” and “extreme willingness to help” and “This is a partnership, not a contractual relationship.”</p> <p>Hatmaker (2018) reported AT&T physical infrastructures used as “peering sites” via the Fairview program. Gallagher and Moltke (2018) provided a detailed map of the AT&T map of “points of presence.”</p> <p>Jones (2018), reported that AT&T developed a program called Project Hemisphere that searches trillions of phones records, analyzes cell data.</p> <p>Menn (2016) reported that Yahoo secretly built a custom software program to search its customers’ incoming emails for specific information needed by the National Security Agency.</p> <p>Zetter (2013) reported that the NSA uses Google’s ubiquitous “PREF” cookies that companies force on users to pinpoint targets they want to hack, according to Edward Snowden’s leaked document.</p> <p>Marquis-Boire, Greenwald, and Lee (2015) reported that NSA has a powerful tool of mass surveillance called XKEYSCORE program on Google to track email addresses, internet searches documents, usernames, and passwords.</p> <p>Simpson and Brown (2013), reported how NSA uses Facebook and other social media profiles to create maps of social connections.</p> <p>Leswing (2016) confirmed how Facebook was used to access a New Zealand pro-democracy advocate Tony Fullman.</p> <p>Armasu (2018), reported Facebook defense against a suit against the NSA surveillance in an Irish court which was based on preserving “national security.”</p> <p>Lowe (2013), reported that Microsoft assisted the FBI and NSA in encryption bypass to access services which include Outlook.com, Hotmail, Skype, SkyDrive and more.</p> <p>Techrights (2017), reported Microsoft as one of the most cooperative software companies because they provided NSA with backdoors to their operating systems and receives payments for their surveillance collaboration.</p>	Collaboration	The belief in the protection of the country	National Security
<p>Nakashima and Horwitz (2013), provided newly declassified documents of Verizon Wireless Secondary Order to partake in NSA surveillance (see appendix A).</p> <p>Baker (2018), reported that AT&T Director of Corporate Communications Jim Greer said “Like all companies, we required by law to provide information to government and law enforcement entities by complying with court orders, subpoenas, lawful discovery requests, and other legal requirements.”</p> <p>Menn (2016) quoted Yahoo’s brief response to Reuter’s question regarding NSA surveillance programs “Yahoo is a law-abiding company, and complies with the laws of the United States.”</p>	Mandated to comply	Compelled to Act	No Liability
<p>Kavets (2013) reported Randy Milch, Verizon’s general counsel letter to employees “Verizon continually takes steps to safeguard its customer privacy.”</p> <p>Hasseldahl (2014), reported that Verizon Wireless challenged the legality of the NSA’s phone data collection and lost (see Appendix A to see court ruling).</p> <p>Fitchard (2014), reported that Verizon Wireless released its first transparency report stating the numbers of subpoenas and wiretap requests.</p> <p>Nakashima (2014), reported that Sprint Corporation was the only telecommunications company to demand a legal basis for</p>	Resistance to the NSA requests.	Reform	Individual Liberty

NSA surveillance before the revelations of Edward Snowden (see Appendix 4). A spokesman for Sprint John Taylor said in a statement "Sprint has a long-standing commitment to protecting our customers' privacy and challenge an order for customer information that we don't think complies with the law." Whittaker (2018) reported T-Mobile experienced an uptick in government data demands in its 2017 transparency report. Toor (2016) reported the displeasure of Yahoo regarding the NSA surveillance programs by asking the director of national intelligence James Clapper to clarify the need for the NSA surveillance programs requests (see Appendix A). Miller (2013) reported Google's Director for Law Enforcement and Information Security Richard Salgado called on the U.S government to improve privacy laws and warns of the threat to open internet and the United States economy. He believes that Edward Snowden's revelation "has gained considerable traction since the revelation of the Prism program," and companies like Google "could be barred from doing business in one of the world's most significant markets." Hudson (2013) quoted Google's Executive Chairman Eric Schmidt after Edward Snowden's revelation and posited that "Google does not have a 'backdoor' for the government to access private user data." Nick (2014), reported that Facebook CEO Mark Zuckerberg called President Obama to express his displeasure with the NSA after the revelations of Edward Snowden "I've called President Obama to express my frustration over the damage the government is creating for all of our future." Bailey (2013) reported Facebook general counsel Ted Ulyot reveal six months ending Dec.31,2012 the total number of user-data requests from governmental agencies in a bid to be transparent.

Severin (2014) reported that the German government canceled Verizon Wireless contract because of Edward Snowden's revelation. Jones (2018), AT&T developed a program called Project Hemisphere and sold to the U.S government for millions of dollars. Lipp (2016) shows that AT&T wants to keep Project Hemisphere. Lenzner (2013), informed that the NSA pays AT&T, Verizon and Sprint several hundred million dollars a year for access to international calls into the U.S. Newman (2014) reported Sprint being sued for \$21 million by U.S government for overcharging federal agencies for wiretapping services (see appendix A). While Robertson (2015), reported Sprint's settlement of \$15.5 million. Techrights (2017) reported Microsoft as one of the most cooperative software companies because they provided NSA with backdoors to their operating systems and receives payments for their surveillance collaboration. Solove (2016) reported a victory in court for Microsoft in a matter that involves a warrant to search a certain account controlled and maintained in Ireland.

Data Order
Processed

Business-
Transactions

Profit Making

The two tables above showed the progression from the raw data which were inductively used to code, which resulted into categories and eventually led to themes. The process started when I sought for articles about the eight companies that are involved in the NSA surveillance programs. Having researched the articles and analyzed relevant documents to the NSA surveillance programs and the identified companies; I pulled the relevant data related to why and how the identified companies got involved in the NSA surveillance programs, then created and compiled them as raw data. After that, the

relevant data are then collated as the raw data which I manually coded. Basit (2003) compared manual and electronic coding and posited that “the choice will be dependent on the size of the project, the funds and time available, and the inclination and expertise of the researcher” (p.143). However, I used manual coding because the raw data gathered from the eight companies (participants) were viewed as relatively small and were efficiently coded to reflect the substance in the data. After that, the coding led to categories which eventually led to themes.

Four final codes were discovered based on the lens in which I was assessing the created raw data. Auerbach and Silverstein (2003) recommended that researchers should keep a copy of their research concern, theoretical framework, central research questions, goals of the study, and all major issues on one page in front of them to get focused and allay fears because the page focuses on their coding decisions. I used the research concern of understanding the private sector involvement in the NSA surveillance programs, the theoretical framework of policy feedback theory and narrative policy framework, and the research questions of understanding why and how the private companies cooperated with the NSA in the surveillance programs were used to identify the codes from the created raw data.

- The first code discovered from the raw data was a preliminary code of the willingness of the eight identified companies to cooperate with the NSA, and how they cooperated in the surveillance program. The data further suggest that the companies were not only enabling the NSA, but they were working alongside the NSA to provide surveillance of their customers’

data which led to the final code of collaboration. The final code of collaboration transitioned into the category which showed from the raw data that the companies believe in the protection of the country as one of the reasons they collaborated which later transitioned into the theme of national security.

- The second code discovered from the raw data was a preliminary code of legal demands that the companies should provide their customers information to the NSA. The legal demands transition to mandated to comply with the NSA surveillance directive as suggested by the raw data. The code that the companies were mandated to comply transitioned to the category that the companies were compelled to comply because they were acting as law-abiding companies, which later transitioned to the theme that they are not liable for any illegal activity that might have occurred during the warrantless NSA surveillance programs.
- The third code discovered from the raw data was a preliminary code of transparency because the companies started to distance themselves from the NSA surveillance programs after the revelations of Snowden in a bid to be transparent. However, this led to a form of resistance from the companies whereby they sometimes went to the court to challenge the legality of the NSA surveillance requests which led to the final code of resistance. The final code of resistance transitioned to the quest for reform as a category. Appeals were made by these companies that the government

should reform NSA surveillance programs to protect privacy which eventually transitioned into the theme of individual liberty.

- The fourth and the final code discovered from the raw data was a preliminary code of data request from the government that the companies should provide their customers information. The preliminary code later transitioned to the final code as data order processed because the companies felt obligated to process the order in line with their business philosophy of customer satisfaction. The final code of data order process led to the category of business transactions which eventually transitioned to the theme of profit making which is the core reason why a private company is established.

The raw data provided the necessary information that led to the four themes that were discovered with quotations to buttress my submission. It is pertinent to state that two themes developed from the raw data conform with my pre-coded themes of security and individual liberty based on the literature review as proposed in Chapter 3. However, it is imperative to state that discrepancies were observed among the eight companies (participants) concerning their degree of participation in the NSA surveillance programs because not all the eight companies provided a clear presentation of all the four themes. A case in point is that AT&T did not provide any evidence of transparency before I identified the final code of resistance. However, information from multiple companies (participants) suggests AT&T is an outlier in that regard since the majority of the companies conform with the narrative of resistance. Either by distancing themselves from

the NSA surveillance programs by publicly denying their involvement in the program or by going to court to challenge the legality of the programs, which resulted in the acceptance of the final code of resistance as one of the final codes derived from the raw data. Discrepancies are invalidated whenever multiple companies (participants) comport to a particular trend from the information derived from the raw data.

Evidence of Trustworthiness

The credibility of the research was implemented as planned in Chapter 3 because I ensured the use of reflexivity approach whereby my past experiences and values did not color the creation of the raw data. I ensured internal validity by providing all the relevant information regarding the private companies' involvement in the NSA surveillance programs. The raw data that were used to develop the codes, which eventually led to the themes were identified from a pool of numerous articles and original document analysis, and no personal preferences, experiences, nor values were used to compile the raw data. However, the coding of the raw data was influenced by the lens that I was assessing the data which was based on the purpose of the research, nature of the study, central research questions, theoretical framework, and the significance of the study. The raw data provided evidentiary value that reflects the activities of the private companies regarding the NSA surveillance programs from different perspectives that relates to the research concerns, and are fact based.

The transferability of the research was implemented as planned in Chapter 3 because I ensured the use of triangulation whereby multiple sources provided data which provided cross verification before themes eventually emerged. The raw data comprises

eight companies (participants), four major telecommunications companies, and four major Internet companies which produced a balanced representation of the private sector involvement in the NSA surveillance programs. The raw data provided information from the eight identified companies (participants) in the United States of America. The raw data comprises multiple sources of data from reports from congressional hearings, corporate statements of executives that runs these organizations, and credible investigative journalism that produces original documents to buttress their investigations.

The data were discovered from a pool of numerous articles and documents analysis, and I endeavored to provide multiple sources of data for each company's contribution for cross verification which ensures the authenticity of the data. The results of the research can be applied to similar situations because I provided multiple sources of data from all the eight companies (participants) which enhances the credibility of the data. I also provided different points of view from the companies (participants) before the data were transcribed into codes, then to categories, and eventually themes to answer the research concerns.

The dependability of the research was implemented as planned in Chapter 3 because accurate citing of the sources of data was provided in the raw data. The raw data I created provided adequate information about the NSA surveillance programs via stating the sources of the information with the names of the author, and the year of publication. The raw data provided the sources and links where the corroborating documents were provided in the appendix section. The raw data provided statements by the corporate executives of some of the eight identified companies to signify corporate records, and the

sources of these statements are adequately cited. The accurate citing of the sources of information provides an audit trail for whosoever want to identify or confirm the sources of the information which in turn provides more credibility to the research.

