

Unauthorized Disclosures and Press Publication of Classified

Intelligence Information: a Case Study

Dissertation

Submitted to Northcentral University

Graduate Faculty of the School of Business and Technology Management
in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

by

PATRICK F. BARTON

Prescott Valley, Arizona
April 2016

Copyright 2016

PATRICK F. BARTON

ProQuest Number: 10109620

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 10109620

Published by ProQuest LLC (2016). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

APPROVAL PAGE


Unauthorized Disclosures and Press Publication of Classified

Intelligence Information: a Case Study

by

Patrick F. Barton

Approved by:


Chair: Dr. Cynthia Akagi _____ Date 5/9/16

Subject Matter Expert: Dr. Martin Crossland

Methodologist: Dr. C. Jerome Fore


Dean: School of Business & Technology Management _____ Date 5/9/16
Dr. Peter Bemski, Ph.D.

Abstract

The press regularly publishes classified intelligence information leaked to them by those with authorized access and varied motives. This information, to an adversary, is held to a standard equivalent to information gathered through standard espionage tradecraft. Traditionally, leaks had disclosed elements of a single programs but, given advances in technology, today leaks to the press entail the unauthorized disclosure of, at times, millions of classified documents on a myriad of topics. In 2013, Mr. Edward Snowden gave at least 1.7 million highly classified U.S. and intelligence documents to the press. The problem to be addressed in this study are the impacts to U.S. intelligence from the unauthorized bulk disclosure of classified intelligence information from Edward Snowden to the press including, but not limited to, revealing intelligence sources and methods, capabilities, loss of intelligence liaisons and accesses to territories essential for U.S. national security. The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may include, but may not be limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. The sample was the leaked, published, classified U.S. intelligence documents. Quantitative research, specifically a single-case, holistic study, was conducted using an examination of the leaked and published classified intelligence information and expert assessments of the national security impact. The study revealed significant impacts to U.S. and allied intelligence agencies and national security as a whole. Mosaic-making, on the part of the press, validated long-standing axioms and provided additional insight into the underdeveloped Mosaic Theory.

Acknowledgements

I am incredibly privileged to be able to conduct this research and am indebted to numerous individuals both outside and within the Northcentral University system. Mr. Randy Elliott was the standard by which I judged academic achievement and excellence. I have tried to emulate his example. Mr. Dan Law was an unending source of academic discourse on a variety of topics. My conversations with him, sometimes lasting hours, encouraged critical thought and reminded me that a topic can be examined through numerous lenses. Drs. Pat Ford and Suzanne Hebert became my most valuable advocates and friends that I have placed on a high pedestal. Every conversation with them suggested new approaches to problems, provided endless encouragement, and fueled the flame that burned brightly throughout this project. They were the pillars that held the academic roof over my head. My daughter and son, Joanna and Kevin, were beside me through this journey and were an unconditional source of love and support.

My life, as it exists today, is a direct result of my service in the intelligence community. This dissertation is in no small part dedicated to the thousands in that community who serve in silence, for the greater good, with little fanfare or accolades.

Last but certainly not least I owe a tremendous debt of gratitude to my dissertation chair, Dr. Cynthia Akagi. Dr. Akagi was a source of unlimited patience and encouragement, always available for counsel, without which I would have been lost in the proverbial wilderness of mirrors. Thank you, one and all!

Table of Contents

Chapter 1: Introduction	1
Background	3
Statement of the Problem	4
Purpose of the Study	5
Theoretical Framework	6
Research Questions	8
Nature of the Study	9
Significance of the Study	11
Definition of Key Terms	12
Summary	16
Chapter 2: Literature Review	17
Documentation	17
Rational for Intelligence Secrecy--Theoretical Perspectives	18
Mosaic Theory	28
The Lunev Axiom	29
United States Intelligence Case Law	31
Intelligence Precedents	34
Intelligence Perspectives	37
Press Perspectives	38
United States Government Perspectives	47
The Secrecy Debate	54
Emerging Trends	56
Summary	57
Chapter 3: Research Method	60
Research Method and Design	61
Population	62
Sample	62
Materials/Instruments	62
Data Collection, Processing, Analysis	63
Assumptions	64
Limitations	65
Delimitations	66
Ethical Assurances	66
Summary	67
Chapter 4: Findings	69
Results	69
Evaluation of Findings	86
Summary	99
Chapter 5: Implications, Recommendations, and Conclusions	100

Implications.....	103
Recommendations.....	114
Conclusions.....	120
References.....	127
Appendixes	144
Appendix A: Study Findings References.....	145

List of Tables

Table 1 <i>Number of News Articles as Analyzed Per Newspaper Source</i>	71
Table 2 <i>U.S. Intelligence Documents, Lowest to Highest Intelligence Classification</i>	72
Table 3 <i>Originating Agency, Number of Leaked Documents and Intelligence Classification</i>	72
Table 4 <i>Themes from Findings, SQ1: Impacts on U.S. Intelligence Sources and Methods</i>	74
Table 5 <i>Themes from Findings, SQ2: Impacts on U.S. Intelligence Capabilities</i>	80
Table 6 <i>Themes from Findings, SQ3: Impacts on U.S. Liaisons and Accesses</i>	83
Table 7 <i>Theme from Findings, SQ4: Other Impacts</i>	85

List of Figures

Figure 1. This figure illustrates the data triangulation analysis process of aligning each leak to published articles to the impact on U.S. intelligence which produced the themes for each sub-question. 70

Chapter 1: Introduction

The press regularly publishes classified intelligence information leaked to them by those with authorized access and varied motives (Bruce, 2003; Ross, 2011; Schoenfeld, 2011). Naturally this information, to an adversary, is held to a standard equivalent to information gathered through standard espionage tradecraft (Bruce, 2003; Lunev & Winkler, 1998). The stream of leaked classified intelligence information has not stopped, nor has their publication by a press eager to broadcast the nation's secrets (Ross, 2011; Schoenfeld, 2011). Where traditionally leaks had involved high-level individuals disclosing elements of a single program or a program itself today, given advances in technology (Danielson, 2011; Papandrea, 2011; Heemsbergen, 2013; McCraw & Gikow; 2013), leaks to the press entail the unauthorized disclosure of, at times, millions of classified documents on a myriad of topics by low-level individuals within government.

Edward Snowden personifies this increasing phenomenon of classified intelligence leaks. In 2013, Mr. Snowden gave highly classified U.S. intelligence information to the press, specifically Britain's Guardian newspaper and the Washington Post (Heemsbergen, 2013; Lears, 2013). Given the concept of Mosaic theory, a picture can be created from seemingly disparate pieces of information (Pozen 2005, 2010, 2013). As a function of Mosaic theory (Pozen, 2005, 2013) these leaks, when published, form a picture of U.S. intelligence operations that, at a minimum, compromise the ability and effectiveness of the U.S. to conduct intelligence operations, a critical component of government policymaking and national security statecraft (Doorey, 2007; Ross, 2011; Sales, 2012). Although prosecutions of the press for this activity have, historically, been

threatened, not a single prosecution has been attempted (Ross, 2011; Schoenfeld, 2011; Kitrosser, 2013).

The information compromised by unauthorized disclosures of classified material is deemed classified by an original classification authority based upon the level of potential damage to national security that may be incurred should that information be compromised (Kitrosser, 2013; Defense Intelligence Agency, 2013). Subordinate to the original classification authority are all others that apply classifications to material. These individuals or groups utilize a classification guide developed by the original classification authority and are known as derivative classifiers (Kitrosser, 2013).

Information related to the impacts of press publication of leaked classified intelligence information has not revealed the impacts to U.S. national security (Inkster, 2014; Johnson, 2014). Thus, attempts at damage assessments or any approximation thereof, had been typically characterized as exercises in indeterminacy, with the U.S. government estimating that damage costs ran into the hundreds of millions of dollars (Schoenfeld, 2011; Senate, 1997; Kessler, 2008). Debate vis-à-vis classified intelligence leaks and their publication has been polarized on political or constitutional grounds with few considering the damages caused by publication of the information (Doorey, 2007; Fenster, 2012; Mascolo & Scott, 2013). This disregard was further compounded when organizations rewarded the leaking of classified documents, as evidenced by the Swedish Parliament's 2014 Right Livelihood Award, considered the alternative Nobel Prize, to Mr. Snowden (Right Livelihood, 2014).

Background

In 2013 the U.S. National Security Agency (NSA) contractor Edward Snowden, seemingly motivated by the need to inform the public, gave some 1.7 million classified intelligence documents to reporters from Britain's Guardian and the U.S.'s Washington Post newspapers (Caplan, 2013; Meyer, 2014; Papandrea, 2014). The leaks and its subsequent and continuing publication have exposed a considerable number of intelligence collection operations, sources, and methods to the public (Lowe, 2014). Historically, little has been done by governments to stem the tide of the leaked documents publication phenomenon (Meyer, 2014), and the Snowden case was no different. Contributing to the lack of action by the U.S. government was a lack of understanding of the status of the leaker, existing press freedoms, and the fear that prosecuting the leaker would result in the revelation of additional classified information (Caplan, 2013; Papandrea, 2014).

Arguments exist on numerous fronts and were aligned with the self-interests of the authors that opined on the topic. Few had insight as to the impact that press publication of leaked classified intelligence operations had on the ability of a nation to defend its citizens and inform its government in order to perform national security and statecraft functions (Inkster, 2014; Johnson, 2014). Where much work had addressed the topic of leaks of a single document or program by high level individuals and subsequent publication by the press, little had been researched on the paradigm shift of bulk leaks of classified information and their subsequent publication (Inkster, 2014).

Statement of the Problem

The problem addressed in this study was what are the impacts to U.S. intelligence from the unauthorized bulk disclosure of classified intelligence information from Edward Snowden to the press including, but not limited to, revealing intelligence sources and methods, capabilities, loss of intelligence liaisons and accesses to territories essential for U.S. national security (Ross, 2011; Schoenfeld, 2011; Johnson, 2014). An estimated 1.7 million documents were given by Edward Snowden to the Guardian newspaper and other media entities (Heemsbergen, 2013; Lears, 2013; Johnson, 2014). Though most damage assessments were concerned with leaks of single documents or issues (Richelson, 2012), this event represented a paradigm shift, unexplored, and when addressed in this study would contribute to Mosaic Theory (Pozen, 2005; Pozen, 2013).