The confirmability of the research was implemented as planned in Chapter 3 because the I created a raw data from credible sources which include analysis of congressional hearings, public statements by corporate executives from some of the eight identified companies (participants), investigative sources with reputable institutions, and documents to buttress the data were provided for document analysis. Accurate citing of the sources of information was provided, which includes the name of the author and the year of publication to provide an audit trail. I also used cross verification of data from multiple credible sources and ensured that data are trending towards the same conclusions before they are included in the raw data. I also used the reflexivity approach to create the raw data to reduce the influence of value judgment, whereby my biases, values, and experiences were divorced from compiling information regarding the NSA surveillance programs. I believe that creating raw data from a pool of numerous articles has provided a unique perspective to the understanding of the private companies' involvement in the NSA surveillance programs. It has also created a high degree to which the findings can be corroborated by others who intend to investigate the research or add more value to scholarship.

Results

The data collected was used to answer the two central research questions for the research, which are:

Private Companies Cooperate With NSA

Why did the private internet and telecommunications companies cooperate with the NSA surveillance programs activities? The answers to this question were obtained from the raw data compiled as I was able to elucidate on the question through the process of creating codes to categories and which eventually led to themes. The data showed three reasons why the private companies cooperated with the NSA. The first reason is national security which was discovered through data analysis that led to the discovery of collaboration as a code, which led to the discovery of a category which explained that these companies believed in the protection of the country, and which eventually led to the theme of national security as a pattern from the data collected. Bankston (2013) reported that John Stratton Verizon Enterprise Solutions President was quoted that it is important for technology firms to ‘grandstand a bit and wave their arms and protest loudly so as not to offend the sensibility of their customers.’ Condon (2013) reported Senate Majority Leader Harry Reid’s statement regarding Verizon “Right now I think everyone should just calm down and understand that this isn’t anything that is brand new, it’s been going on for some seven years, and we have tried to often to try to make it better and work and we will continue to do that.” Wolf (2006) reported AT&T CEO Edward Whitacre’s statement “We follow the law.” Armasu (2018) reported Facebook defense against a suit against the NSA surveillance programs in an Irish court that they cooperated because it is based on preserving “national security.”

The data explained the second reason why the private internet and telecommunications companies cooperated with the NSA surveillance programs was that

they felt they had no liability when they were secretly collecting data of Americans without adequate legislative and judicial oversight. This conclusion was reached through the process of data analysis that led to the discovery that they were mandated to comply as a code, which led to the led the discovery of them being compelled to act as a category which eventually resulted to the theme of no liability. Nakashima and Horwitz (2013) provided newly declassified documents of Verizon Wireless Secondary Order to partake in NSA surveillance programs (see Appendix A for document analysis). Baker (2018) reported AT&T Director of Corporate Communications Jim Greer's statement "Like all companies, we are required by law to provide information to government and law enforcement entities by complying with court orders, subpoenas, lawful discovery requests, and other legal requirements." Menn (2016) reported yahoo's brief response to Reuter's question regarding NSA surveillance programs "Yahoo is a law-abiding company, and complies with the laws of the United States."

The data explained the third reason why the private companies cooperated with the NSA surveillance programs without adequate judicial and legislative oversight was for profit making. This conclusion was reached through the process of data analysis that led to the discovery of the need to process data order as a code, which led it to be seen as standard business transactions as a category, which resulted into a theme of profit making as a motive. Jones (2018) reported that AT&T developed a program called Project Hemisphere and sold it to the U.S government for millions of dollars. Lipp (2016) provided a link that showed that AT&T wants to keep Project Hemisphere. Lenzner (2013) reported that NSA pays AT&T, Verizon and Sprint several hundred million

dollars a year for access to international calls into U.S. Newman (2014) reported Sprint being sued for \$21 million by U.S government for overcharging federal agencies for wiretapping services (Appendix A). While Robertson (2015) reported Sprint's settlement of \$15.5 million. Techright (2017) reported that Microsoft provided NSA with backdoors to their operating systems and receives payments for their surveillance collaboration. Lowe (2013) also confirm that Microsoft receives payment for their surveillance collaboration.

How Private Companies Cooperated With Surveillance

How did the private internet and telecommunications companies cooperate with the Government NSA surveillance programs? The raw data provided evidence of how the internet and telecommunications companies helped in the NSA surveillance programs in three ways. The first way was that the companies directly provided their customers' information to the NSA; the second way was that the companies granted the NSA access to their networks in the form of collaboration; while the third way was when the NSA hack the companies' network while the companies provided little or no resistance. The answers to this research question were obtained from the raw data I created, and the methods that showed how the surveillance programs were achieved cut across all the four themes of national security, no liability, individual liberty, and profit making.

The first way how the private internet and telecommunications cooperated with the Government NSA surveillance programs was when the companies directly provided their customers information to the government. Kavets (2013) reported Verizon Wireless response to the allegation that it is providing metadata of customers to the government on

an on-going basis for three months. Randy Milch, Verizon's general counsel, wrote in a letter to employees "Verizon continually takes steps to safeguard its customer's privacy. Nevertheless, the law authorizes the federal courts to order a company to provide information in certain circumstances, and if Verizon were to receive such an order, we would be required to comply." Toor (2016) reported that Yahoo called on the U.S government to explain why it compelled the company to scan millions of its users' e-mail account in response to Reuter's bombshell revelations (see a copy of the letter in Appendix A). Jones (2018) reported that AT&T developed a program called Project Hemisphere that allows the searches of trillions of phones records, and analyzes data. Lipp (2016) reported that Project Hemisphere are staffed by federal agents and local law enforcement, while AT&T employees analyze data on behalf of law enforcement clients. Menn (2016) reported that Yahoo secretly built a custom software program to search its customers' incoming mails for specific information needed by the National Security Agency.

The second way how the private Internet and telecommunications companies cooperated with the Government NSA surveillance programs was that the companies granted the NSA access to their networks in the form of collaboration. Angwin and Larson (2015) reported the revealed document which lauded AT&T as "highly collaborative" and "extreme willingness to help" and "This is a partnership, not a contractual relationship." He reported a statement credited to a retired AT&T retired technician Mark Klein in a lawsuit filed against AT&T in the year 2006. He claimed that 3 years earlier, he had seen a secret room in a company's building in San Francisco

where NSA had installed equipment which was used to access internet traffic from other telecommunications companies known as “peering” which is a cooperative agreement between carriers. Hatmaker (2018) reported the physical infrastructures used as “peering sites” by AT&T, and he reported the AT&T surveillance program used for the “peering” as Fairview Program. Gallagher and Moltke (2018) provided a detailed map of the AT&T map of “point of presence.” Zetter (2013) reported that the NSA uses Google’s ubiquitous “PREF” cookies that companies force on users to pinpoint targets they want to hack, according to Edward Snowden’s leaked document. Lowe (2013) reported that Microsoft assisted the FBI and the NSA in encryption bypass to access services which includes Outlook.com, Hotmail, Skype, SkyDrive and more. Techright (2017) confirmed that Microsoft as one of the most cooperative software companies because they provided NSA with a backdoor to their operating systems.

The third way how the private internet and telecommunications companies cooperated with the Government NSA surveillance programs was when the NSA hacked the companies’ network while the companies provided little or no resistance. Marquis-Boire, Greenwald, and Lee (2015) reported that the NSA has a powerful tool of mass surveillance called XKEYSCORE program used on Google to track email addresses, internet searches, documents, usernames, and passwords. Simpson and Brown (2013) reported that NSA uses Facebook and other social media profiles to create maps of social connections, while Leswing (2016) confirmed how the NSA used the Prism Program to hack a New Zealand pro-democracy advocate named Tony Fullman.

However, it is pertinent to state that the theme of individual liberty does not explain why the private internet and telecommunications companies cooperate in with the NSA surveillance program activities, nor did it explain how the private Internet and telecommunications companies cooperate with the Government NSA surveillance programs. This theme served as a discrepant case because the theme of individual liberty answered the opposite of the research questions. Why did the private Internet and telecommunications companies did not want to cooperate with the NSA surveillance programs activities was answered by discovering resistance to the NSA request as code, which later developed to a be reform as a category, which eventually resulted to individual liberty as a theme. It posited that the private companies did not want to cooperate by stating the importance of privacy which is needed to guarantee individual liberty. Kavets (2013) reported Randy Milch, Verizon's general counsel letter to employees which stated that "Verizon continually takes steps to safeguard its privacy." Whittaker (2018) reported T-Mobile experienced an uptick in government data demands in its 2017 transparency report to counter the backlash from privacy advocacy groups. Toor (2016) reported the displeasure of Yahoo regarding the NSA surveillance programs by asking the director of national intelligence James Clapper why they compelled the company to scan millions of its users' email account in a bid to protect privacy (see a copy of the letter in Appendix A). Miller (2013) reported Google's Director for Law Enforcement and Information Security Richard Salgado called on the U.S government to improve privacy laws and warns of the threat to open internet and the United States economy. He believes that Snowden's revelation "has gained considerable traction since

the revelation of the Prism program,” and companies like Google “could be barred from doing business in one of the world’s most significant markets.” Nick (2014) also reported Facebook CEO Mark Zuckerberg called President Obama to express his displeasure with the NSA after the revelations of Snowden “I’ve called President Obama to express my frustration over the damage the government is creating for all of our future.”

However, the raw data also provided evidence of how the private internet and telecommunications companies did not want to cooperate with the Government NSA surveillance programs in two ways. The first way that the private companies did not want to cooperate with the NSA surveillance programs is by challenging the legality of the programs at the courts. Hasseldahl (2014) reported that Verizon Wireless challenged the legality of the NSA’s phone data collection and lost (see Appendix A to see court ruling). Nakashima (2014) reported that Sprint Corporation was the only telecommunications company to demand the legal basis for the NSA surveillance programs before Edward Snowden’s revelation (see the appendix for a legal challenge). A spokesman for Sprint John Taylor said in a statement, “Sprint has a long-standing commitment to protecting our customers’ privacy and challenge an order for customer information that we don’t think complies with the law.” Solove (2016) reported a victory for Microsoft in a matter that involved a warrant in searching a specific account controlled and maintained in Ireland.

The second way how the private Internet and telecommunications companies did not want to cooperate in the NSA surveillance programs is by openly criticizing the extent to which the NSA executed their surveillance programs. Hudson (2013) quoted

Google's Executive Chairman Eric Schmidt after Snowden's revelation and posited that "Google does not have a 'backdoor' for the government to access private user data."

Bailey (2013) reported Facebook general counsel Ted Ulyot reveal 6 months ending Dec.31,012 the total number of user-data requests from governmental agencies in a bid to be transparent and protect privacy. Nick (2014) reported Facebook CEO Zuckerberg called President Obama to express his displeasure with the NSA surveillance programs after the revelations of Snowden "I've called President Obama to express my frustration over the damage the government is creating for all of our future."

Haven explained the findings of the research to answer the research questions, the table below provides a comprehensive picture of the themes and the answers to the research questions. The table is not the same as two tables proposed in the proposal stage of the dissertation in Chapter 3, as the inclusion of the raw data table in data collection stage makes only one table necessary to capture the entire research findings. The first column states the central research questions, and the themes discovered to answer the research questions, while the second column states the answers to the research questions and how the themes that were used to answer the research questions were discovered.