The Constitutionally-protected press had historically ignored but a relative handful of requests from the U.S. government to abstain from publishing national security secrets (Silver, 2008; Schoenfeld, 2011; Sedler, 2011; McCraw & Gikow, 2013). Presidents and Congress had not mitigated unauthorized disclosures that, due to informational and technological advances, increased in volume and scope (Danielson, 2011; Papandrea, 2011; Heemsbergen, 2013; McCraw & Gikow; 2013). The United States people, the press, and Congress due to a lack of reporting or mis-reporting about unauthorized intelligence disclosures, seemed unaware of this problem that hampered the U.S. Intelligence Community's ability to conduct its mandated intelligence collection function to preserve national security (Papandrea, 2012). Failure to document and analyze this phenomenon will continue to leave the United States people, the press, and

Congress uninformed about how the publishing of classified intelligence impacts U.S. national security (Freivogel, 2009; Sales, 2010, 2012; Pozen, 2013).

Purpose of the Study

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. The population was the unauthorized documents disclosed to the media. The sample was the published documents that significantly compromised national security. The leaked intelligence documents, the subsequent media frenzy reporting the leaks, and the damage incurred formed the basis for exploring the phenomenon of the impacts of unauthorized leaks and publication of classified U.S. intelligence documents, as it related to Mosaic Theory in the modern era (Pozen 2005, 2010, 2013). Primary data -- the leaked and published classified documents, including intelligence reports, intelligence sources, method documents, briefings, and inter-office government emails was collected from online databases including, but not limited to, EBSCOhost, ProQuest, and LexisNexis. Secondary data in the form of media and expert assessments was collected through these same databases as well as queries of archival databases, archived physical records, and other declassified records within the holdings of the U.S. National Archives and Records Administration (NARA), if available. The data were compiled and coded. The leaked documents were examined to document the impacts to U.S. intelligence activities and U.S. national security as a whole. Findings from the study would contribute to Mosaic Theory which theorizes the ability of

disparate pieces of information to form an understanding of a far greater picture, unseen when looking at the separate pieces (Pozen, 2005; Pozen, 2013; Sales, 2012; Weaver & Pallitto, 2005). Findings from this study documented and analyzed the impacts of leaking classified intelligence information as it affected U.S. national security, extending what we knew about this emerging phenomena and Mosaic Theory.

Theoretical Framework

Mosaic Theory has been posited by Pozen (2005, 2010, and 2013) as a valid argument for safeguarding information. His development of Mosaic Theory informed and guided this research. Application of Mosaic Theory argued achieved synergies as disparate pieces of information yield a total picture greater than the sum of their parts (Pozen, 2005). Although Mosaic Theory had been cited as an example for U.S. intelligence gathering and analysis (Pozen, 2005), an adversary could use the same techniques given leaked classified intelligence information. Strategic national security vulnerabilities, not seen when examining the information as pieces, may reveal themselves upon assembly. Initially, Pozen (2005) argued for classification and protection of the nation's classified information. As information relating to leaks of classified information developed others, including Pozen (2010, 2013), presented compelling arguments grounded in theory to counter, advocating leak benefits and citing instances of over classification of documents and an excessive secrecy environment within government.

Notwithstanding the perceptions of those on the side of press freedoms or government secrecy, de facto perceptions of the U.S. Intelligence Community were unheard due to a missing portion - the U.S. national security impact. Knowing this

information would contribute to Mosaic Theory by bringing an analysis of Mr. Snowden's 2013 leak of classified intelligence information to light using a theory heretofore underexplored within the scholarly community in both depth and breadth (Pozen, 2005, 2013).

Bruce (2003) theorized on the press' ability to function as the intelligence arm of the nation's adversaries when publishing leaked classified intelligence information. Contemporary modifications or views related to Bruce's (2003) concepts took on many forms but, unfortunately, much of the theory related to the phenomenon is relegated to issues regarding First Amendment freedoms including rights to publish and right of access, secrecy laws and information control, as well as personal accountability (Lee, 2008; Papandrea, 2011; Pozen, 2005; Pozen, 2010; Silver, 2008). These tangential theories ignored important aspects of the phenomenon, for example the impact on the national security of the U.S. (Pozen, 2013). Even Pozen himself failed in his examination of the growing problem, limiting himself to only single instances of leaks and publication and not the trend of leaks by individuals, disclosing hundreds of thousands of documents for publication by the press (Pozen, 2013).

The U.S. Congress, although sieve-like in their ability to generate leaks, rarely leaked classified intelligence information relating to sources and methods. Instead, the primary leaks involved the final analytic reports produced by the country's various intelligence agencies (Divoll, 2011; Posner & Vermeule, 2007). When deconstructed these reports may have, when analyzed and deduced, revealed sources or methods and validated Pozen's (2005, 2010, 2013) application of Mosaic Theory.

Research findings from the study contributed to Pozen's (2005, 2010, 2013) Mosaic Theory by examining the impact through an analysis of Mr. Snowden's 2013 unauthorized disclosure of classified intelligence information. Research results intended to inform practical application related to the phenomenon that had, thus far, been limited to political rhetoric (Pozen, 2005) and not based on the long-term security of the nation. The case studied, relating to Mr. Snowden's leaks and their subsequent publication, documented how basic research techniques with Mosaic Theory as the overarching framework could reveal and affect intelligence operations.

Research Questions

The press regularly published classified intelligence information leaked to them by those with authorized access and varied motives (Bruce, 2003; Ross, 2011; Schoenfeld, 2011). Naturally this information, to an adversary, was held to a standard equivalent to information gathered through standard espionage tradecraft (Bruce, 2003; Lunev & Winkler, 1998). Edward Snowden, in 2013, gave highly classified U.S. intelligence information to the press, specifically Britain's Guardian newspaper and the Washington Post (Heemsbergen, 2013; Lears, 2013). The following question and sub questions guided this study.

Q1. What are the impacts on U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press?

SQ1. What are the impacts on U.S. intelligence sources and methods?

SQ2. What are the impacts on U.S. intelligence if capabilities were revealed that were previously unknown to adversaries?

SQ3. What are the impacts on U.S. intelligence if liaisons and access to territories in which to conduct intelligence activities were revealed?

SQ4. What emerged as other impacts on U.S. national security from Snowden's unauthorized disclosure of classified intelligence information to the press?

Nature of the Study

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not be limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. A single-case, holistic case study was appropriate as a research design to answer the research question and sub-questions. Reasons included the lack of a concrete understanding of the phenomenon, the lack of scholarly examination of the phenomenon vis-à-vis its impact, and the contemporary nature of the topic (Yin, 2014). Likewise, the case study was appropriate because one was describing the impact of events and considering that this event affected many different parties (Kohn, 1997).

The constructs to be analyzed were the impacts to U.S. national security, due to unauthorized leaks and media publication of U.S. classified intelligence information (Heemsbergen, 2013; Lears, 2013). The phenomenon being investigated was Edward Snowden's bulk, unauthorized classified intelligence documents leaked to the Guardian and Washington Post newspapers. Data collection was bound by time and activity (Baxter & Jack, 2008). The time constraint was bound by the beginning of Mr. Snowden's unauthorized disclosures. Since disclosure and publication relating to the event were ongoing, the ending time constraint for the case study coincided with

Northcentral University's IRB approval of the research. Similarly, activity boundaries were set (Baxter & Jack, 2008). Although Mr. Snowden released millions of documents relating to a myriad of national security issues, only those related to the unauthorized disclosure of classified intelligence information that were subsequently published were addressed.

After receiving NCU IRB approval, primary data, the original leaked classified documents and the media reporting thereof, including intelligence reports, intelligence sources and method documents as well as briefings and inter-office government emails were collected from online databases. These databases included, but were not limited to, EBSCOhost, ProQuest, and LexisNexis. These data included records and quotes to document the national security ramifications of publishing classified intelligence information leaked to the media (Patton, 2002).

Secondary data in the form of intelligence experts' assessments were collected through the same databases as the primary data as well as queries of archival databases, archived physical records, and other declassified records within the holdings of the U.S. National Archives and Records Administration (NARA), if available (Yin, 2012, 2014). The data were compiled and coded. The leaked documents were examined using government assessments as to damages affecting U.S. intelligence activities and U.S. national security as a whole. Similarly, court records and first person accounts of the impacts to U.S. intelligence were collected.

As a general analytical strategy, the research relied on theoretical propositions (Mosaic Theory, Pozen, 2014; Yin, 2014) with the overarching proposition that unauthorized disclosure and publication of classified U.S. intelligence information

affected national security. Analysis of the data identified and described various elements of the phenomenon in relationship to the national security of the nation. The published articles were matched (pattern-matching) to U.S. Intelligence documentation and analyzed using expert assessments of damage to U.S. intelligence sources and methods, capabilities, loss of intelligence liaisons and accesses to territories essential for U.S. national security (Yin, 2014). This identified intelligence sources and methods that otherwise were unavailable to the public and the nation's adversaries, before the leaks. These findings provided a framework for further analysis, methodological triangulation of the primary data (Bryman, 2002), and filled data shortfalls, increasing validity of the research and further documenting the phenomenon.

Significance of the Study

The study was significant because the phenomenon in question, press leaks and publication of classified intelligence information, had been examined using single leaks from relatively highly placed government officials and their publication, versus bulk leaks from low-level individuals. The contributions to the field of study came through a thorough understanding of the impact to U.S. national security from the Edward Snowden event. Answering the research questions sought to provide context and weight to an event that seemingly had the ability to cripple intelligence collection efforts. Understanding of this event existed under the lens of the press that had a monetary interest in keeping leak streams open (Risen, 2009). Governments seemed slow to react to leaks and their publication that, in the best case, informed the public of government wrongdoing or mismanagement and, in the worst case, informed a country's adversaries of the nature, sources, and methods of its intelligence collection operations (Ross, 2011; Schaffert,

1992). This investigation of the impact to intelligence collection operations could influence subsequent events of this nature by either preventing future leaks or, more desirably, limiting press publication of a nation's intelligence tradecraft. Study findings would also add to the literature on Mosaic Theory.

Definition of Key Terms

Adversary gain. Adversary gain is the strategic, tactical, or propaganda advantage gained as a result of press publication of classified intelligence information (Author definition).

Communications intelligence (COMINT). COMINT is one of three portions of the signals intelligence umbrella consisting of encrypted or “plaintext” – unencrypted – information exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purpose of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, or analysis of the substantive meaning of the communication (ODNI, 2011).

Cryptology. Cryptology is the science and art of making and breaking codes and ciphers (NSA, 2016).

Degradation. Degradation is defined as it pertains to intelligence vis-à-vis the phenomena, the reduction in effectiveness of sources and methods due to adversary adaptation to revealed intelligence collection capabilities by the press (Author definition).

Derivative Classifiers. Derivative classifiers apply classifications to material utilizing a classification guide developed by an original classification authority (Kitrosser, 2013).

Electronic intelligence (ELINT). ELINT is a portion of the SIGINT umbrella, ELINT is information derived primarily from electronic signals that do not contain speech or text or information obtained for intelligence purposes from the interception of electromagnetic non-communications transmissions by other than the intended recipient. Most common of this type are radar signals (ODNI, 2011).

Foreign instrumentation signals intelligence (FISINT). FISINT is a portion of the SIGINT umbrella, FISINT is the interception of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems and can include telemetry, beaconry, electronic interrogators, and video data links, or the intelligence information derived from these means (ODNI, 2011).

Human intelligence (HUMINT). HUMINT is intelligence collected by human sources rather than primarily technical means. It includes both secret and unclassified collection activities, using overt or clandestine means (Odom, 2003, p. xxxv; Richelson, 1999).

Imagery intelligence (IMINT). IMINT is intelligence that includes representations of objects reproduced by numerous electronic or optical means, including film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro optics (ODNI, 2011).

Intelligence community. This community is a collection of agencies or entities, under the U.S. Office of the Director of National Intelligence, that conduct intelligence activities necessary for the conduct of foreign relations and the protection of US national security. They include Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard, Defense Intelligence Agency, Department of Defense, Department

of Energy, Department of Justice, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and Navy Intelligence (ODNI, 2011).

Intelligence. Intelligence is information relating to sources, methods, or identities of individuals involved in the intelligence process, as well as the results of effectiveness of intelligence operations. In the research, intelligence is both a noun and a verb (Author definition).

Leaked. Leaked is classified intelligence information divulged to unauthorized recipients by individuals with authorized access to the material but lacking authority to release that same material to unauthorized or un-cleared individuals (Author definition).

Lunev Axiom. The Lunev Axiom is defined as classified intelligence information disclosed in the press [being] the equivalent of intelligence gathered through traditional foreign espionage (Bruce, 2003).

Open source intelligence (OSINT). OSINT is information derived from public sources, in print or electronic form, including but not limited to radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings used to enhance intelligence analysis and reporting. While unclassified, knowledge of its collection or intended use may approach level of classification revealing targeting or strategic/tactical intent (ODNI, 2011).

Nonstate actor. A non-state actor is an organized political actor not directly connected to the state but pursuing aims that affect vital state interests (Pearlman & Cunningham, 2012, p. 3).

Press. Press, for the purposes of this research, is considered media in the form of traditional newspapers, news magazines, or electronic in the form of traditional radio and television and their associated post-information revolution electronic equivalents administered and manned by individuals with journalism education, background, and credentials. It also includes new media such as weblogs, internet-based news services, or any form of social media. (Author definition).

Signals intelligence (SIGINT). SIGINT is the act of, or intelligence derived from, signals intercepts comprising, individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and/or FISINT (ODNI, 2011).

Sources and methods. A term used to describe the practice of intelligence collection and analysis. Intelligence sources and the nature of information obtained vary. Intelligence sources include information obtained from espionage, images obtained by satellites, intercepted communications, and publicly available media reporting. The term “methods” is synonymous with tradecraft, techniques used by intelligence officers and analysts to carry out their duties. Sources and methods are heavily guarded because they explain how intelligence information is collected and analyzed and can give opponents opportunity to assess the capabilities and interests of their enemy. Intelligence agencies classify and protect their sources and methods because they are significant in the success of ongoing and future operations and analysis (Wirtz, 2010).

Summary

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that included, but may not be limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. Data gathered included, but may not have been limited to, the actual classified documents as well as media reports of the leaked classified intelligence information, including intelligence reports, intelligence source and method documents and briefings as well as inter-office government emails, obtained through unauthorized disclosure and published by the Guardian newspaper and the Washington Post. Analysis of the primary raw data, as compromised by Mr. Snowden and the secondary data reported by the media was triangulated to build a mosaic of the total impact to the national security of the United States. Findings contributed to Mosaic Theory and furthered literature on the phenomenon in question.

Chapter 2: Literature Review

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. This review of the literature related to the impact of press publication of classified intelligence information examined theoretical perspectives directly related, as well as tangential to, the problem so as to illuminate all sides of this issue. Information from peer-reviewed research studies as well as texts authored by individuals with first-person knowledge of the phenomenon, intelligence, the press, and U.S. government perspectives was also discussed.

Documentation

The review of the literature was based on scholarly, peer-reviewed sources contained in online libraries within the Northcentral University system. Databases within the library included EBSCOHost, Proquest, and Praeger Security. Database search terms included, but were not limited to, national security, whistleblower, press leak, secrecy, Snowden, Manning, WikiLeaks, classified information, and compromise. Additionally, sources within the researcher's archives, digital and hard-copy, were consulted. These included hard-copy journals from Taylor and Francis. Online archival databases from the U.S. Central Intelligence Agency and the Social Science Research Network supplement the Northcentral University library resources.

Rational for Intelligence Secrecy--Theoretical Perspectives

National security interests prudently dictated that one's national security secrets, specifically classified intelligence information revealing intelligence sources and methods, be kept from one's adversaries (Ross, 2011). With secrecy being the key to the surveillance of adversaries and intelligence planning (Schoenfeld, 2013) and thus critical to the nation's security, Green (2005) invoked three theories to explain why the United States Intelligence Community did not share information. Organizational in nature, the theories included Bureaucratic Inefficiency Theory, the Theory of the Information Itself vis-à-vis its classified nature and the power that information brought by virtue of possession and, finally, the Theory of Collective Inaction (Green, 2005).

The Theory of Bureaucratic Inefficiency contended, in part, that although the U.S. Intelligence Community may be a true community, its organization more resembled a bureaucracy. As a result, bureaucratic tendencies – inefficiencies – existed (Green, 2005). The Theory of the Information itself contended that the intelligence information must be classified in order to protect intelligence sources and methods. Because the collecting agency essentially owned the information, this theory compounds the bureaucratic inefficiency theory. More importantly, the Theory of Information and its classification related to the ability to deny opponents and adversaries access to classified intelligence information (Green, 2005). Both of these theories were consistent with Kitrosser's (2007b) Theory of Bureaucracy, noting "Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret" (Weber, 1946, as cited in Kitrosser, 2007b, p. 889). Finally, Green (2005) advances the Theory of Collective Inaction which asserted that groups of individuals,

contrary to the assumption that they will act on behalf of common interests, act to maximize personal welfare before group objectives. These three theories supported why the U.S. Intelligence Community does not share information and may compound the importance that the press places on this information when it is received (Pozen, 2013). More importantly, the latter of the three theories may have explained one reason for leaking classified intelligence information to the press.

Three additional theories, Utilitarian, Liberal Democratic, and Constitutional, supported the press publication of leaked classified information and advocated the press's freedom to publish (Pozen, 2010). Utilitarian Theory, in part, advocated state secrecy to prevent adversary access to information that would harm the national interest. Although acknowledged that secrecy enhanced government deliberation and protection of privacy, it may have also consolidated power, bred suspicion, and resulted in poor policymaking (Pozen, 2010).

Pozen's (2010) Liberal Democratic Theory maintained the notion of transparency, openness, choice, and consent as the bedrock of a democratic society. Secrets, kept from the public, were deemed counter to the public's ability to monitor their government and elected officials, and were further assessed as a breeding ground for immoral actions, limitations on rights and liberties, and denial of information to citizens. Constitutional Theory however, according to Pozen (2010), failed to address adequately the topic of secrecy and thus it was assumed, arguably, that the public had a paramount right to access and, generally, the right to know about the government's affairs. But this right to know was the subject of considerable debate at all levels, most specifically, judicial. This theory seemed to comingle with Nilsson and Sjölin's (2005) assessment that social

responsibility affirmed the liberty of the media, but holds that the media had certain obligations towards society.

Radó (2011) maintained that leaks of classified information fell under the International Relations Theory problem of delineation of private and public spheres. In this sense, Radó (2011) assumed that the growing open nature of the world due to advances in digital technology would result in additional releases of classified information, blurring the line between transparency and secrecy. Some theorized that the press was as culpable as the leaker. Lee's (2008) Journalistic Liability Theory introduced the concept of liability for the journalist knowing that they were receiving classified information illegally. This theory seemed critical in prosecuting journalists under both the Espionage Act and the Intelligence Identities Protection Act of 1982. Ross (2011) built upon Lee's (2008) theory, proposing Rational Choice Theory as an alternative approach to legislation possibly limiting press freedoms. Focusing on the individual's decision-making processes, this theory allowed the rational assessment of the perceived costs versus benefits prior to a given behavior, i.e., the cost-benefit assessment that the press must undertake before publishing classified intelligence information.

Bruce (2003) theorized that publication of leaked classified intelligence information harmed the U.S. Intelligence Community and, resultantly, U.S. national security. Richelson (2012) assessed that problems exist in the assessment that damage from traditional espionage equated to damage from leaks and their publication. His opinion was that espionage detailed considerably more information than was published in the press. Yet when considering Mosaic Theory, perhaps Richelson's (2012) argument didn't stand the test when one considered that Mosaic Theory, when applied to

intelligence gathering, drew inferences from fitting together disparate pieces of information (Goodwin, 2010). Mosaic making was further enhanced by technological advances and, in practice, applicable to cases involving the Freedom of Information Act, National Security Letters, and state secrets (Goodwin, 2010).

Similarly, Bruce (2003) advanced the notions that government does not over classify information and that classified information published by the press was eagerly read by foreign intelligence services and terrorist organizations alike. The thought that government did not over classify its national security information was countered by Kitrosser (2013). She characterized the practice of classifying information as over-classification, questioning whether classification affected First Amendment protections for the same material that was otherwise unclassified, arguing that the classification system was near politicized. Kitrosser (2013) noted that a former government official stated that the classification system was characterized by the notion that the system was more concerned with preventing embarrassment than with national security.

Bruce (2003) commented that any evidence supporting claims that leaks were causing damage to national security were available only in the classified domain. Although Bruce was an insider with access qualified to assess damages, his views were discounted and even belittled by authors and scholars alike with profit motives related to the phenomenon continuing. Richelson (2012) for example characterized Bruce and Schoenfeld, leading authors advocating the prosecution of leakers and those who publish their stories, as desperados. Richelson (2012) called Bruce's credibility into question due to Bruce's stance that government didn't classify too much information. Schoenfeld is called into question because of his desire to punish, in some cases, those who publish

leaked classified information (Richelson, 2012). Richelson's (2012) criticism of these authors and refuting their claims seemed to be in order to elicit a response and thus gain information for upcoming publication versus serious scholarship. Therein lied the conflict of interest. Consistent in the argument was the press insistence that the government classified too much information and that classification levels were over-inflated. (Risen, 2009) and that a portion of that information was an effort to hide potentially incriminating information (Sagar, 2009). Many as a result had become advocates of declassification and, as the media, were usually profit oriented (Ross, 2011). Sagar (2009) cautioned that declassification could not take place without examining potential harm from publication, precisely the step omitted when one leaked classified information.