Table 3

Research Findings

Why did the private companies participate in the NSA surveillance programs?	How did the private companies participate in the NSA surveillance programs?	The preservation of national security as a theme to why the private companies participated in the NSA surveillance programs.	No liability as a theme to why the private companies participated in the NSA surveillance programs.	Profit- making as a theme to why the private companies participated in the NSA surveillance programs.	The protection of individual liberty as a theme of why private companies did not want to participate in NSA surveillance programs.
1.The preservation of national security. 2. No liability. 3. profit-making.	1. The private companies directly provided their customers information to the government. 2. The private companies granted the NSA access to their networks in the form of collaboration. 3. The NSA hacks the private companies' network while the companies provided little or no resistance.	This theme was discovered from the raw data created by the researcher. A preliminary code of the willingness to cooperate was discovered which led to a final code of collaboration, which resulted into the category of the belief in the protection of the country, which eventually transitioned into the theme of national security.	This theme was discovered from the raw data created by the researcher. A preliminary code of legal demands was discovered which led to a final code of mandated to comply, which resulted into the category of compelled to act, and which eventually transitioned into the theme of no liability.	This theme was discovered from the raw data created by the researcher. A preliminary code of data request was discovered which led to a final code of data order processed, which resulted into the category of business transactions, and which eventually transitioned into the theme of profit making.	This theme was discovered from the raw data created by the researcher. A preliminary code of transparency was discovered which led to a final code of resistance, which resulted into the category of reform, and which eventually transitioned into the theme of the protection of individual liberty.

Summary

The raw data created from the multiple secondary data provided adequate information which established four themes of national security, no liability, profit making, and individual liberty that were used to answer to the research questions. The answers to the research question of why did the private Internet and telecommunications companies cooperate with the NSA surveillance program activities showed with clear evidence that the preservation of national security, the belief that these companies are not liable for their actions, and the desire to make profit as the reasons why they cooperated with the government NSA surveillance programs. However, the protection of individual liberty provided a discrepant outcome when it explained that it served as a motivation to why the private companies did not want to cooperate with the NSA surveillance programs activities. The research question of how did the private internet and telecommunications companies cooperate with the Government NSA surveillance programs shows that it was done in three ways. The first way is that the private companies directly provided the government their customers' information in some instances. The second way is that the private companies granted the NSA access to their networks in the form of collaboration, while the third way is that the NSA hacked the private companies' network while the companies provided little or no resistance. The findings to these central research questions are interpreted in chapter 5 to provide more clarity to the research concern and provide an assessment to the validity of the existing literature regarding the NSA surveillance programs.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of the research was to understand how the federal government gained compliance of the private sectors to agree to execute public policy and why the private sector abided by the dictates of the government even if it was against their core values. The nature of the study was qualitative to provide a better understanding of how and why Internet and telecommunications companies provide customers' information to the government. The research was conducted to understand whether to include or exclude the private sector in a holistic evaluation of public policies to determine whether the private sector influences public policy outcome or private sector only abide by the dictates of the government in executing public policy. The study of the private sector participation in the NSA surveillance programs might provide insights into the relationship between the private and public sector in public policy.

I found three reasons why the private Internet and telecommunications companies cooperated with the NSA surveillance programs activities: the preservation of national security, the belief that they do not have any liability because they were compelled to participate, and because they were making a profit from the NSA surveillance programs. However, a discrepant case revealed that the private Internet and telecommunications companies did not want to cooperate with the NSA surveillance programs activities because they desired to protect personal privacy to guarantee individual liberty. I also revealed three ways how the private Internet and telecommunications companies cooperated with the government NSA surveillance programs. The private companies

provided their customers' information directly to the government, they granted the NSA access to their networks in the form of collaboration, and the NSA hacked the private companies' network while the companies provided little or no resistance. However, a discrepant case revealed two ways how the private Internet and telecommunications companies did not want to cooperate with the government NSA surveillance programs by challenging the legality of the surveillance programs at the courts and publicly criticizing the extent to which the NSA surveillance programs were executed.

Interpretation of the Findings

The findings confirmed and extended the existing peer-reviewed literature described in Chapter 2. My findings confirmed existing literature on two ideological spectrums of those who supported the NSA surveillance based on the preservation of national security and those who opposes the NSA surveillance programs to protect personal privacy to guarantee individual liberty. I also confirmed the negative consequences of the NSA surveillance programs by explaining why and how the companies were trying not to cooperate with the NSA surveillance programs to counter the backlash the programs have generated. Moreover, I confirmed the ability of the NSA surveillance programs to store and retrieve data when raw data produced evidence of the capacity of the NSA to get data by stating the three ways of how the private companies cooperated with the government NSA surveillance programs. I confirmed a rationale why the private companies provided their customers' information to the government to be the immunity granted to the companies. Government immunity to the private companies made them comply with the directive.

The research extended knowledge to the discipline by providing comprehensive motives to why the private Internet and telecommunications companies cooperated with the NSA surveillance programs activities. I revealed that the preservation of national security, the belief that the private companies do not have any liability because they were compelled to participate, and the desire for these companies to make a profit encouraged them to support the NSA surveillance programs. I revealed that the protection of individual liberty was a reaction to the backlash to the revelations by Snowden regarding the NSA surveillance programs activities. Individual liberty was meant to be the basis on why the private companies did not want to cooperate with the NSA. I explained the relevance of major events in determining the activities of the NSA surveillance programs. I provided a timeline that proved that the quest for the preservation of national security was due to the effect of 9/11 terrorists' attacks that promoted the preservation of national security as a motive on why the private companies cooperated with the NSA. The revelations by Snowden in 2013 promoted the quest for the promotion of individual liberty as a reaction to the capacity and extent of the NSA surveillance programs.

I also extended knowledge to the discipline by explaining how the private companies cooperated with the NSA. I provided evidence on how the private companies cooperated. The three ways of how the private companies cooperated with the NSA surveillance programs added to the body of knowledge by providing information on the extent and method in which NSA surveillance programs were conducted. The research also added to the body of knowledge by providing a narrative of how the private companies did not want to cooperate with the NSA surveillance programs, which was

also a reaction to Snowden's revelation. I showed the method in which the private companies resisted the NSA by challenging the legality of the surveillance programs at the courts and by publicly criticizing the extent to which the NSA surveillance programs were executed.

The theoretical frameworks used for this research were the policy feedback theory and narrative policy framework. Policy feedback theory is based on the premise that historical political/policy precedent determines the new politics/politics of the present. The policy commitment of the past led to the creation of FISC to curb the excesses of the executive branch of government, which determines or impacts the operations NSA surveillance programs of the present. A deviation from precedent not to seek warrants for surveillance from FISA court in the United States formed the basis for the preservation of national security as an excuse on why the NSA did not follow the historical precedent of FISA court approval. On the other hand, some scholars believe that warrantless NSA surveillance is an affront to privacy, which threatens individual liberty. The two contending viewpoints resulted in two schools of thought of those who favor national security and those who favor individual liberty. The narrative policy framework was used to analyze the divergent views regarding the benefits/drawbacks of the NSA surveillance programs. I used the narrative policy framework as a guide to analyze how the advocates of the NSA surveillance programs who favors the preservation of national security to prevent terrorists attack, and the opponents of the surveillance programs who emphasize the need to protect privacy to guarantee individual liberty are both marketing their views to influence public opinion. I was able to precode the themes of security and individual

liberty at the start of the research based on existing literature and the choice of the theoretical framework that guided the research.

Consequently, in the raw data created from multiple sources, I was also able to identify national security and individual liberty as valid themes, in conformity with the precoded themes that were identified using the theoretical framework. However, I found the theme of national security as one of the reasons why the private companies cooperated in the NSA surveillance activities, while individual liberty was revealed as a reason why the private companies did not want to cooperate in the NSA surveillance programs.

Policy feedback theory, which emphasizes precedent as a guide to public policy, was also instrumental to the discovery of two more additional themes from the raw data on why the private companies cooperated with the NSA in the surveillance programs. The belief that the private companies do not have any liability because they were compelled is a deviation from the precedent from seeking the approval of FISA courts, and the excuse for cooperating with the NSA for profit making is also a deviation from precedent. Information about how the private companies were cooperating with the NSA, and how the private companies did not want to cooperate with the NSA, were derived from the raw data that were used to determine the themes. The theoretical framework used for the research provided the structure for the research that ensured that the research stayed within the scope of the study to answer the research questions.

Limitations of the Study

The limitations of the study were the same as envisaged because creating the raw data from multiple sources of data was a challenge. The concentration on the private sector participation allowed me to extract the relevant information from the aggregate data. However, I decided to compile articles that were relevant to each company (participant) together, with sources and dates when creating the raw data. Inferences were drawn from the sources of information to understand why and how the NSA executed the surveillance programs. The sourcing and compilation of data as envisaged in the proposal stage was the same during the execution of the study. The deficiencies of the case study approach did come to bear during the execution of the research because I could not quantify the data collected on each company (participant), as some companies provided more relevant information than the others. However, the case study approach provided an in-depth understanding of the NSA surveillance programs from the private sector perspective. I stopped reviewing here due to time constraints.

Recommendations

This research is a contemporaneous topic that produces revelations on a regular basis, which makes the research a reservoir of knowledge about the NSA surveillance programs. This research should be seen as a reference point for other scholars to generate new ideas because limited investigations have been conducted regarding the NSA surveillance programs. I recommend further studies be conducted to complement the findings of the research that has identified the reasons why and how the private companies cooperated with the government in the NSA surveillance programs. I

recommend further studies due to the limitations of the research in some areas such as, the inability to determine the major or the most important reason why the private Internet and telecommunications companies cooperate with the NSA surveillance programs. I recommend the following studies:

- Further studies are recommended to understand what is the most important reason why the private companies cooperated with the NSA surveillance programs between the preservation of national interests, the belief that they have no liability, and the quest for profit making for further clarifications about the topic.
- I recommend further studies in the area of internal operations of the identified eight companies (participants) to determine why some companies are willing to cooperate with the government than the others. The investigation revealed that AT&T was more willing to cooperate with the NSA than the other telecommunications companies, while Sprint Corporation was the only telecommunications company that attempted to resist the NSA before the revelations of the Edward Snowden. It is worth investigating perhaps, the corporate vision or mission statements of these companies to determine the extent of cooperation, whether the nature of their businesses permit more cooperation or resistance, or the companies' executive make up influences their corporate decisions regarding the NSA surveillance programs.

- I also recommend further studies to understand how these companies cooperated with the government. Perhaps, the nature of their businesses determines how they cooperate, and whether the location of their businesses also influences their cooperation because Microsoft sued the government on the basis that their server was in another country (Ireland).
- I recommend further study in the area of comparative analysis in the area of surveillance between the United States and another country to be able to understand if this cooperation between the companies (participants) and the government is only peculiar to the United States or is universal to all countries or multiple countries.
- I recommend further research in the area of direct sourcing of information regarding the NSA surveillance programs from the direct participants like, the conduct of interviews with the executives of these organizations to be able to elicit further information to why and how they cooperated with the government in the NSA surveillance programs.

Implications

This research was conducted to understand private sector participation in public policy by using NSA surveillance programs as a case study to provide insights into private-public sector collaboration. The research was expected to provide the basis to either include or exclude the private sector analysis in a holistic evaluation of public policy, which might provide useful knowledge to public policy practitioners/observers

whether to incorporate private-public analysis for a comprehensive evaluation of public policy for better public policy performance.

The completion of the research revealed the enormous power of the government to influence the private companies to abide by the government's bidding which is evident with the government's ability to convince private companies that they are not liable when they secretly provided their customers information to the government. The research also revealed that the government has enormous power to coerce the private companies to abide by its directives to achieve a public policy goal. The research also revealed the influence of profit motivation as a factor for private companies' involvement in public policy. It is noteworthy to state that the government might not get the level of private sector collaboration if they were not paid for their services in NSA surveillance programs. The research also revealed the influence of current events to public policy because it shapes the mood of the country which in turn influences public policy. The 9/11 terrorists attack of the year 2001 influenced the desire for the preservation of national security, and the willingness to deviate from precedent to secure FISA warrant for NSA surveillance programs due to the nationalistic mood of the country. While Snowden's revelations of the year 2013 changed the mood of the country, whereby the consciousness for the protection of personal privacy to safeguard individual liberty was encouraged. It is important to state that resistance to the NSA surveillance programs accelerated when Snowden exposed the activities of the NSA surveillance programs. The government gains compliance of the private sectors to agree to execute public policy through the instruments of coercion, influence, and persuasion.