Bruce's (2003) thoughts, although older than five years, were reintroduced by Papandrea (2011) as an important consideration given advances in technological capabilities of not only the media, but perceived adversaries as well. Scholarship was lacking when considering communications advances and its impact on the phenomenon and included, but were not limited to, the rise of non-traditional media sources and data storage and transmission increases (Papandrea, 2014). A particular by-product of these advances was a difficulty of discerning leaker from whistleblower and more importantly discerning traditional espionage activities. These ideas were important and needed to be reconsidered because they added to an understanding of – and provide a new window to view – a phenomenon that, seemingly, was increasing in both volume and scope. Theory in the field relating to the impact of leaks and their publication, though, was remarkably sparse (Kitrosser, 2007b), as was the delta between theory and reality (Vladeck, 2007). This delta was exemplified by the U.S. Government historically having done little to stem

the tide of classified information leaks as well as their subsequent publication due to perceived First Amendment constraints as well as reluctance by the U.S. Government to disclose additional classified information, identifying the extent of harm (Alson, 2008; Ross, 2011).

Papandrea's (2011) resurrection of the Bruce (2003) contribution injected predictions relating to the increase of the phenomena vis-à-vis advances in technology but was countered by Hillebrand (2012), who noted that "...critics within government often ignore the fact that media outlets do not normally reveal such sensitive stories immediately, but carefully weigh their potential damage to national security and discuss the material with officials off-the-record" (p.695). Scholarly discourse on the subject of leaks of classified intelligence information and their subsequent publication ran the gamut from Constitutional concerns to Executive privileges and were generally aligned with the interests or biases of their authors (Ross, 2011; Sutter, 2001). Notwithstanding, the perceptions of those on the side of press freedoms or government secrecy and the perceptions of those in the Intelligence Community should be heard so as to address a missing portion of the theoretical model, the U.S. national security impact. Knowing this information could modify theory and thus, in practice, inform relevant policymaking related to the phenomenon.

Although theory related to leaking and publishing classified information was relatively well developed, theory related to unauthorized disclosure and publication of classified intelligence information was sparse (Kitrosser, 2007b) and even more so when considering the impact of the phenomenon. Current theories advocating the prohibition of publishing classified intelligence information considered the protection of intelligence

sources and methods as paramount to openness concerns or First Amendment freedoms. Given previous legislation – the Espionage Act of 1917, the Communications Intelligence (COMINT) statute, and the Intelligence Identities Protection Act – Alson (2008) proposed new legislation to prohibit publication of intelligence information. Alson’s (2008) belief was that current legislation was inadequate given the advances in technology and adversary informational capabilities. Lee (2008) supplemented Alson’s (2008) thought, introducing issues relating to the initial act, the leak, alleging that individuals with authorized access violated non-disclosure agreements. The press, knowing that the classified intelligence information was disclosed illegally, bore a portion of the liability, violating the Espionage Act (Lee, 2008).

Mixed messages, disguised as theory, came far from reaching a level of “grand” theory worthy of phenomena with such a level of importance and generally indicated a lack of understanding of the phenomena itself (Wacker, 1998). Practice, or policy in the case of the phenomena, could not be fully or effectively implemented without a full understanding of all aspects of the phenomena. Perceptions existed from most stakeholders related to the phenomenon and not surprisingly most of these perceptions existed on the two ends of a very broad continuum. Sides argued that the press had a right of access as well as a right to publish, no matter the information (Papandrea, 2011; Pozen, 2010) and some saw leaks as tolerated by the American public (Lee, 2008). The other end of the spectrum saw the press as behaving akin to the intelligence and propaganda arms of the nation’s adversaries (Ross, 2011) and should self-censor (Sedler, 2011) or be prosecuted for publication of classified information (Vladeck, 2007). The press role, though, was assessed as important in the field despite a less than persistent,

piecemeal effort at government oversight (Hillebrand, 2012). Significant information existed on the tangential topics that comprised the larger topic but, unfortunately, little information existed on the impact to the U.S. Intelligence Community and overall U.S. national security.

Theory and practice were operating separately relating to the proposed topic. cursory research of peer-reviewed, scholarly sources revealed a remarkable lack of application of prevailing theory, specifically those originated by Bruce (2003) and Pozen (2005, 2010, 2013) to the problem of publication of leaked classified intelligence information, a void between theory and practice (Vogel, 2010). Policy, dating back to the 1970s, dictated that intelligence functioned better under external oversight mechanisms, with the leaking of secrets part and parcel to an unofficial checks and balances system where openness trumped secrecy (Lacquer, 1998). The seeming lack of understanding of the theory, a by-product of the lack of understanding of the phenomenon, had resulted in a lack of deterrence in both leaking classified intelligence information as well as its publication (Pozen, 2013). Fundamentally, this lack of leak deterrence had been a detractor to an effective intelligence apparatus (Lacquer, 1998). Although Lacquer (1998) advocated oversight of the intelligence community both internally and externally, he implied by omission that the press was not part of that oversight function.

When considering the topic of leaks, typically one was are only considering unauthorized leaks of information, a small portion embedded within the continuum of leaks and publication. Applications of theory to practice were offered in two fields relating to the phenomenon, protection of information and protection of people (Schoenfeld, 2013; Papandrea, 2014). Both attempts at applying theory to practice failed

in that the phenomenon – publication of leaked classified intelligence information – had not abated (Bruce, 2003; Papandrea, 2011; Ross, 2011).

A separate and distinct phenomenon existed when individuals received permission from a competent authority to leak information to the press under the guise of national security politics and process (Schoenfeld, 2013). For government, this practice was another way to communicate with the masses as well as test public opinion (Kitrosser, 2013; Pozen, 2013, Schoenfeld, 2013). Although at times important, this phenomenon – that of the authorized leak and its legitimacy as a tool of statecraft (Schoenfeld, 2013) – was beyond the scope of this research, but was mentioned at points throughout this review so as to isolate the phenomenon and case under investigation.

The U.S. Congress, for example, although sieve-like in their ability to generate leaks, rarely leaked classified intelligence information relating to sources and methods (Posner & Vermeule, 2007). Instead, the primary leaks involved the final analytic reports produced by the country's various intelligence agencies (Divoll, 2011; Posner & Vermeule, 2007). Divoll (2011) assessed that when an adversary deconstructed these reports, after analysis, they may reveal and subsequently compromise and possibly terminate sources or methods, validating Pozen's (2005, 2013) application of Mosaic Theory. Divoll (2011) contended that:

Putting aside the horror of lost human life and the cost of lost technology, the damage to our national security caused by leaks of sensitive information can be, and has been, far broader than it may appear to the naked eye (p. 523).

Divoll's (2011) assessment was critical; emphasizing that research has not been accomplished on the impact to the nation related to the phenomenon.

At the U.S. Central Intelligence Agency (CIA), its Inspector General (IG) is charged with the investigation of wrongdoings, providing a forum for grievances, and required to provide records of its investigations to the U.S. Department of Justice (Check & Radsan, 2010). A portion of this activity involved the protection of whistleblowers that reported wrongdoings in good faith (Check & Radsan, 2010; Lacquer, 1998). Operating on the theory, discussed previously, that the publication of leaked classified intelligence information harmed the U.S. Intelligence Community and further harmed U.S. national security, one would think that whistleblowers would be coddled by the IG. Such may not be the case. Sagar (2009) implied that the whistleblower was acting in an unlawful manner, undermining the executive branch's role as keeper of the nation's secrets and that the whistleblower would leak secrets anonymously rather than risk prosecution. Practical application failed theory again as it forces classified intelligence information out of its classified domain (Sagar, 2009). Finally, no mention was made relating to follow-up with the whistleblower that, when concerns are not satisfactorily addressed, turned into a potential leaker. Given that leakers, typically, took issue with the activities of colleagues and are unable or unwilling to proceed with internal remedies, this was an important issue (Pozen, 2010).

Whistleblowers, in the case of the CIA, were functioning in a dual role many times as leakers (Check & Radsan, 2010). Many IG investigations were initiated as a result of outside reporting. Of the five IG investigations examined by Check and Radsan (2010), none were first discovered by the IG. Whistleblowers were dual reporting to the IG and the media, apparently on the presumption that the media garnered better and faster results as well as serving as greater punishment for the violation in question (Check &

Radsan, 2010).

That the CIA had failed in retaining information deemed classified in the national interest was seemingly testament to a failure of the theory-practice relationship (Kessler, 2008). Whether an accurate understanding of the theory was present is unknown but, given the persistent nature of the phenomenon, application of theory to practice did not approach levels required to conclude with reasonable certainty that leaks of classified intelligence information related to the national security interest would not be published. Success or failure in the cyclical relationship between theory and practice was seemingly field-dependent and, many times, a function of the communications relationship between scholars and practitioners (Udo-Akang, 2012).

Mosaic Theory

Mosaic Theory had traditionally been applied to Fourth Amendment law (Kerr, 2012) but was also cited by government when referencing national security, specifically: “What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene” (Slobogin, 2012, p. 4). Mosaic making is synergistic, the whole being greater than the sum of the disparate parts (Pozen, 2005). Pozen (2005) developed Mosaic Theory through the filter of the Freedom of Information Act, believing the topic lacked any theoretical development. Slobogin (2012) agreed, believing that Mosaic Theory was little more than a name.

Pozen (2005) also concluded that Mosaic Theory, as a defense, invited government abuse and overreach vis-à-vis information control. A landmark case using Mosaic Theory was Central Intelligence Agency vs. Sims (McQueen, 2007). The Supreme Court ruled in favor of the Central Intelligence Agency, stating its Director need

not disclose intelligence researcher names or their affiliation (McQueen, 2007). Government had also used Mosaic Theory claims to deny access to innocuous information (Setty, 2012). Schulhofer (2013) further criticized Mosaic Theory as a defense because: “Mosaic theory shuts down any possibility of review, deferential or otherwise, because it attributes reality to risks that only an intelligence expert – or not even an intelligence expert – can detect” (para. 2.2.3)

The Mosaic argument posited that enemy intelligence experts can piece together small details, insignificant in themselves, in order to construct a revealing picture of sensitive U.S. secrets (Schulhofer, 2013). The Mosaic Argument has gathered inertia in a post 9/11, information-centric world (Pozen, 2005), and this argument has been validated in the Federal Court system (Papandrea, 2005). But importantly, the executive branch believes that the courts cannot recognize when an innocuous piece of information can fit into a damaging national security mosaic (Kitrosser, 2011). Intelligence gathering and resultant analysis is much like building a mosaic (Pozen, 2010; Sales, 2010). It has been posited that investigative journalists would be the mosaic builders rather than terrorists, seemingly implying that the press is functioning as the intelligence apparatus for the terror group (Pozen, 2010). Ross (2011) considers the press as filing in the mosaic when government only divulges partial information to the public.

The Lunev Axiom

Stanislav Lunev, a former Soviet military intelligence officer, considered the U.S. press to be an intelligence asset (Lunev & Winkler, 1998). His account of the Soviet assignment of value of the U.S. press in the furtherance of Soviet intelligence operations is chilling:

I was amazed - and Moscow was very appreciative - at how many times I found very sensitive information in American newspapers. In my view, Americans tend to care more about scooping their competition than about national security, which made my job easier. (Lunev & Winkler, 1998, p. 135)

Bruce (2003) concurred with the Lunev assessment and was first to use the term the Lunev Axiom, defined as: classified intelligence disclosed in the press [being] the equivalent of intelligence gathered through foreign espionage. Bruce's assessment of the threat environment cannot be overstated due to the nature of the nation's adversaries, actual or potential. Unfortunately, the literature and the debate attached to the literature, continues to be mired in legal technicalities and rhetoric that seem to increase potential harm or damage to the nation's intelligence capabilities. Examples include issues related to First Amendment concerns and ambiguities in existing law that weaken enforcement and accountability (Bruce, 2003).

Gup (2004) considered that the obstacles that challenge the journalist and intelligence operatives are remarkably the same and suggested a transparency between the two. The difference, in the end, was the end user of the resultant product. The value of press exposure of classified intelligence information to an adversary could not be overstated, with pro-adversary propaganda, anti-U.S. propaganda, intelligence collection, and operational disruption a by-product of the act. Alson (2008) noted that adversarial entities such as al Qaeda rely on press reporting for their information, with al Qaeda training manuals citing the value of press reporting and giving press credit for about 80% of all al Qaeda-gathered information. Classified information reported by the press then

equated to the press functioning as an intelligence apparatus, validating assessments by Bruce (2003) and Lunev (Lunev & Winkler, 1998).

The publication of leaks had also hindered further intelligence collection and hampered intelligence liaisons with other nations (Schaffert, 2011). Kessler (2008) stated that no less than six countries, unnamed, have scaled back cooperation with U.S. intelligence agencies due to leaks of classified information and publication of their roles related to sensitive projects relating to the War on Terror (Kessler, 2008). Cost studies related to security were many (U.S. Senate, 1997) but studies investigating the impact of press leaks and subsequent publication were lacking or constrained from full public consumption due to the classified nature of U.S. intelligence (U.S. Defense Intelligence Agency, 2013). For example, a portion of the operational costs for a human intelligence operation could include the establishment of a cover and legend as a backstop to the curious (McCadden, 1961). Mission importance determined the type of cover used and damage inflicted by a leak seemed a direct function of the depth of the cover (Wilson, 2007).

United States Intelligence Case Law

Although seemingly flying in the face of the U.S. Constitutional First Amendment freedoms, laws existed that are applicable to the phenomenon (Elsa, 2011). These laws, Elsa (2011) admits, "...are a patchwork of statutes [designed] to protect [classified] information depending upon its nature, the identity of the discloser and of those to whom it was disclosed, and the means by which it was obtained" (p.6). Specifically, these laws were the Espionage Act of 1917, Section 798 of Title 18, commonly referred to as the

COMINT Statutes, and the Intelligence Identities Protection Act of 1982 (Alson, 2008; Caplan, 2013; Richelson, 2012; Schoenfeld, 2010).

The Espionage Act of 1917, enacted two days after the United States entered World War I, was designed to prevent interference with the war effort and, to this day, is the seminal law to dissuade leaks of classified information (Alson, 2008; Meyer, 2014; Schoenfeld, 2013). The Espionage Act included major portions of the Defense Secrets Act of 1911 prohibiting communication of information from or about military installations (Alson, 2008). Coincidentally, further legislation was proposed to censor the press but never enacted (Meyer, 2014). A year later, the Sedition Act of 1918 was passed, which for a three-year period penalized anti-U.S. writing (Meyer, 2014).

In 1921 Congress repealed the Sedition Act and Section 798 of 18 U.S.C. became known as the COMINT Statute, narrowing a portion of information the United States wished to protect, specifically information about communications intelligence activities. This modification was a direct result of the Chicago Tribune's near disastrous compromise of the U.S.'s capabilities to exploit Japanese coded messages in World War II (Alson, 2008). That reporting was, as Schoenfeld (2011) assessed, a function of political differences between the Tribune's editor and then President Roosevelt. It wasn't until 1950 that the Espionage Act was amended to add what are termed the COMINT statutes, designed to protect communications intelligence activities from compromise. The amendment came about as a result of a 1942 story in the Chicago Tribune suggesting that the U.S. had broken Japanese Codes (Risen, 2009; Schoenfeld, 2013).

Although the Espionage Act was quickly enacted by Congress, it took 54 years before, in 1971, the first prosecution for leaking classified documents under its guidance

was attempted, with Daniel Ellsberg being indicted for leaking what became known as the Pentagon Papers to the New York Times (Meyer, 2014). Since Ellsberg's indictment similar indictments, further discussed in this section, were occurring with increasing frequency (Meyer, 2014). Kitrosser (2007b) categorized current government responses to press leaks as "cracking down". Her research attempted to fill in informational gaps due to the belief that there existed a lack of theory and scholarship on the subject of press leaks and free speech.

Revealing the name of a covert agent of the United States was punishable under the Intelligence Identities Protection Act of 1982 (Caplan, 2013). The Intelligence Identities Protection Act of 1982 was enacted as a result of leaks and publication of classified intelligence information. Specifically, the law was a direct result of a book published by an ex-CIA officer, Philip Agee (Risen, 2009; Schoenfeld, 2010). With intent to expose CIA officers operating abroad, Mr. Agee published a book and a periodical dedicated to compromising CIA operatives. One of the CIA officers exposed by Agee was Athens Station chief, Richard Welch. Weeks after publication of his identity, Mr. Welch was assassinated outside his residence in Athens by a Greek terrorist group. A similar armed attack took place in Jamaica. In the end, more than 1,000 CIA agents had been compromised (Schoenfeld, 2010). Although most statutes prosecuted those with authorized access to classified information, when delivering that information to unauthorized individuals receipt of classified information procured in violation of existing statutes was not considered (Elsea, 2011).

Intelligence Precedents

Presidents from Franklin Roosevelt to Barack Obama had been plagued and hampered by leaks of classified government information to the press (Richelson, 2012). Each had taken a decidedly different approach toward the problem and many have weighed the option of pursuing the press in addition to pursuing the leaker (Richelson, 2012). A compendium of representative cases related to press leaks of classified intelligence information is discussed here, as these cases were critical to understanding the evolution of the problem and the steps that constituted reaction from government.

Daniel Ellsberg, leaker of what became known as the Pentagon Papers, attempted to bring his concerns to the U.S. Senate in the months before releasing his documents to the press (Etzioni, 2014). Ellsberg (2010) writing seemed an attempt to justify his actions in compromising, to the press, classified government documents to which he was entrusted. The Pentagon Papers consisted of roughly 4,000 pages of information related to the Vietnam War (Ellsberg, 2010). One of the issues that Ellsberg (2010) concentrated on was the issue of wrongful secret keeping. Unfortunately, he did not denote who is the arbiter of what could be considered "wrongful". Ellsberg (2010) realized that there was a need to keep certain information secret, but admitted that breaking the secrecy agreement was above breaking a normal verbal contract and noted that keeping secrets equates to lying to prevent outsiders from knowing the information that one is privy to. Ellsberg (2010) saw his actions as a form of opposition to the administration and a justification of his views on dissent. As with most other authors commenting on the topic, Ellsberg (2010) steered the conversation toward the concept of over classification of information. Ellsberg (2010) proposed a system for managing the government secrecy apparatus that

included, but was not limited to, immunity from prosecution for leaking information to the press. This point was but one of the myriad of points that would result in an enormous amount of information released to the adversary.

Given technological advances in data transfer and storage as well as an increasingly aggressive and opinionated press, a new era of progression in the phenomenon of classified information leaks and their publication has emerged (Papandrea, 2011). Prosecutions related to leaking classified information have risen and have included Thomas Drake, charged with leaking National Security Agency information to the press and Jeffrey Sterling, charged with providing classified information related to the Central Intelligence Agency to journalist James Risen (Elsa, 2011).

Two seminal cases preceding the Edward Snowden event document the changing leaker-publisher paradigm (Elsa, 2011). These cases involved U.S. Army Private First Class Bradley Manning, who provided hundreds of thousands of classified documents to the WikiLeaks organization and Mr. Stephen Jin-Woo Kim, charged with providing classified information to Fox News, in which Fox News urged Mr. Kim to break his secrecy agreement with the government and violate existing statutes (Elsa, 2011).

In 2010, U.S. Army Private First Class Bradley Manning was convicted of violating the Espionage Act for disclosing approximately 750,000 classified documents relating to national security operations in Iraq and Afghanistan, Guantanamo Bay and policy to the WikiLeaks organization (Caplan, 2013; Etzioni, 2014). Sangarasivam (2013) addressed the Manning event as an act of cyber rebellion, characterizing it in the same context as the struggle between David and Goliath.

The Manning/WikiLeaks event represented the first of a changing paradigm in the leak/publication continuum – moving from a single document leak from a relatively high-level individual to bulk data releases from low-level individuals with little knowledge of the potential impact. Heemsbergen (2013) coined the term “radical transparency” in regards to journalistic and democratic evolution stemming from technological and informational advances. The leak-to-publication paradigm had been altered by these advances and a changing consideration of who is considered a journalist. Using the Bradley Manning/WikiLeaks case as an example, Heemsbergen (2013) illustrated the rapidly changing landscape from traditional publication of classified information to mass release of documents with little regard to impact or public interpretation.

Vladeck (2012), discussing the Bradley Manning/WikiLeaks event, questioned if WikiLeaks founder, Julian Assange, would have First Amendment protections, leading one to question whether the entity known as WikiLeaks can qualify as journalist? Elsea (2011) also considered the concept of whether information leaked from an American to the foreign press, and subsequently published, violated U.S. criminal law, specifically, whether the foreign press – in the form of WikiLeaks – could be prosecuted?

In another example, in 2010 Stephen Jin-Woo Kim was charged with giving Fox News reporter James Rosen classified documents related to North Korea’s nuclear program that specifically stated that the U.S. had an intelligence source placed within the North Korean leadership (Etzioni, 2014; Meyer, 2014). This case was highlighted by Mr. Rosen’s efforts to establish a relationship in order to elicit information from Mr. Kim and labelled “covert solicitation” (Meyer, 2014; Schoenfeld, 2013). Mr. Kim received a 13-month prison sentence and his accomplice, Mr. Rosen, was never charged (Meyer, 2014).