The government coerced the private companies to provide their customers' information to the NSA surveillance programs without adequate legislative and judicial oversight. The government also used the instrument of influence to convince the private companies to comply by stating the need to preserve national security when the mood of the country favored more security after the 9/11 terrorist attack. The government also used the instrument of persuasion by promising the private companies that they are not liable to any charges regarding the NSA surveillance programs, and they also paid these companies for their services which increases their profitability which served as a form of inducement to cooperate.

The above analysis implies that the government has enormous power to influence public policy to compel private companies to abide by its directives. However, it must also be noted that the ability to compel these private companies alone cannot guarantee compliance, but the benefit of profit motivation is also needed to gain compliance, while the mood of the society which is influenced by current events are needed to sustain the compliance to government's directive. The research implies that private sector analysis is necessary for the proper understanding of public policy because it shows the extent of collaboration for better public performance. Governmental power and the willingness of the government to exert such power is paramount to public policy execution, and the interest of the private companies is also paramount to the success of public policy execution. Societal mood possesses enormous influence to sustain public policy because it changes the desire of private companies to collaborate with the government. The positive social change implication for the research has shown that it is necessary to

include private sector analysis in a comprehensive review of public policy because of the enormous private-public sector interdependencies in public policy implementation.

The cooperation or collaboration of the private sector is contingent upon their liability exposure to the policy, while self-interest (profit-making) is paramount for effective cooperation or collaboration of the private sector in public policy. Private sector cooperation or collaboration in public policy is fluid because of the influence of major events that changes the mood of the society affects and guides the actions of the private companies, which in turn determines if a public policy will be sustained. For public policy practitioners/observers to thoroughly evaluate public policy, they must assess the relationship between the private and the public sector because public policy is dependent on both sectors for effective implementation.

Conclusion

This research was about the use of a case study approach to provide an in-depth understanding of a particular case of why and how the Internet and the telecommunications companies provided their customers' information to the government without adequate legislative and judicial oversight. The purpose of the research is to determine how the government gained compliance of the private sector and why the private sector abided by the dictates of the government by cooperating in the NSA surveillance programs. The research revealed three reasons why the private companies abided by the directive of the government in the NSA surveillance programs as the preservation of national security, the belief that they do not have any liability because they were compelled to participate and because they were making a profit. The research

also provided a discrepant case of why they did not want to cooperate with the government because of the desire to protect personal privacy in order to guarantee individual liberty.

The research also revealed three ways how the private companies cooperated in the NSA surveillance programs to be, they provided their customers information directly to the government, they granted the NSA access to their networks as a form of collaboration, and the NSA hacked the private companies' network while they provided little or resistance. The research also revealed two ways how the private internet and telecommunications companies did not want to cooperate with the government in NSA surveillance programs by challenging the legality of the surveillance programs in courts, and by publicly criticizing the way the programs were conducted to show their displeasures and frustrations towards the NSA surveillance programs.

Based on the above findings, the first take home message of this research is that the private companies cooperate with the government even when it is against their core values when they perceive that they will not be held liable for their actions. When it serves their corporate interest (profit-making), and they change their position whenever major events occur in line with the mood in the country because they favored national security after the 9/11 terrorist attack, and changed position to individual liberty after the revelations of Snowden. The second take home is that the degree to how the private companies cooperate with the government is dependent on what is convenient to them, perhaps they provide back door to their network based on the nature of the business. Perhaps their internal organization's preference/culture also determines how they provide

customers information directly to the government or permit them to allow the government to hack into their network. While current events determine how or how not to cooperate with the government because changes in the mood in the country affects the private companies' responses to public policy. The third and final take home message is that it is necessary to include private sector analysis in a comprehensive public policy review because of the high level of inter-dependence, interactions and connections between private-public sector in public policy implementation have made private sector relevant in the public policy process.

References

- ACLU. (2007). Verizon admits turning over customer records to the federal government. ACLU. Retrieved from <https://www.aclu.org/.../verizon-admits-turning-over-customer-records-federal-govern...>
- Anderson, T. (2014). *Toward institutional reform of intelligence surveillance: A proposal to amend the foreign intelligence surveillance act*. Harvard Law & Policy Review, 8(2), 413-436.
- Angwin, J. & Larson, J. (2015). NSA spying relies on AT&T's extreme willingness to help. *ProPublica*. Retrieved from <https://www.propublica.org/.../nsa-spying-relies-on-atts-extreme-willingness-to-help>
- Armasu, L. (2018). Facebook defends U.S. mass surveillance of EU citizens security' reasons. Retrieved from <https://www.tomshardware.com/.../facebook-defends-us-mass-surveillance,36882.html>
- AT&T Helped NSA Spy on Internet Traffic. (2015). The property of John Birch Society. *New American*, 31(17), 7.
- Auerbach, C. F., & Silverstein, L. B. (2003). *Qualitative data: An introduction to coding and analysis*. New York, NY: New York University Press.
- Austin, L. (2015). Surveillance and the rule of law. *Surveillance & Society*, 13(2), 295-299.
- Bailey, B. (2013). Facebook reveals number of requests under government internet surveillance program. *Mercury News*. Retrieved from

<https://www.mercurynews.com/.../facebook-reveals-number-of-requests-under-govern>

Baker, S. (2018). AT&T buildings around US reportedly used as part of NSA spying... *Business Insider*. Retrieved from <https://www.businessinsider.com/att-buildings-around-us-reportedly-used-as-part-of-n>

Bankston, K. (2013). Telcos like Verizon and AT&T are silent on NSA surveillance. *SLATE, New America, and ASU*. Retrieved from www.slate.com/.../telcos_like_verizon_and_at_t_are_silent_on_nsa_surveillance.html

Barton, G., & Ashkan, S. (2014). NSA surveillance program reaches 'into the past' to retrieve, replay phone calls. *Washington Post*. Retrieved from <https://www.washingtonpost.com/.../nsa-surveillance-program-re>

Basit, T. N. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational Research, 45*(2), 143-54.

Bauerlein, M. & Jeffery, C. (2016). *Opposing viewpoints: The impact of the tech giants*.

Berman, E. (2016). The two faces of the foreign intelligence surveillance court. *Indiana Law Journal, 91*(4), 1191-1250.

Burkholder, G. (2010). *Doctoral research: Why critique research?* Baltimore, MD:

Author

Byman, D., & Wittes, B. (2014). Reforming the NSA. *Academic Journal Foreign Affairs, 93*(3), 127-138.

Clayton, M. (2013). Snowden leaks give new life to lawsuits challenging NSA surveillance program. *Christian Science Monitor, N*.

- Condon, S. (2013). NSA's Verizon records collection: "Calm down," Reid says. CBS News. *CBS NEWS*. Retrieved from <https://www.cbsnews.com/news/nsas-verizon-records-collection-calm-down-reid-says/>
- Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage Publications.
- Creswell, J. W. (2013). *Qualitative inquiry & research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- David Simpson, D, & Brown, P. (2013). NSA mines Facebook, including Americans' profiles. *CNN*. Retrieve from <https://www.cnn.com/2013/09/30/us/nsa-social-networks/index.html>
- Fitchard, K. (2014). Verizon's first transparency report sheds no light on NSA data collection. *Gigaom*. Retrieve from <https://gigaom.com/.../verizons-first-transparency-report-sheds-no-light-on-nsa-data-c>
- Galagher, R., & Moltke, H. (2018). The NSA's hidden spy hubs in eight U.S. cities. *The Intercept*. Retrieved from <https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/>
- Glenn Greenwald, G. & MacAsKill, E. (2013). NSA Prism Program yaps into user data of Apple, Goggle and others. *Guardian*. Retrieved from <http://www.guardian.co.uk/world/2013/jun/06/>
- Gonzales, A. (2006). Is the National Security Agency's Domestic Surveillance Program legal? Pro. *Periodical Congressional Digest*, 85(4), 106-114.

- Goss, K. (2010). Civil society and civic engagement: Towards a multi-level theory of policy feedbacks. *Journal of Civil Society*, 6(2), 119-143.
- Greenberg, A. (2013). National intelligence director apologizes for 'clearly erroneous' congressional testimony on NSA surveillance. *Forbes*. Retrieved from <https://www.forbes.com/.../national-intelligence-director-clapper-apologizes-for-clearl>
- Gross, G. (2006). Verizon-NSA case raises tough questions. *InfoWorld*, 28(21), 12-12.
- Harvard Law Review (2018). Cooperation or resistance?: The role of tech companies in government Ssurveillance. *Harvard Law Review*. Retrieved from <https://harvardlawreview.org/.../cooperation-or-resistance-the-role-of-tech-companies->
- Hatmaker, T. (2018). AT&T collaborates on NSA spying through a web of secretive buildings in the US. *Techcrunch*. Retrieved from <https://techcrunch.com/2018/06/25/nsa-att-intercept-surveillance/>
- Hesseldahl, A. (2014, April. 26). Verizon challenged the NSA's phone data collection program and lost. *Recode*. Retrieved from <https://www.recode.net/.../verizon-challenged-the-nsas-phone-data-collection-program>.
- Hudson, J. (2013). Google chief wrote about 'terrifying surveillance months before NSA leaks. *Foreign Policy*. Retrieved from <https://foreignpolicy.com/.../google-chief-wrote-about-terrifying-surveillance-months->
- Hustad, K. (2013). Apple files first- ever transparency report, calls out federal government. *Christian Science Monitor*, N.

- Janesick, V. (2011). *"Stretching" exercises for qualitative researchers* (3rd ed.). Thousand Oaks, CA: Sage Publications.
- Jones, M. (2018). AT&T helps NSA spy on Americans. *Komando*. Retrieved from <https://www.komando.com/happening-now/467544/att-helps-nsa-spy-on-americans>
- Katyal, N., & Caplan, C. (2008). The surprisingly stronger case for the legality of the NSA surveillance program: The FDR precedent. *Stanford Law Review*, 60(4), 1023-1077.
- Kerner, S. (2014). Feds threatened Yahoo with \$250-a-day fine over user data. *Periodical eWeek*, 1.
- Kirkus Reviews (2009). The secret sentry: Uncovering the untold history of the national security agency. *Kirkus Review*, 77(9), 66.
- Kravets, D. (2013). Verizon breaks silence on top-secret surveillance of its customers. *WIRED*. Retrieve from <https://www.wired.com/2013/06/verizon-responds/>
- Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. Published by IEEE Computer Society.
- Laureate International Universities. (no date). *Understanding social change*. Retrieved from [http:// UnderstandingSocialChange](http://UnderstandingSocialChange)
- Leahy, P. (2006). Is the national security agency's domestic surveillance program legal? *Periodical Congressional Digest*, 85(4), 107-111.
- Lenzner, R. (2013). ATT, Verizon, Sprint are paid cash by NSA for your private communications. *Forbes*. Retrieved from

<https://www.forbes.com/.../attverizonsprint-are-paid-cash-by-nsa-for-your-private-co>

Leswing, K. (2016). NSA Prism target had gmail and Facebook hacked. *Business Insider*. Retrieved from <https://www.businessinsider.com/nsa-prism-target-had-gmail-and-facebook-hacked-20>

Liamputtong, P., & Ezzy, D. (2005). *Qualitative research methods* (2nd ed.). Melbourne: Oxford University Press.