Peculiar to the Manning and Kim cases, and what has been reported through the media on the Snowden case, was the behavior of the press in communicating with their sources (Schoenfeld, 2013). Espionage tradecraft, in the form of codes, encrypted communication, digital dead drops, and the use of aliases has been present in all three cases (Schoenfeld, 2013). As Schoenfeld (2013) surmised, "...the line between journalist and spy blurs..." (p. 66).

Intelligence Perspectives

Intelligence had always, by its nature, been a secretive affair, and importantly, leaks to the press were not a new phenomenon. Both Dulles (1963) and Bruce (2003), former intelligence officers, discussed the value of press leaks of classified intelligence information. The former Director of Central Intelligence and Office of Strategic Services operative, Dulles (1963) highlighted the case of Pavel Monat, a Polish intelligence officer assigned to conduct espionage in the United States on behalf of the Polish government in the 1950s. Monat assessed, relating to U.S. national security weaknesses, that American's craved public recognition and that "Americans are not only careless and loquacious in their speech, they also give away far more than is good for them in print" (Dulles, 1963, p. 239). Although dated, the same sentiment was echoed exactly by Bruce (2003) 40 years later using Lunev as his example suggesting the same level of persistence in the phenomenon in the 21st century.

Solutions to the problem reflected the tone of the day. Dulles (1963) mentioned, but did not suggest, moving toward a version of Britain's Official Secrets Act, primarily due to press protections afforded journalists through the First Amendment. Britain's Official Secrets Act of 1989 penalized the possession of classified security, defense,

intelligence, or international relations information to unauthorized individuals regardless of whether the individual's status was as a member of the press (Official Secrets Act, 1989). A decidedly more aggressive stance was taken by Bruce (2003), calling for reconsideration of First Amendment press freedoms. The change in attitudes over the span of 40 years seemed to be explained by two factors. The first factor was a changing national security threat environment, moving toward nonstate actors versus the traditional state or state-sponsored entities. The second was the rapid advancements in technology that allow nonstate actors access to technology, infrastructure, and information, that was on par if not better than a state's intelligence services, allowing nonstate actors instantaneous information, infrastructure, and the ability to quickly act (Bruce, 2003; Papandrea, 2011; Ross, 2011).

Former CIA Director, James Woolsey, suggested a three question litmus test that the press should apply before publishing classified national security information (Smolkin, 2006). Woolsey's suggestions centered on 1) whether oversight mechanisms are in place? 2) whether abuse had taken place? and, 3) whether what was being reported concerned collecting intelligence on national threats (Smolkin, 2006). Although one of many opinions on whether or not answering these questions would mitigate compromising national security information to the nation's adversaries, it was one of the few opinions published from an intelligence community insider (Smolkin, 2006).

Press Perspectives

The press has differing views on the impact of publishing leaked information. Reporters are motivated by significant personal gain in the monetary or notoriety form when considering whether or not to publish a story, regardless of national security impact

(Risen, 2009). The press' concept of providing comfort to those afflicted by government and, at the same time, afflicting those in a position of power self-proclaimed the watchdog role to monitor government (Kovach & Rosenstiel, 2007). Hillebrand (2012) suggested that one should fit the media into the intelligence oversight framework, citing a need for openness and accountability. And, further, the role of the media in intelligence oversight was an under-explored area in academia, noting that the typical form of media discovery of intelligence activities was through leaks of classified information.

Evidence also suggested that press had become, in its self-proclaimed role as the fourth branch of government, increasingly adversarial due to its ability to influence government policy and decisions (Schaffert, 1992). The press, "the fourth estate," as it had become known, behaved on the principle that the government's affairs should be known to all citizens, not just restricted to those in the government itself (Kovach & Rosenstiel, 2007).

Risen's (2009) research suggested that reporters felt they considered the national interest first and foremost and were cognizant of their power and ability to harm national security. This was in sharp contrast to the Wallace/Jennings reaction as documented by White (1996) and Schoenfeld (2013). In 1987 journalists Mike Wallace and Peter Jennings, panelists on a workplace ethics roundtable discussion, were given a hypothetical scenario. In the scenario they were embedded with enemy forces and learned that those same forces were about to ambush American troops. The reporters were asked if they would film the ambush or warn the American troops ahead of the attack. Both answered that they would not inform the Americans of the impending ambush (White, 1996).

Arguments were made that the press had a duty to inform the public and that without leaks the job would be near impossible (Nelson, 2002) and leaks are tolerated by the public (Lee, 2008). Similarly, Papandrea (2014) notes that the trend in attempting prosecution of the press had resulted in a decrease in individuals – potential sources – willing to come forward and leak information and that, in turn, underserves the public’s right to know about the inner workings of government.

Confusion existed, though, that the Constitutional First Amendment right to publish equated to a right to access (Schaffert, 1992). Such was not the case, affirmed by numerous instances within case law (Schaffert, 1992). The press, then, seemed to be relegated to subsisting on “leaks” to ply their trade in government information. The government disclosing information surreptitiously, without source attribution, was termed an “authorized leak” and lent itself toward a symbiotic relationship with the media (Sedler, 2007). Conversely, “unauthorized leaks” from government officials lent themselves toward an adversarial relationship with the media. Arguments were made that the government selectively leaked information to further its own agenda as well as influence foreign governments, a sort of propaganda effort (Elsea, 2011; Papandrea, 2011).

As a function of reporting on the nation’s intelligence efforts, views existed on diametrically opposed points on the spectrum. Gup's (2003) argument was that "sources and methods" are valuable, but not sacred, and that the press should be the arbiter of whether an intelligence source or method of collecting intelligence is valuable. Gup (2004) noted that implications had been presented in literature that the press holds the same status as the nation’s intelligence apparatus and should be skeptical regarding

intelligence reports. Gup's rationale invoked past intelligence failures as well as politicians who cited politically motivated and massaged intelligence information. These intelligence failures included, but were not limited to, the 1960's Bay of Pigs invasion and the incorrect assessment of support against Fidel Castro, target misidentification in Yugoslavia resulting in the 1999 aerial bombing of the Chinese Embassy in Belgrade, and the incorrect Iraq Weapons of Mass Destruction assessments (Gup, 2004). Other views suggested alternate perspectives on information secrecy versus newsworthiness (Stone, 2007), and a level of illegitimacy for the reasons that government classifies information (Stone, 2011). These illegitimate reasons included the prevention of embarrassment of government officials, a reluctance to face public criticism, or denying other branches of government an opportunity to provide oversight of decisions (Stone, 2011).

Analyzing the press and their hunger for a "scoop", Schaffert (1992) noted that the press tends to magnify levels of violence. The existing press mentality to sensationalize and comment (Perl, 2006), versus report on stories, reflected a pack journalism mentality to report no matter the harm because, in their view, "[The obligation of the press] is not to deliver the news. [The press'] obligation is to do good programming" (Kovach & Rosenstiel, 2007, p. 151). Conversely, a body of knowledge existed that the "media should be left to control themselves so long as they control themselves" (Schaffert, 1992, para. 1). Of the three levels of censorship noted by Graber (2002), two of the three considered utilizing measures of media self-restraint or self-censorship. Self-restraint was, many times, non-existent, because some media believed disclosure of classified material did not inflict damage to national security (Risen, 2009).

Sedler (2011) presented a bi-polar world relating to press self-censorship. The researcher posited that self-censorship had both in its form, good and bad. He considered press self-censorship a good quality in a couple of instances, specifically, when national security is at issue. He also made the case that, when related to government intervention in the publication process, post-publication sanctions would not have been tolerated unless the government could prove damage to national security. Sedler (2011) further contended that this sort of post publication sanction came with its own pitfall, revealing more classified information to stem the tide of the already compromised classified information. This concept of revealing additional information had traditionally been a roadblock to the prosecution of publishers (Schoenfeld, 2013). The press' controlling standard was to report a story if it is newsworthy, and although the press may listen to government concerns, it would make the final decision as to what was published (Smolkin, 2006).

Unfortunately, intelligence sources and methods revealed by the press as a result of leaks have done considerable damage (Kessler, 2008). Kessler (2008) assessed that the work of the intelligence community was safer in the present day, using a lack of any new terrorist attack on US soil as testimony. Unfortunately, Kessler failed to realize that a lack of a new attack may not have been a measure of success on the side of the intelligence community, but perhaps a level of patience on the part of the adversary (Lumbaca & Gray, 2011).

According to Sedler (2007), as the First Amendment protected the media, it also seemed to encourage editorial discretion, allowing the media to decide what got published. As a function of the reporting process, the press asserted that their decision to

release leaked classified information was a deliberative process, beginning with a tip and usually involving multiple sources (Smolkin, 2006). Papandrea (2014) noted that the traditional press had been cooperative with government and responsible in their publication decisions. This relationship Papandrea (2014) characterized as routine, with the press self-limiting their publication of classified material in order to protect the national security interest. This seemingly had not been the case with what once was considered the non-traditional press. But the press seemed to have a persistent fear. The press, in general, feared the prospect of being prosecuted and more so the possibility that the espionage statutes may apply to them (Smolkin, 2006). Kitrosser (2007b) comments that much of what was accepted and encompassed under the rubric of modern journalism could encroach on the Espionage Act.

Sedler (2011), quoting editors of the New York Times and the Los Angeles Times in a 2006 op-ed article, noted that these publishers believed that their reporters did a credible job removing operational intelligence from their articles due, in part, to the ability of the adversary in the digital age to read their reports. What was not addressed was the long-term mosaic effect of the reporter's dispatches when examined and analyzed by the adversary (Kitrosser, 2008). These editors also believed themselves to be stewards of classified information, when considered with government requests to withhold or suspend publication in many, but not all, cases (Sedler, 2011). Hillebrand (2012) stood up for the media, citing their normal tendency to withhold stories until they were checked with government off the record. Few reported instances existed where the press did not publish classified information leaked them (Schoenfeld, 2013). Smolkin (2006) noted that even at the request of the President to refrain from publication, the press published

stories that seemingly harmed national security. If any variance existed, it would present itself in the form of time, whereby the press published the story only after a period of time had passed (Smolkin, 2006). For example, in 2005, The New York Times was personally asked by then President George W. Bush to refrain from publishing a story on the National Security Agency's monitoring of terrorist communications (Schoenfeld, 2013). Despite the President's pleas, the story was published, followed by another story discussing sensitive counterterrorism programs. The press had managed to broadcast details of sensitive government surveillance programs to the public, including those considered adversaries, without reprisal from government (Schoenfeld, 2013).

Prosecutions of the press for leaking classified information had, historically, been few and insignificant in nature (Papandrea, 2014). Criminal leak prosecutions were, until recently, a rarity. However, perhaps due to the function of increasing press aggressiveness, a global press readership, and technological advances in information distribution, prosecution of leakers and the press are at an all-time high (Papandrea, 2014). Leak prosecutions undertaken by the administration of U.S. President Barack Obama have eclipsed the number of leak prosecutions by all his predecessors combined, eight versus three (Meyer, 2014; Schoenfeld, 2013).

In addition to Mr. Snowden, the focus of this research, and in the cases of Private First Class Bradley Manning and Mr. Stephen Jin-Woo Kim, discussed previously, the administration of President Barack Obama has prosecuted Thomas Drake, Shamai Leibowitz, John Kiriakou, Jeffrey Sterling, and James Hitselberger under the Espionage Act of 1917 (McCraw & Gikow, 2013; Meyer, 2014). Mr. Thomas Drake, a National Security Agency executive, leaked sensitive classified documents to the press related to

National Security Agency collection program inefficiencies (Meyer, 2014). Mr. Drake's case was remarkable in that, originally facing ten felony counts of providing classified information via covert digital dead drop techniques to the Baltimore Sun, he pled to a simple misdemeanor (Papandrea, 2014; Schoenfeld, 2013). Shamai Leibowitz leaked material detailing communications intelligence activities to a blogger relating to U.S. efforts to gather intelligence in Israel. He was convicted and received 20 months in prison (Meyer, 2014; Richelson, 2012).

Jeffrey Sterling, a Central Intelligence Agency employee, leaked classified intelligence information to James Risen of the New York Times (Caplan, 2013). Specifically, Mr. Sterling leaked classified details of U.S. government efforts to affect Iran's nuclear program (Schoenfeld, 2013). John Kiriakou, a former Central Intelligence Agency employee, was charged under the Intelligence Identities Protection Act with disclosing to numerous members of the press the names of at least one Central Intelligence Agency agent and other classified programs. He received a 30-month prison term (Meyer, 2014). Lastly, James Hitzelberger was charged under the Espionage Act for revealing U.S. intelligence gaps in the Persian Gulf region to a university think tank (Meyer, 2014).

Although acknowledging that secrecy was essential to national security and democracy, excessive security was viewed as undermining both: thus, news outlets were their own arbiter as to what constitutes a true "secret" (Risen, 2009). Sedler (2011) commented on Schoenfeld's (2011) work extensively, with much emphasis on the concept that the press was acting as the unelected authority as to what may have been a legitimate secret or not. This question lies at the heart of the research and seems primarily

a factor of not knowing the impact of the press publication of the leaked classified information.

History justified the press believing automatically that a wrong was being committed and that the national capabilities of the intelligence services were being turned on its own citizens (Ross, 2011, Pozen, 2013). The press believed that they should decide if and when to publish national security secrets due to an inherent mistrust of government officials and, in their view, the government's tendency to over classify information (Freivogel, 2009). The press was the sole evaluator and, thus, arbiter of a classified document or, at times, in the case of Manning and Snowden, hundreds of thousands or millions of documents, respectively (Etzioni, 2014). Risen (2009) noted that "...a decision to disclose a national security secret ought to balance the benefit to public knowledge against the national security harm of disclosure" (p. 2236). Some editors have noted that when making a decision to publish leaked classified material, a balance between the public's right to know and national security had to be struck and many times that decision was based on instinct (Smolkin, 2006). Some in the press tasked with making the publication decision acknowledged that they were not qualified to assess the information thrust in front of them and yet, when the decision was made to publish, the government was powerless to appeal (Etzioni, 2014).

Freivogel (2009) asked important questions concerning reporter qualification to judge the national security impact and the societal gain of publication of classified national security information. Specifically, when a journalist was not trained and qualified to evaluate classified national security information and lacked appropriate security clearances, how could the journalist judge the national security impact and

societal gain if classified information was published? Secondly, was the decision to publish national security information based on an editor's judgment or the judgment of a staff of lawyers? Finally, he questioned how journalists held themselves above existing law in publishing information gathered through illegal leaks. The researchers concluded that reporters should maintain the status quo of retaining confidential sources and fighting for reporters' rights under the First Amendment of the U.S. Constitution. This conclusion was reached under the filter of overwhelming public support for a reporter's right to protect confidential sources (Freivogel, 2009).

In fact, significant debate existed as to who could be qualified as the "press". Freivogel's (2009) interpretation of what constitutes the press extended existing definitions to add that the person should regularly gather news as part of a person's livelihood and exact financial gain from the endeavor. Vladeck (2012) suggested three standards to make the determination of what constitutes the "press". These standards included whether there was a set of professional standards for the organization, an accrediting body to assess educational standards, and legal precedent to determine who qualified as a practitioner in the field (Vladeck, 2012).

U.S. Government Perspectives

The United States government assessed that press publication of leaked classified intelligence information has cost the American taxpayer hundreds of millions of dollars as well as impaired its intelligence collection capabilities (Bruce, 2003; Silberman & Robb, 2005). Risen (2009) further noted that exact details of the damage existed in classified reports, not available to the public and, more importantly, fear existed that damage reports may compromise more secrets. One reason for a lack of prosecution in

many of the leak and publication cases was the concept that bringing a case to trial would reveal additional secrets as well as the importance and gravity of the initially revealed information (Risen, 2009).

Divoll (2011) reported that, in Congress, the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence was the repository for classified information, and charged with its safe handling and dissemination to the members of Congress. Seemingly, it stands to reason that because Congress represents the people, the people are informed by proxy of classified intelligence information without releasing the information to an adversary. Further, should extraordinary information of a classified nature about covert action programs require the executive branch of government to inform Congress, the executive branch had the option of narrowing the number of people that he notified to a select eight (Divoll, 2011). These individuals, the select eight, included the chairmen and ranking members of the House Permanent Select Committee on Intelligence and the Senate Intelligence Committee, and the majority and minority leaders of the House and Senate. The eight members were chosen due to their positions and functioned as a clearing house for intelligence information within Congress (Divoll, 2011).

Leaks of classified intelligence information were cited by government as a challenge, increased by the fact that few journalists had the background to assess the information that they happened to receive through leaks (Hillebrand, 2012). The U.S. Government had questioned how the press could render assessments of the national security value of leaked information, categorizing them as arrogant and misunderstanding of the information (Smolkin, 2006). The press seemed to want to be the only arbiter as to

whether a piece of information is classified, as well as make the assessment as to its national security value. The government believed that trained intelligence personnel should be the arbiters of whether to inform citizens about classified national security programs citing, in part, a lack of legal precedent granting journalists protection of their confidential sources (Freivogel, 2009).

Invoking the First Amendment of the Constitution of the United States may not be an automatic defense for journalists (Silver, 2008). But the press had been seemingly empowered by the Supreme Court – exemplified in the Pentagon Papers case – acknowledging the press’s freedom to reveal government secrets and inform the people (Smolkin, 2006). The press believed that, when publishing classified national security information, they were afforded protections under the First Amendment – a concept only partially true and as a result of a lack of prosecutions by government (Freivogel, 2009). Protection of confidential sources were not a First Amendment right, but more a contractual agreement resulting from a reporter’s verbal assurances (Freivogel, 2009).

As of late 2007, scholars believed that the government could not punish a journalist unless that journalist incited a leaker to disclose classified information, knew the information would harm national security, and knew that the information would not contribute to the public debate (Vladeck, 2007). How any of these criterion are measured was a matter of debate, with the press thinking they were the sole deciding entity. The first element was addressed by the press’ self-assessment that the material they publish was newsworthy and of public concern on the basis of exposing government wrong-doing (Vladeck, 2012). Relating to the second criterion, Vladeck (2012) admitted that journalists were, at best, highly skilled amateurs when assessing threats to national

security, but also believed that much of the government's classified material should have not been classified in the first place. Interestingly, Weaver and Pallitto (2005) indicated that even federal judges felt incompetent in assessing whether information, if revealed in the public domain, would harm national security.

Government options in response to press publication of classified national security information, according to Freivogel (2009), came in three forms: a) obtaining an injunction barring publication; b) prosecuting journalist and source alike under the provisions of the Espionage Act; and, c) compelling the journalist to reveal their source to a grand jury. The government could punish the leaker in two capacities, as an employer or as the sovereign (Kitrosser, 2013). The employer function could be applied as the employee/leaker was violating the secrecy oath that was signed as a prerequisite for access to classified information. Indeed, these individuals were placed in a position of trust by the government, their employer, and relied upon to protect the information in their charge. Thus, an implication exists that the employee, by virtue of his/her access, waived First Amendment protections as a condition of that same access (Kitrosser, 2013).

Government had two options when attempting to stem the tide of information that effortlessly reaches an adversary: either stop the leaker or stop the publisher (Etzioni, 2014). Traditionally, this had come in the form of prosecution using two existing statutes, the Espionage Act of 1917 and the Intelligence Identities Protection Act of 1982 (Elsa, 2011; Klarevas, 2006; Risen, 2009; Vladeck, 2007). These statutes were considered flawed due to limitations on applicability and their assessment as being unwieldy and imprecise instruments (Lee, 2008).

A continuing topic related to the phenomenon was government punishment of journalists for publishing classified information (Schoenfeld, 2010, 2013; Silver, 2008). Silver (2008) noted that this punishment could be for either the possession or publication of classified material, the former addressed in statutes and the latter a topic of great debate and increasing frequency. Arguments arose debating that when the media published classified information they were in fact in possession of the material. Indeed, there may be a case when the media were themselves aware that the information that they published was stolen (Silver, 2008).

In 2008, Silver summarized the 1973 seminal work of Edgar and Schmidt examining the Espionage Act of 1917. Importantly, Edgar and Schmidt believed the Espionage Act did not apply to the press (Silver, 2008). The release of classified information was prosecutable for those who have authorized access i.e., the government employee. One with unauthorized access, the publisher, seemed to escape any level of liability unless a pattern could be established showing the publisher was intentionally harming the state (Papandrea, 2011). Regardless of one's views of the Espionage Act, the Act remained standing law and could be used to prosecute journalists (Freivogel, 2009).

First Amendment rights protected the press and forbade government from restraining publication unless the story threatened "grave and immediate danger to the security of the United States" (Kovach & Rosenstiel, 2007; Stone, 2011). Cohen (2009) admitted that although the First Amendment of the Constitution provided for freedom of speech, there were instances where the government could attempt to restrict speech. Issuing injunctions in cases such as the Pentagon Papers was an example of government attempting to exercise prior restraint (Cohen, 2009).

The prior restraint doctrine, compelling publishers to withhold publication of information when that publication would result in damage to the nation, was a possible remedy to the current phenomenon (Sedler, 2007). Referencing the Pentagon Papers case against the New York Times newspaper, Justice Stewart affirmed that certain circumstances could exist to allow the doctrine to be applied (Sedler, 2007). All of the released Snowden information falls under a category that would allow the application of the prior restraint doctrine (Lowe, 2014). Specifically, this was information relating to the communications intelligence activities of the United States or foreign governments or the information resulting from those activities (Sedler, 2007).