Lipp, K. (2016). AT&T Is spying on Americans for profit. *Daily Beast*. Retrieved from <https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit>

Lowe, S. (2013). Microsoft's alleged collaboration with NSA surveillance programs detailed. *IGN*. Retrieved from <https://www.ign.com/.../microsofts-alleged-collaboration-with-nsa-surveillance-progra>

Marquis-Boire, M., Greenwald, G., & Lee, M. (2015). NSA's Google for the world's private communications. *Intercepts*. Retrieved from <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/>

Masnick, M. (2013). NSA boss asks congress for blanket immunity for companies that helped NSA spy on everyone. *Techdirt*. Retrieved from <https://www.techdirt.com/.../nsa-boss-asks-congress-legal-immunity-companies-that-html>

Menn, J. (2016). Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence- sources. *Reuters*. Retrieved from <https://www.reuters.com/...yahoo-nsa.../exclusive-yahoo-secretly-scanned-customer-e>

- Miles, M., Huberman, M., & Saldana, J. (2014). *Qualitative data analysis. A methods sourcebook*. (Edition 3). Thousand Oaks, CA: SAGE Publications, Inc.
- Miller, C. C. (2013). Google employees speak out about government spying. *New York Times*. Retrieved from <https://bits.blogs.nytimes.com/.../google-employees-speak-out-about-government-spyi>.
- Miller, M. (2007). Standing in the wake of the terrorist surveillance program: A modified standard for challenges to secret government surveillance. Rutgers-Hein Online.
- Mother Jones (2013). Ask a FISA court judge! *Mother Jones*, 38(6), 13.
- Nakashima, E. (2014). U.S. reveal secret legal basis for NSA program to Sprint, declassified files show. *Washington Post*. Retrieve from <https://www.washingtonpost.com/...nsa...sprint.../f593612a-ce28-11e3-937f-d302623>
- Nakashima, E., & and Horwitz, S. (2013). Newly declassified documents on phone records program released. *Washington Post*. Retrieve from <https://www.washingtonpost.com/...verizon...senate-hearing/.../233fdd3a-f9cf-11e2-a>
- Newman, L. (2014). The U.S. government is suing Sprint in a lawsuit over \$21 million. *SLATE*. Retrieved from www.slate.com/.../_the_u_s_government_is_suing_sprint_in_a_lawsuit_over_21_mill...
- Nicks, D. (2014). Mark Zuckerberg calls Obama over NSA spying. *Time Magazine*. Retrieved from time.com › Politics › Domestic Surveillance
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

- Pearlman, M. (2010). The secret sentry: Uncovering the untold history of the national security agency. *Military Review*, 90(2), 123-123.
- Rash, W. (2013). Tech companies don't tell whole truth about data they give to feds. *Periodical eWeek*, 10.
- Robertson, A. (2015, April. 10). Sprint settles \$21 million wiretap fraud allegations for \$15.5 million. *Verge*. Retrieved from <https://www.theverge.com/2015/4/10/.../sprint-doj-wiretap-fraud-overcharge-settleme...>
- Rudestam, K. E., & Newton, R. R. (2015). *Surviving your dissertation: A comprehensive guide to content and process* (4th ed.). Thousand Oaks, CA: Sage.
- Sabatier, P. A., & Weible, C. M. (Eds.). (2014). *Theories of the policy process* (3rd ed.). Boulder, CO: Westview Press.
- Saldana, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). Los Angeles, CA: SAGE.
- Schindler, J. (2010). Uncovering no such agency. *Naval War College Review*, 63(4), 144-147.
- Severin, T. (2014). German government cancels Verizon contract in wake of US spying row. *Business News*. Retrieved from <https://www.reuters.com/...verizon/german-government-cancels-verizon-contract-in-w>
- Shanahan, E., Mcbeth, M., & Hathaway, P. (2011). *Narrative policy framework: The influence of media policy narratives on public opinion*. *Politics & Policy*, 39(3), 373-400. doi:10.1111/j.1747-1346.2011.00295. x

- Simon, M. K. (2011). Validity and reliability in qualitative studies. In *Dissertation and scholarly research: Recipes for success* (pp. 1–3). Seattle, WA: Dissertation Success. Retrieved from <http://dissertationrecipes.com/wp-content/uploads/2011/04/Validity-and-Reliability-in-a-Qualitative-Study.pdf>
- Sledge, M. (2014). CIA director grilled on domestic surveillance, torture at senate hearing. *Huffington Post*. Retrieve from https://www.huffingtonpost.com/2014/01/.../cia-domestic-surveillance_n_4688475.html
- Snapsurveys. (2014). Advantages and disadvantages of face-to-face data. Retrieved from: www.snapsurveys.com/.../advantages-disadvantages-facetoface-data-coll
- Solove, D. (2016). Microsoft just won a big victory against government surveillance—why it matters. *Linkedin*. Retrieve from <https://www.linkedin.com/.../microsoft-just-won-big-victory-against-government-why>
- Techrights. (2017). Microsoft and the NSA. *Techrights*. Retrieved from techrights.org/wiki/index.php/Microsoft_and_the_NSA
- Thibodeau, P. (2013). U.S. cloud vendors face backlash over prism. *Computerworld Periodical*, 47(14), 7.
- Toor, A. (2016, Oct. 20). Yahoo wants the US to explain its email surveillance order. *Verge*. Retrieved from <https://www.theverge.com/2016/10/.../yahoo-email-surveillance-letter-us-government>.
- United Business Media LLC. (2006). Online groups reveal details, legalities of NSA surveillance. *Information Week*.

- Van der Velden, L. (2015). Leaky apps and data shots: Technologies of leakage and insertion in NSA-Surveillance. *Surveillance & Society*, 13(2), 182-196.
- Whittaker, Z. (2018). T- Mobile quietly reveal uptick in government data demands. *Techcrunch*. Retrieved from <https://techcrunch.com/.../t-mobile-quietly-reveals-uptick-in-government-data-deman>
- Wolf, B. (2006, June 22). Senator grill AT&T CEO over NSA database. *ABC News*. Retrieved from <https://abcnews.go.com/Politics/story?id=2108595&page=1>
- Woolcott, L. (2014). Metadata in the archives. Retrieved from Digital commons.USU.edu
- Yin, R. (2014). *Case study research-design and methods*. (5th ed.). Thousand Oaks, CA: Sage Publications.
- 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.
- Zetter, K. (2013). Google cookies help NSA identify targets for hacking and Sspying. *WIRED*. Retrieved from <https://www.wired.com/2013/12/nsa-spy-cookies/>
- Zetter, K. (2013). DoJ secretly granted immunity to companies that participated in monitoring program. *WIRED*. Retrieved from <https://www.wired.com/2013/04/immunity-to-internet-providers/>

Appendix A: Letter of Introduction to the Identified Organization and Supporting Documents

Name of Company

Address

Dear (Name),

My name is [REDACTED], and I am a doctoral candidate at Walden University.

I am conducting a dissertation research on how and why the internet and telecommunications companies provide customer information to the government.

There have been numerous studies about the National Security Agency (NSA) surveillance programs with some scholars supporting the programs to keep America safe, and while others claim it is against individual liberty. Some researchers have also studied the capacity of the NSA surveillance program to show that they collected data from the private sectors, and some scholars have studied the negative consequences of the surveillance programs to the companies. However, no research has studied how and why these companies abided by the directive of the government to secretly collect data of their customers without adequate legislative and judicial oversight. Therefore, this research will provide insight into how the government gained compliance of the private sector which might help us to understand private/public sector collaboration in public policy.

I at this moment request your assistance to conduct this research by helping to identify and grant access to public documents about the NSA surveillance programs will be greatly appreciated. I am looking forward to receiving your calls on line [REDACTED] [REDACTED] or email at [REDACTED] to discuss any clarifications regarding the proposed research.

Sincerely,

[REDACTED]

Doctoral Candidate

Walden University

TOP SECRET//SI//NOFORN

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

TOP SECRET//SI//NOFORN

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

TOP SECRET//SI//NOFORN

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

TOP SECRET//SI//NOFORN

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION OF
TANGIBLE THINGS

Under Seal
Docket No. BR 14-01

OPINION AND ORDER

On January 22, 2014, [REDACTED]

[REDACTED] filed a
Petition pursuant to 50 U.S.C. § 1861(f)(2)(A) and Rule 33 of the Foreign Intelligence
Surveillance Court ("FISC" or "the Court") Rules of Procedure "to vacate, modify, or
reaffirm" a production order issued [REDACTED] January 3, 2014 ("Petition"). After
conducting the initial review required by Section 1861(f)(2)(A)(ii) and FISC Rule 39, the
Court determined that the Petition is not frivolous and issued a Scheduling Order
pursuant to FISC Rule 39(c) on January 23, 2014. Pursuant to the Scheduling Order, the
United States filed its Response to the Petition on February 12, 2014 ("Response"). The
Petition is now ripe for review. For the reasons set forth below, the Court concludes


~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

Pursuant to 50 U.S.C. § 1861(f)(2)(B), the Secondary Order is affirmed, [REDACTED] is directed to continue to comply with the Secondary Order until it expires by its own terms.

Since last summer, the Government has declassified and made public substantial details regarding the NSA telephony metadata program. Among other things, substantial portions of this Court's January 3 Primary Order and all predecessor orders have been publicly released. In light of those disclosures and the ongoing public debate regarding this program, both the Government [REDACTED] submit memoranda (or a joint memorandum) stating their views with respect to whether this Court can or should unseal the Petition, the Government's Response, and this Opinion and Order, and whether appropriately redacted versions of these documents should be published pursuant to FISC Rule 62(a). Such memoranda are to be submitted, under seal, no later than 5:00 p.m. Eastern Time on April 10, 2014.

SO ORDERED, this 20th day of March, 2014.


ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

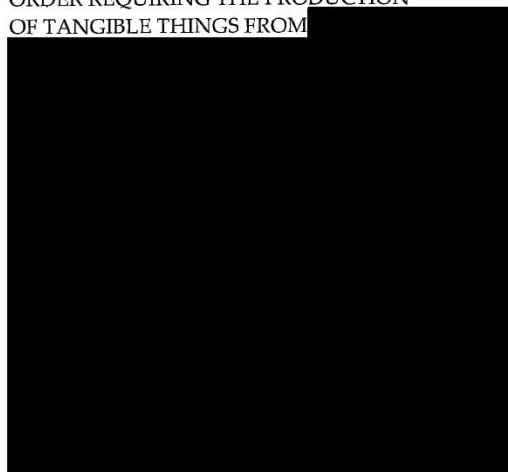
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

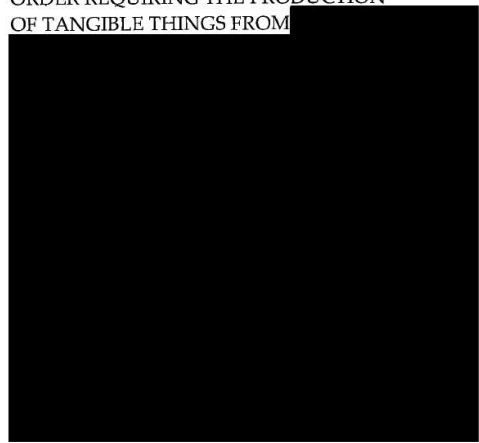
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

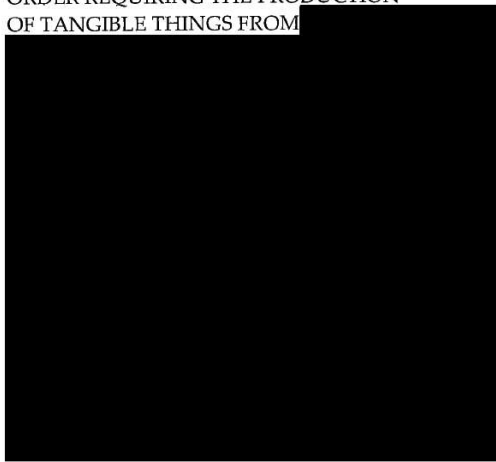
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

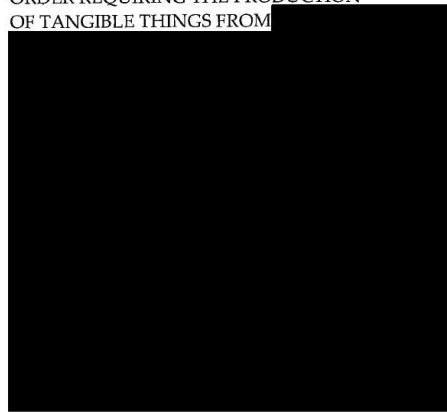
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11: 03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

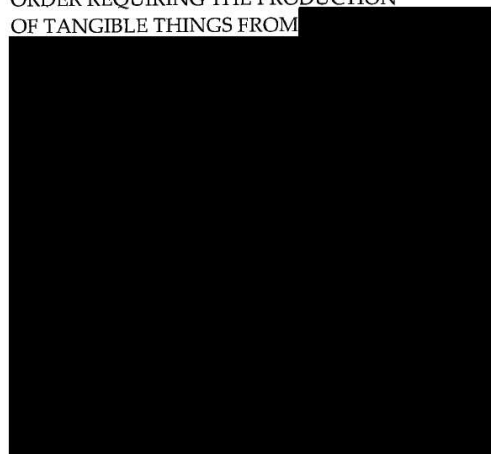
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

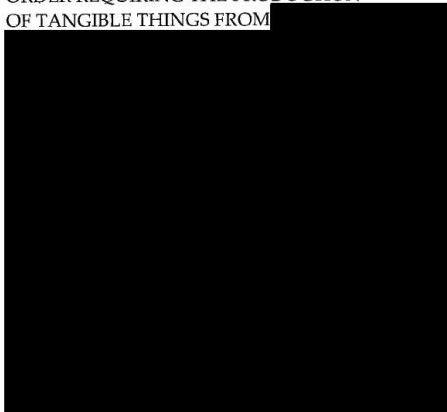
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ
Reason: 1.4(c)
~~Declassify on: 7 January 2035~~

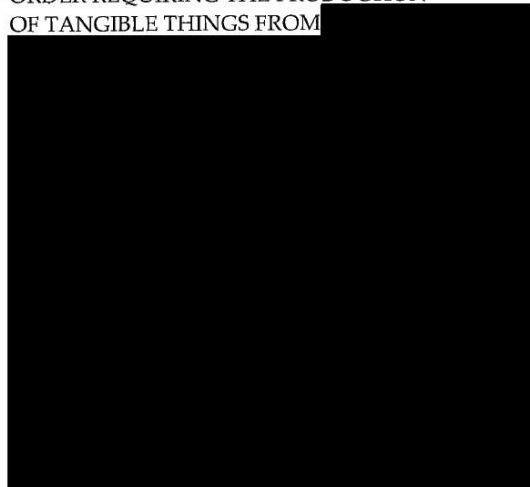
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,

NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

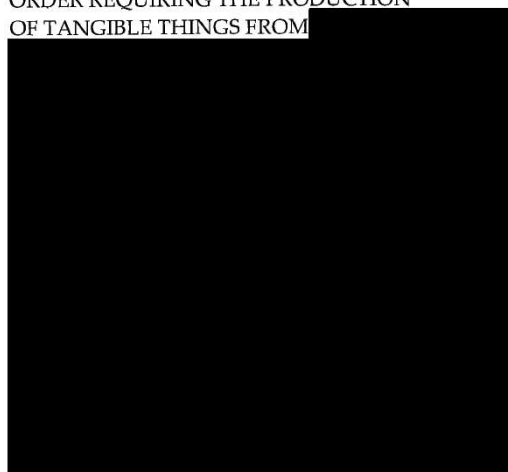
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

Approved for public release May 14, 2014.

~~TOP SECRET//COMINT//NOFORN~~

investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c) (1)]

b. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c) (2) (D)]

c. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 09-09 and its predecessors. [50 U.S.C. § 1861(c) (1)] ~~(TS//SI//NF)~~

3. The Government incorporates by reference the application, all documents filed in support of the application, and the orders issued in this docket. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN~~

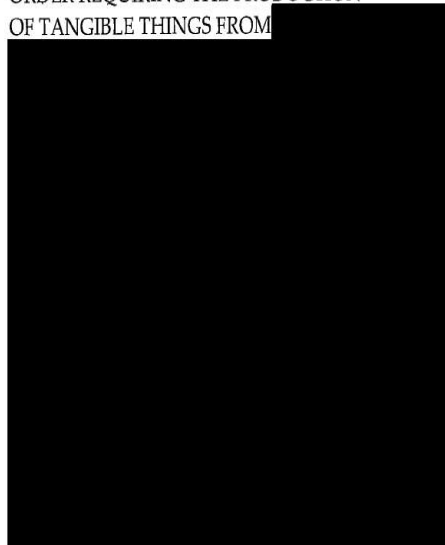
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

~~TOP SECRET//COMINT//NOFORN~~

2010 JAN -8 AM 11:03

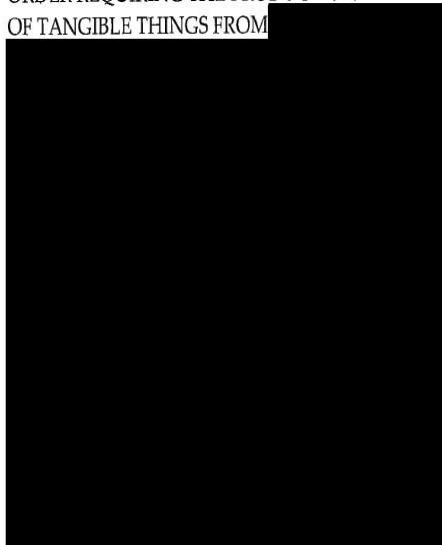
UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

CLERK OF COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

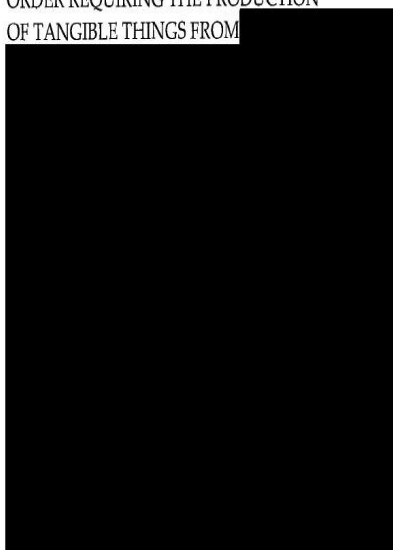
~~TOP SECRET//COMINT//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2010 JAN -8 AM 11:03

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM



Docket Number: BR 09-19

MOTION TO UNSEAL RECORDS (U)

The United States of America, by and through the undersigned Department of
Justice attorneys, hereby moves this Court, pursuant to the Foreign Intelligence

~~TOP SECRET//COMINT//NOFORN~~

Classified by: David S. Kris, Assistant Attorney General,
NSD, DOJ

Reason: 1.4(c)

~~Declassify on: 7 January 2035~~

1 MELINDA HAAG (CSBN 132612)
United States Attorney

2 ALEX G. TSE (CSBN 152348)
3 Chief, Civil Division

4 STEVEN J. SALTIEL (CSBN 202292)
Assistant United States Attorney

5 450 Golden Gate Avenue, Box 36055
6 San Francisco, California 94102-3495
7 Telephone: (415) 436-6996
8 FAX: (415) 436-6748
steven.saltiel@usdoj.gov

9 Attorneys for Plaintiff

10 UNITED STATES DISTRICT COURT
11 NORTHERN DISTRICT OF CALIFORNIA
12 SAN FRANCISCO DIVISION

13 UNITED STATES OF AMERICA,)	Case No.
14 Plaintiff,)	UNITED STATES' COMPLAINT
15 v.)	JURY TRIAL DEMANDED
16 SPRINT COMMUNICATIONS, INC.,)	
17 formerly known as SPRINT NEXTEL)	
18 CORPORATION; SPRINT PCS,)	
19 Defendants.)	

20
21 For its Complaint, Plaintiff, the United States of America, alleges as follows:

22 **I. NATURE OF ACTION**

23 1. The United States brings this action to recover treble damages and civil penalties under the
24 False Claims Act, 31 U.S.C. §§ 3729-33, and to recover damages and other monetary relief under the
25 common law theories of unjust enrichment and payment by mistake.

26 2. The United States bases its claims on Defendants' submission of false claims for
27 reimbursement of expenses they incurred in providing facilities or assistance to federal law enforcement
28

UNITED STATES' COMPLAINT

1 agencies in executing court orders authorizing the interception of a wire, oral, or electronic
2 communication (commonly referred to as a “wiretap”), and orders authorizing the installation of a pen
3 register or trap device. A pen register is a device that records or decodes dialing, routing, addressing or
4 signaling information transmitted by a particular telephone line, but not the contents of a
5 communication. 18 U.S.C. § 3127(3). A trap device is a device or process that captures the incoming
6 impulses which identify the source of a communication, but not its contents. 18 U.S.C. § 3127(4).

7
8 3. Within the time frames detailed below, Defendants Sprint Communications, Inc. and Sprint
9 PCS (collectively referred to as “Sprint”) knowingly submitted false claims to federal law enforcement
10 agencies, such as the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), U.S.
11 Marshals Service (USMS), Bureau of Alcohol, Tobacco and Firearms (ATF), Immigration and Customs
12 Enforcement (ICE), and others, by including unallowable costs in their charges for carrying out court
13 orders authorizing wiretaps, pen registers, and trap devices.

14
15 4. Like other providers of wire or electronic communications, Sprint is authorized by statute to
16 bill law enforcement agencies for the reasonable expenses it incurs in providing facilities or assistance to
17 accomplish a wiretap, pen register, or trap device (referred to herein as “intercept charges”). 18 U.S.C.
18 §§ 2518(4), 3124(c). In 1994, Congress passed the Communications Assistance in Law Enforcement
19 Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (“CALEA”), which required telecommunications
20 carriers to ensure that their equipment, facilities, or services were capable of enabling the government,
21 pursuant to a court order, to intercept and deliver communications and call-identifying information. 47
22 U.S.C. § 1002(a). On May 12, 2006, the Federal Communications Commission (FCC) resolved a
23 dispute between law enforcement agencies and telecommunications carriers, and ruled that carriers were
24 prohibited from using their intercept charges to recover the costs of modifying equipment, facilities or
25 services that were incurred to comply with CALEA. *In the Matter of Communications Assistance for*
26 *Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, Second
27
28

1 Report and Order and Memorandum Opinion and Order, 21 F.C.C.R. 5360, ¶¶ 69-74 (May 12, 2006)
2 (“*Second Report and Order*”). The FCC ruled that the carriers’ exclusive mechanism for recovering
3 these costs was from the United States Attorney General, under the limitations set forth in section 109 of
4 CALEA. Sprint participated in the FCC rulemaking proceeding.

5
6 5. Despite the FCC’s clear and unambiguous ruling, Sprint knowingly included in its intercept
7 charges the costs of financing modifications to equipment, facilities, and services installed to comply
8 with CALEA. Because Sprint’s invoices for intercept charges did not identify the particular expenses
9 for which it sought reimbursement, federal law enforcement agencies were unable to detect that Sprint
10 was requesting reimbursement of these unallowable costs.

11
12 6. By including the unallowable costs of financing CALEA modifications in their intercept
13 charges, Sprint inflated its charges by approximately 58%. As a result of Sprint’s false claims, the
14 United States paid over \$21 million in unallowable costs from January 1, 2007 to July 31, 2010.

15 II. JURISDICTION AND VENUE

16 7. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§
17 1331, 1345, 1367(a), and 31 U.S.C. § 3732. The Court may exercise personal jurisdiction over
18 Defendants pursuant to 31 U.S.C. § 3732(a) because Defendants transact business in this District.

19 8. Venue is proper in the Northern District of California under 31 U.S.C. § 3732(a) and 28
20 U.S.C. § 1391(b) and (c) because Defendants transact business in this District.

21 III. INTRADISTRICT ASSIGNMENT

22
23 9. This action did not arise in any one county of this District for the purposes of Civil L.R. 3-
24 2(c).

25 IV. PARTIES

26 10. The United States brings this action on behalf of all federal law enforcement agencies
27 (“LEAs”), including the FBI, DEA, USMS, ATF, ICE, United States Postal Inspection Service (USPIS),
28

1 Internal Revenue Service (IRS), the Defense Criminal Investigative Service (DCIS), and the United
2 States Secret Service.

3 11. Defendant Sprint Communications, Inc., formerly known as Sprint Nextel Corporation, is a
4 Kansas corporation with its principal place of business in Overland Park, Kansas. Sprint
5 Communications, Inc. is a wholly owned subsidiary of Sprint Corporation. At all times relevant to the
6 complaint, Sprint Communications, Inc. was a communications company offering wireless and wireline
7 communications products and services in all fifty states, Puerto Rico, and the U.S. Virgin Islands.

8 12. Defendant Sprint PCS is a joint venture established in 1994 by Sprint Communications, Inc.,
9 TCI, Comcast Corporation, and Cox Communications, Inc. In 1998, Sprint Communications, Inc.
10 assumed 100% ownership and management control of Sprint PCS. At all times relevant to the
11 complaint, Sprint PCS submitted invoices for intercept charges to LEAs.
12

13 V. THE FALSE CLAIMS ACT

14 13. The False Claims Act, 31 U.S.C. §§ 3729-33, provides, in pertinent part, that:

15 [A]ny person who—

16 (A) knowingly presents, or causes to be presented, a false or fraudulent claim for
17 payment or approval;

18 is liable to the United States Government for a civil penalty of not less than \$5,000 and
19 not more than \$10,000, as adjusted by the Federal Civil Penalties Inflation Adjustment
20 Act of 1990 (28U.S.C. § 2461 note; Public Law 104-410), plus 3 times the amount of
21 damages which the Government sustains because of the act of that person.

22 31 U.S.C. § 3729(a)(1).

23 14. Pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended by the
24 Debt Collection Improvement Act of 1996, 28 U.S.C. § 2461 (notes), and 64 Fed. Reg. 47099, 47103
25 (1999), the False Claims Act civil penalties were adjusted to \$5,500 to \$11,000 per false claim for
26 violations occurring on or after September 29, 1999.

27 15. The False Claims Act defines “knowing” and “knowingly” as follows:
28

1 [T]he terms “knowing” and “knowingly”—

2 (A) mean that a person, with respect to information—

- 3 (i) has actual knowledge of the information;
- 4 (ii) acts in deliberate ignorance of the truth or falsity of the information; or
- 5 (iii) acts in reckless disregard of the truth or falsity of the information; and

6 (B) require no proof of specific intent to defraud.

7
8 31 U.S.C. § 3729(b)(1).

9 **VI. STATUTORY AND REGULATORY FRAMEWORK FOR INTERCEPT CHARGES**

10 **A. Cost Recovery Pursuant to Intercept Statutes**

11 16. Telecommunications carriers are authorized by statute to recover their “reasonable
12 expenses” in complying with a valid wiretap order. 18 U.S.C. § 2518(4) provides, in pertinent part:

13
14 An order authorizing the interception of a wire, oral, or electronic communication under
15 this chapter shall, upon request of the applicant, direct that a provider of wire or
16 electronic communication service . . . shall furnish the applicant forthwith all
17 information, facilities, and technical assistance necessary to accomplish the interception
18 unobtrusively and with a minimum of interference with the services that such service
19 provider . . . is according the person whose communications are to be intercepted. Any
20 provider of wire or electronic communication service . . . furnishing . . . such facilities or
21 technical assistance shall be compensated therefor by the applicant for reasonable
22 expenses incurred in providing such facilities or assistance.

23 17. Similarly, with respect to pen registers and trap devices, 18 U.S.C. § 3124(c) provides, in
24 pertinent part, that a “provider of a wire or electronic service . . . who furnished facilities or technical
25 assistance pursuant to this section shall be reasonably compensated for such reasonable expenses
26 incurred in providing such facilities and assistance.”

27 **B. Communications Assistance for Law Enforcement Act**

28 18. In 1994, Congress passed CALEA. Congress described CALEA as an Act “to make clear a
telecommunications carrier’s duty to cooperate in the interception of communications for law
enforcement purposes.” The legislative purpose of CALEA was to “preserve the government’s ability,

1 pursuant to court order or other lawful authorization, to intercept communications involving advanced
2 technologies such as digital or wireless transmission modes, or features and services such as call
3 forwarding, speed dialing and conference calling, while protecting the privacy of communications and
4 without impeding the introduction of new technologies, features, and services.” H.R. Rep. No. 103-
5 827(I), 1994 U.S.C.C.A.N. 3489.
6

7 19. Section 103 of CALEA provides, in pertinent part, that:

8 [A] telecommunications carrier shall ensure that its equipment, facilities, or services that
9 provide a customer or subscriber with the ability to originate, terminate, or direct
10 communications are capable of—

11 (1) expeditiously isolating and enabling the government, pursuant to a court order or
12 other lawful authorization, to intercept, to the exclusion of any other communications, all
13 wire and electronic communications carried by the carrier within a service area to or from
14 equipment, facilities, or services of a subscriber of such carrier concurrently with their
15 transmission to or from the subscriber’s equipment, facility, or service, or at such later
16 time as may be acceptable to the government;

17 (2) expeditiously isolating and enabling the government, pursuant to a court order or
18 other lawful authorization, to access call-identifying information that is reasonably
19 available to the carrier—

20 (A) before, during, or immediately after the transmission of a wire or electronic
21 communication (or at such later time as may be acceptable to the government);
22 and

23 (B) in a manner that allows it to be associated with the communication to which
24 it pertains, except that, with regard to information acquired solely pursuant to the
25 authority for pen registers and trap and trace devices (as defined in section 3127
26 of title 18, United States Code), such call-identifying information shall not
27 include any information that may disclose the physical location of the subscriber
28 (except to the extent that the location may be determined from the telephone
number);

(3) delivering intercepted communications and call-identifying information to the
government, pursuant to a court order or other lawful authorization, in a format such that
they may be transmitted by means of equipment, facilities, or services procured by the
government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying
information unobtrusively and with a minimum of interference with any subscriber’s
telecommunications service and in a manner that protects—

1 (A) the privacy and security of communications and call-identifying information
2 not authorized to be intercepted; and

3 (B) information regarding the government's interception of communications and
4 access to call-identifying information.

5 47 U.S.C. § 1002(a).

6 20. Section 109 of CALEA authorized the U.S. Attorney General, subject to the availability of

7 funds, to "pay telecommunications carriers for all reasonable costs directly associated with the

8 modifications performed by carriers in connection with equipment, facilities, and services installed or

9 deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section

10 103." 47 U.S.C. § 1008(a). The Attorney General was authorized to pay the reasonable costs of

11 equipment, facilities, or services deployed after January 1, 1995 only upon a determination by the FCC

12 that compliance with Section 103 of CALEA was not "reasonably achievable." 47 U.S.C. § 1008(b).

13 Pursuant to section 109(e) of CALEA (codified at 47 U.S.C. § 1008(e)), the Attorney General

14 promulgated regulations to effectuate the submission of claims by, and payment to, telecommunications

15 carriers for the reasonable costs of compliance with section 103. These regulations are codified at 28

17 C.F.R. § 100.9 *et seq.* Claims submitted under these regulations were separate and distinct from

18 carriers' intercept charges, i.e., their claims for the reasonable expenses of providing facilities or

19 assistance in complying with a valid intercept order.

20 21. Congress appropriated a total of \$500,000,000 for fiscal years 1995, 1996, 1997, and 1998,

21 to carry out Title I of CALEA. 47 U.S.C. § 1009.

22
23 **C. FCC Second Report and Order**

24 22. In March 2004, the U.S. Department of Justice, the FBI, and the DEA filed a petition for

25 expedited rulemaking with the FCC, requesting that the FCC initiate a proceeding to resolve various

26 outstanding issues relating to the implementation of CALEA. The FCC responded in August 2004 by

27 issuing a Notice of Proposed Rulemaking. *Second Report and Order*, ¶ 4. Many telecommunications

28

1 carriers, including Sprint, participated in this proceeding by submitting comments.

2 23. In September 2005, the FCC issued its *First Report and Order* in the rulemaking
3 proceeding. See *Communications Assistance for Law Enforcement Act and Broadband Access and*
4 *Services, First Report and Order and Further Notice of Proposed Rulemaking*, ET Docket No. 04-295,
5 RM-10865, 20 FCC Rcd 14989 (2005). The *First Report and Order* stated: “In the coming months, we
6 will release another order that will address separate questions regarding the assistance capabilities
7 required of the providers covered by today’s Order pursuant to section 103 of CALEA. This subsequent
8 order will include other important issues under CALEA, such as compliance extensions and exemptions,
9 cost recovery, identification of future services and entities subject to CALEA, and enforcement.” *Id.*,
10 ¶ 3 (emphasis added).

11
12 24. On May 12, 2006, the FCC issued its *Second Report and Order* in the rulemaking
13 proceeding. In its Notice of Proposed Rulemaking, the FCC sought comment on a number of issues
14 related to the recovery of CALEA compliance costs, including the nature of such costs and from which
15 parties the costs could be recovered. The FCC also inquired into CALEA cost recovery pursuant to
16 intercept statutes (e.g., 18 U.S.C. §§ 2518(4), 3124(c)). *Second Report and Order*, ¶ 69.

17
18 25. In its Notice of Proposed Rulemaking, the FCC acknowledged its prior statement in an order
19 suggesting that carriers could recover a portion of their CALEA capital costs through intercept charges
20 imposed on LEAs, and that this statement was made without the benefit of a complete and full record on
21 the issue. In the *Second Report and Order*, the FCC repudiated its prior statement:

22
23 “... because we now conclude that CALEA section 109 provides the *exclusive* mechanism by
24 which carriers may recover from law enforcement capital costs associated with meeting the
25 capability requirements of CALEA section 103, the Commission’s prior statement was incorrect
to the extent it suggested that carriers may recover CALEA capital costs through intercept
charges.”

26 *Second Report and Order*, ¶ 71 (emphasis in original).

27 26. The FCC reasoned that, because CALEA makes the government responsible for compliance
28

1 costs for the period on or before January 1, 1995, and places the responsibility for compliance costs after
 2 January 1, 1995 on carriers (absent a finding by the FCC that compliance is not reasonably achievable),
 3 allowing carriers to recover CALEA compliance costs from the government through intercept charges
 4 would be inconsistent with the cost recovery methodology set forth in § 109. The FCC stated that:

5
 6 Allowing carriers to recover CALEA compliance costs from the government through other
 7 means, such as through intercept charges, would be inconsistent with the cost recovery
 8 methodology set forth in CALEA section 109 because it would disrupt the cost burden balance
 9 between law enforcement and carriers carefully crafted by Congress in enacting CALEA. In
 10 short, as DOJ notes, it “would essentially allow carriers to do an ‘end-run’ around the provisions
 11 of section 109(b) and Congressional intent.”

12 *Second Report and Order*, ¶ 71.

13 27. With respect to the carriers’ ability to recover CALEA compliance costs through intercept
 14 charges, the FCC ruled as follows:

15 We therefore conclude that, while carriers possess the authority to recover through intercept
 16 charges the *costs associated with carrying out an intercept* that is accomplished using a CALEA-
 17 based intercept solution, they are prohibited by CALEA from recovering through intercept
 18 charges the *costs of making modifications to equipment, facilities, or services* pursuant to the
 19 assistance capability requirements of CALEA section 103 and the *costs of developing, installing,*
 20 *and deploying CALEA-based intercept solutions* that comply with the assistance capability
 21 requirements of CALEA section 103.

22 *Second Report and Order*, ¶ 71 (emphasis added).

23 28. The FCC found that, “to the extent carriers do not meet the necessary criteria for obtaining
 24 cost recovery pursuant to section 109(b) of CALEA, carriers may absorb the costs of CALEA
 25 compliance as a necessary cost of doing business, or, where appropriate, recover some portion of their
 26 CALEA section 103 implementation costs from their subscribers.” *Second Report and Order*, ¶ 72. The
 27 FCC declined to adopt a national surcharge to recover CALEA costs. *Second Report and Order*, ¶ 73.

28 VII. FACTUAL ALLEGATIONS

29 29. Pursuant to 18 U.S.C. § 2518(4) and 18 U.S.C. § 3124(c), Sprint, at all times relevant to the
 30 complaint, sought reimbursement of the expenses it incurred in complying with orders authorizing
 31 wiretaps, pen registers, and trap devices (collectively referred to as “intercepts”) by charging LEAs the

1 rates contained on Sprint's Electronic Surveillance Fee Schedule. Sprint's fees included an
2 implementation fee charged per intercept and per geographic area (referred to as a "market"), and a daily
3 maintenance fee.

4 30. Sprint determined its fees by calculating its average cost per intercept, using a cost model
5 that purported to divide the company's expenses in executing intercept orders (the numerator or costs)
6 by the average number of intercepts projected over a period of time (the denominator or demand).
7

8 31. Prior to May 12, 2006, when the FCC issued its *Second Report and Order*, Sprint included
9 in its intercept charges to LEAs the costs of its capital investment in equipment, facilities, and services
10 to comply with section 103 of CALEA.

11 32. In July 2006, after the FCC issued the *Second Report and Order*, Sprint revised its cost
12 model by removing the capitalized costs (i.e., depreciation) of the equipment and upgrades in which it
13 invested in order to comply with section 103 of CALEA.
14

15 33. Although Sprint removed depreciation on its investment in CALEA equipment and upgrades
16 from the cost model, Sprint continued to include in its charges to LEAs the costs of financing that
17 investment, including: (1) the "cost of debt," the annual interest expense on loans the proceeds of which
18 were used to invest in CALEA equipment; (2) the "cost of equity," the dividend payments or growth in
19 stock value to shareholders from an additional stock offering or drawing on existing equity of the
20 company used to invest in CALEA equipment; and (3) taxes associated with both the "cost of debt" and
21 "cost of equity."
22

23 34. By including these expenses in its cost model, Sprint violated the FCC's prohibition against
24 using intercept charges to recover from LEAs the costs of making modifications to equipment, facilities,
25 and services in order to comply with section 103 of CALEA, and/or the costs of developing, installing,
26 and deploying CALEA-based intercept solutions in order to comply with section 103 of CALEA.

27 35. Based on the July 2006 cost model, Sprint published a revised Electronic Surveillance Fee
28

1 Schedule with revised fees. Sprint billed LEAs these fees for carrying out intercepts.

2 36. Sprint did not publish or otherwise disclose to LEAs the July 2006 cost model on which the
3 revised fees were based. Sprint did not disclose to LEAs that the costs of financing its investment in
4 CALEA equipment were included in its intercept charges.

5 37. In or about June 2010, Sprint again revised the cost model on which its intercept charges are
6 based. In the June 2010 cost model, Sprint removed the costs of financing its investment in CALEA
7 equipment, including the cost of debt, cost of equity, and associated taxes. Effective August 1, 2010,
8 Sprint lowered its intercept charges based on the June 2010 cost model. As of this date, Sprint has failed
9 or refused to refund the overpayments made by LEAs based on its pre-August 1, 2010 fees, as described
10 below.
11

12 VIII. FALSE CLAIMS

13 38. During the period January 1, 2007 to July 31, 2010, pursuant to 18 U.S.C. § 2518(4) and 18
14 U.S.C. § 3124(c), Sprint submitted over 29,000 claims to LEAs for reimbursement of its reasonable
15 expenses in carrying out intercepts, charging fees based on the July 2006 cost model. These claims were
16 false because, as described above, the fees charged to the LEAs included hidden costs that the FCC
17 ruled were unallowable.
18

19 39. Sprint submitted these claims in the form of invoices to LEAs from its Subpoena
20 Compliance Department.
21

22 40. By way of example, from January 1, 2007 to July 31, 2010, Sprint submitted invoices for
23 intercept charges to the following LEAs, for which the LEAs paid the following amounts:

24	FBI	\$10,582,237
25	DEA	\$20,973,813
26	USMS	\$ 3,237,435
27	ATF	\$ 461,781
28		

1 ICE \$ 2,396,342

2 Secret Service \$ 31,141

3 41. As described above, the payments made by LEAs to Sprint for intercept charges included the
4 costs of financing Sprint's investment in CALEA equipment, including the cost of debt, cost of equity,
5 and associated taxes, in violation of the *Second Report and Order*. By including these unallowable costs
6 in its intercept charges, Sprint inflated its charges by approximately 58%. As a result of Defendants'
7 false claims, the United States paid over \$21 million in unallowable costs from January 1, 2007 to July
8 31, 2010.

10 **IX. TOLLING OF STATUTE OF LIMITATIONS**

11 42. Sprint executed a series of tolling agreements with the United States tolling the running of
12 time under any applicable statute of limitations, by way of laches or other time limitation (whether
13 statutory, contractual or otherwise) for the period of time between February 1, 2012 and the date of
14 filing suit or March 3, 2014, whichever is earlier.

16 **FIRST CAUSE OF ACTION**

17 (False Claims Act: Presentation of False Claims)

18 (31 U.S.C. § 3729(a)(1)(A))

19 43. The United States repeats and realleges the preceding paragraphs as if fully set forth herein.

20 44. Sprint knowingly presented, or caused to be presented, false or fraudulent claims for
21 payment or approval to the United States for reimbursement of its expenses in furnishing facilities and
22 assistance in carrying out intercepts.

24 45. By virtue of the false or fraudulent claims presented or caused to be presented by Sprint, the
25 United States suffered damages and therefore is entitled to treble damages under the False Claims Act,
26 to be determined at trial, plus civil penalties of not less than \$5,500 and up to \$11,000 for each violation.

SECOND CAUSE OF ACTION

(Unjust Enrichment)

46. The United States repeats and realleges the preceding paragraphs as if fully set forth herein.

47. As a consequence of the acts described above, Sprint was unjustly enriched at the expense of the United States in an amount to be determined which, under the circumstances, in equity and good conscience, should be returned to the United States.

48. The United States claims the recovery of all monies by which Sprint has been unjustly enriched.

THIRD CAUSE OF ACTION

(Payment by Mistake)

49. The United States repeats and realleges the preceding paragraphs as if fully set forth herein.

50. Sprint was not entitled to receive payment from LEAs for the annually recurring expenses of financing Sprint's investment in CALEA equipment, including the cost of debt, cost of equity, and associated taxes.

51. The United States, through the LEAs, paid Sprint for the costs of financing Sprint's investment in CALEA equipment, including the cost of debt, cost of equity, and associated taxes, without knowledge of material facts, and under the mistaken belief that the United States was paying for Sprint's allowable costs in furnishing facilities and assistance in carrying out intercepts. The United States' mistaken belief was material to its decision to pay Sprint for such claims. Accordingly, Sprint is liable to account and pay to the United States the amounts of the payments made in error.

PRAYER FOR RELIEF

WHEREFORE, the United States demands and prays that judgment be entered in its favor against Sprint as follows:

1. On the First Cause of Action under the False Claims Act, for the amount of the United States'

1 damages, trebled as required by law, and such civil penalties as are required by law, together with such
2 further relief as may be just and proper.

3 2. On the Second Cause of Action for unjust enrichment, for the amounts by which Sprint were
4 unjustly enriched, plus interest, costs, and expenses, and for such further relief as may be just and
5 proper.

6 3. On the Third Cause of Action for payment by mistake, for an amount equivalent to the loss
7 sustained by the United States, plus interest, costs, and expenses, and for such further relief as may be
8 just and proper.
9

10 **DEMAND FOR JURY TRIAL**

11 Pursuant to Rule 38 of the Federal Rules of Civil Procedure, the United States demands a jury
12 trial in this case.

13 DATED: March 3, 2014

Respectfully submitted,

MELINDA HAAG
United States Attorney

16 /s/ Steven J. Salties
17 STEVEN J. SALTIEL
Assistant United States Attorney

YAHOO!

October 19, 2016

The Honorable James R. Clapper
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Clapper,

I write to you regarding recent media reports stemming from an October 4 Reuters article about an alleged classified order from the U.S. government. At Yahoo, we are deeply committed to transparency and to protecting the rights of our users. Yahoo was mentioned specifically in these reports and we find ourselves unable to respond in detail. Your office, however, is well positioned to clarify this matter of public interest. Accordingly, we urge your office to consider the following actions to provide clarity on the matter: (i) confirm whether an order, as described in these media reports, was issued; (ii) declassify in whole or in part such order, if it exists; and (iii) make a sufficiently detailed public and contextual comment to clarify the alleged facts and circumstances.

We appreciate the need for confidentiality in certain aspects of investigations involving public safety or national security; however, transparency is critical to ensure accountability and in this context must include disclosing how and under what set of circumstances the U.S. government uses specific legal authorities, including the Foreign Intelligence Surveillance Act, to obtain private information about individuals' online activities or communications. Citizens in a democracy require such information to understand and debate the appropriateness of such authorities and how the government employs them.

As you know, Yahoo consistently campaigns for government transparency about national security requests and for the right to share the number and nature of the requests we receive from all governments. We apply a principled approach to handling government requests for user data, including in the national security context, articulated in our publicly-available Global Principles for Responding to Government Requests and regular transparency reports. Our company not only embraces its privacy and human rights responsibilities, we do so enthusiastically, passionately, and with a deep sense of global and moral responsibility. But transparency is not merely a Yahoo issue: Transparency underpins the ability of any company in the information and communications technology sector to earn and preserve the trust of its customers. Erosion of that trust online implicates the safety and security of people around the world and diminishes confidence and trust in U.S. businesses at home and beyond our borders.

Recent news stories have provoked broad speculation about Yahoo's approach and about the activities and representations of the U.S. government, including those made by the Government in connection with negotiating Privacy Shield with the European Union. That speculation results in part from lack of transparency and because U.S. laws significantly constrain—and severely punish—companies' ability to

701 First Avenue Sunnyvale CA 94089
P: 408 349 3300 F: 408 349 3301