Although there was evidence suggesting a correlation between press publication and adversary effectiveness (Schaffert, 1992), the burden of proof rested on government and, not surprisingly, had resulted in not a single successful prosecution (Lee, 2008; Silberman & Robb, 2005). Importantly, it was considered that the difficulty in prosecution weakened the deterrence provided by the law itself (Morrison, 1966). Similarly, Risen (2009) contended that the media and the concept of media restraint was the solution to the problem of leaks and emphasized that current statutes were essentially unenforceable.

Although the common view advocated press freedoms and leaker prosecutions, Kitrosser (2013) argued that leakers should be afforded equal First Amendment protections under the premise of free information flow in support of a constitutional democracy. Conflict arose when free speech and information flow countered the executive branch's capacity and mandate to keep secrets in the furtherance of national security objectives. Oft cited was the potential for executive branch abuse of power

(Kitrosser, 2013). The question then became what portion of the total leaks of classified intelligence information could be categorized as abuses of power? More so, who defined abuse of power? Indeed, as Kitrosser (2013) admitted, it was unethical for the executive branch to censor an employee of the press by classifying information, but that must be countered by the notion that the executive branch must keep information secret and out of the hands of the nation's adversaries.

Papandrea (2014) considered that leakers had considerable First Amendment rights. This view was counter to prevailing opinion among the public, scholars, and commentators. Papandrea (2014) did support the government's right to prosecute leakers when an immediate threat to national security outweighs the public interest. Missing in this narrative was a discussion on who could be the arbiter of the information's applicability to national security and what may happen when, in the process of informing the public, one also informed the enemy?

Current events seem to suggest a changing tide toward holding the press accountable for its conduct in releasing sensitive and classified documents relating to U.S. national security to the public including, one can assume, her adversaries. Caplan (2013) opened the discussion on leakers, their arguable role as de-facto spies and the culpability of journalists in being their communications apparatus to the adversary. Referencing the Espionage Act of 1917, which was meant to guard against the publication of the nation's secrets, consensus seemed to indicate that a trend is developing in prosecuting the entire leak/publisher team (Caplan, 2013; Etzioni, 2014; Meyer, 2014). Arguments countered this notion under the premise that punishing the

press for publishing classified information considered the fact that no other statute offers the option of punishing the publisher for their words (Silver, 2008).

The problem of leaking classified intelligence information to the press is disturbing, despite the motivation of the leaker, be it carelessness, malice, or greed (Morrison, 1966) or modern political motivations and whistleblower concerns such as wrongdoing, inefficiency, or mistakes (Nelson, 2002). The leaker, before committing the act, had numerous avenues to air the grievances that included, but were not limited to, the immediate supervisor, the given intelligence agency's Inspector General process (Vladeck, 2008), as well as his or her Congressional Representative. Any of these alternatives, should they have been chosen, could keep the classified information "in-house" and out of reach of an adversary's prying eye (Radack & McClellan, 2011).

Alternatively, the government had the option to declassify the information and release it to the public at large. Again, using Mosaic Theory, this option could have allowed an adversary the opportunity to defeat the existing intelligence collection apparatus given the information released (Kosar, 2009; Pozen, 2005). Schoenfeld (2013) argued that declassification will slow leaks but admits that the system by which declassification occurs was inefficient, with 20 million pages declassified of 45 million reviewed in 2013. These though, were pages of documents at least 25 years old and although seemingly a step in the right direction, were not reflective of the 58 million pages of documents that had yet to be reviewed.

The Secrecy Debate

Aftergood (2010) assessed the debate on secrecy as having two sides, the first being that government secrecy was incompatible with a democratic society and yet

necessary for the protection of national security related activities. His central thesis was that too much information has been classified. Goodwin (2010) suggested that secrecy and transparency existed on equal footing but cloaking material under the national security blanket had resulted in excessive secrecy.

Danielson (2011) addressed the topic of secrecy utilizing the filter of the volume of personnel possessing security clearances, questioning whether an item of information could be truly secret if hundreds of thousands of people are witting. This question was previously answered by Doorey (2007), who reported that at times hundreds of personnel are required to address the span of intelligence activities that included, but were not limited to, planning, collection, processing, analysis, and reporting and dissemination of the resultant intelligence. The U. S. Government was placed in a precarious position, where applicable employees were bound by a secrecy agreement that was voluntary in nature (Ellsberg, 2010; Stone, 2011). Violation of that contract existed when the employee leaked the information (Stone, 2011). Thus the argument began on the free speech implications for government employees and translated through to the press's right to publish (McCraw & Gikow, 2014). Many jobs in government required security clearances and one to maintain secrecy as a function of the employee's obligation under a secrecy agreement (Lee, 2008). The agreement was the prerequisite to gaining and keeping one's access to classified material so one can accomplish one's mission or do one's job (Lee, 2008). Ellsberg (2010) assessed that the signing of the secrecy agreement tended to admit the individual into an informal group and was instilled in one's core identity. Critical to that secrecy agreement was the assumption that one would not release the classified information that one was entrusted (Lee, 2008). Ellsberg (2010) also

equated the promise to maintain secrecy as a promise to lie if that lie entailed keeping the secret.

Divoll (2011) emphasized to the reader that many who complain of too much secrecy – including many author’s views in this literature review – were under informed as to the nation's needs vis-à-vis foreign affairs and national defense and that despite democracy’s need for openness, secrets were a necessity. As was the case with most, if not all authors, was the lack of discussing the media’s role of delivering vital information to the adversary instead, in Kitrosser’s (2007b) case, turning the conversation toward the use – or misuse – of classification powers by the executive branch.

Emerging Trends

A share of the blame on the increase of leaks in both depth and breadth may have possibly been related to increased information sharing and responses to the terrorist attacks of September 11th, 2001 (Sales, 2010). Resultant reduction of existing intelligence information stovepipes, erected in the 1970s, allowed even the lowest level of individual access to the most sensitive elements of intelligence information. Schaffert (1992) commented that terror organizations tended to manipulate the media for their advantage but in some countries the media tended to side with the host nation government. Examples of countries where the media sided with government were Italy, the United Kingdom, and Germany, whereas the opposite was true in the United States, with the media taking on an adversarial role. Kitrosser (2007b) saw the adversarial press role as healthy to maintain a balance against government excesses. The adversarial role grew stronger when the press received “unauthorized” leaks (Sedler, 2007).

Leaks of classified information to the press were trending toward lower-level employees revealing information, the rise of bulk releases, a function of technological advances, and the trend of the press submitting to the public that it was in their best interest to know this information as it could possibly be turned against them (McCaw & Gikow, 2014; Papandrea, 2014; Pozen, 2013). Silver (2008) seemed to imply that individuals who seek out national security information through leaks, no matter the motive or employer, should be treated as journalists because they were behaving as journalists. Thus, these individuals required First Amendment protections.

Summary

Consensus held that the release, or leaking of classified intelligence information to the press placed intelligence sources and methods in a dangerous position (Bruce, 2003; Grabo, 2004; Silberman & Robb, 2005), providing a level of "aid and comfort" to adversaries of the U.S. (Smolkin, 2006). Press reporting of an event did not independently corroborate an event (Grabo, 2004) nor did it constitute declassification, but it did validate the information in the eyes of the adversary (Ross, 2011). In either case, the press had made a conscious decision to be the arbiter of whether classified intelligence information was actually classified (Smolkin, 2006) and to endanger classified intelligence sources and methods. The impact relating to the publication of leaked classified intelligence information was the unknown quantity in the equation of First Amendment freedoms, secrecy, Intelligence Community effectiveness, and overall national security. An "all or nothing" mindset or preference has existed in the press, with little regard paid to national security concerns, with some believing that permitting the publication of sensitive national security information, on occasion, was permissible given

the overarching good that a free press played in a democracy (Papandrea, 2011). But two schools of thought ultimately existed. One believed that it is the government's responsibility to keep its information secret (Hoekstra, 2005; Morrison, 1966) and the other that it was the responsibility of the press to report with due diligence, but not compromise information that would potentially jeopardize national security concerns (Bruce, 2003).

Common thinking was typically self-centered as the press as well as academicians cautioned against prosecutions of so-called third party publishers, "the press," focusing instead on the leakers themselves (Kitrosser, 2013). Mr. Snowden's case may exemplify many of the issues raised in this literature review. The impact to the nation's intelligence capabilities and the overall national security as a result of their unauthorized disclosures deserve an in-depth investigation. The under theorized and understudied nature of the phenomenon was echoed by Pozen (2005, 2013), revealing numerous findings on leak cases in which single events or programs were leaked to the press through unauthorized disclosure. But little research had been conducted into all-encompassing "data dumps" and subsequent publication of millions of documents as exemplified by Mr. Snowden's 2013 disclosure. Nowhere in the press view of the phenomenon did the concept arise that they were delivering information to adversaries as well as to the "public" (Schoenfeld, 2010). Etzioni (2014), writing in the William and Mary Bill of Rights Journal, places the problem in its rightful context:

"...although there seems to be considerable evidence of harm, it is very difficult for a non-specialized observer, without access to classified information that has

not been leaked, to render a definitive judgment on the extent of the harm in many of the cases (Etzioni, 2014, p.1159).

Chapter 3: Research Method

The press regularly published classified intelligence information leaked to them by those with authorized access and varied motives (Bruce, 2003; Ross, 2011; Schoenfeld, 2011). Naturally this information, to an adversary, was held to a standard equivalent to information gathered through standard espionage tradecraft (Bruce, 2003; Lunev & Winkler, 1998). Edward Snowden personified this increasing phenomenon of classified intelligence leaks. In 2013, Mr. Snowden gave highly classified U.S. intelligence information to the press, specifically Britain's Guardian newspaper and the Washington Post (Heemsbergen, 2013; Lears, 2013). The problem addressed in this study was what are the impacts to U.S. intelligence from the unauthorized bulk disclosure of classified intelligence information from Edward Snowden to the press including, but not limited to, revealing intelligence sources and methods, capabilities, loss of intelligence liaisons and accesses to territories essential for U.S. national security (Ross, 2011; Schoenfeld, 2011; Johnson, 2014). The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. The following question and sub questions guided this study.

Q1. What are the impacts on U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press?

SQ1. What are the impacts on U.S. intelligence sources and methods?

SQ2. What are the impacts on U.S. intelligence if capabilities were revealed that were previously unknown to adversaries?

SQ3. What are the impacts on U.S. intelligence if liaisons and access to territories in which to conduct intelligence activities were revealed?

SQ4. What emerged as other impacts on U.S. national security from Snowden's unauthorized disclosure of classified intelligence information to the press?

This chapter will cover the research method and design, the population, sample, instruments or materials used for the study, and data collection, processing and analysis. This chapter will then finish with a discussion of research assumptions, limitations and delimitations, and ethical assurances.

Research Method and Design

Qualitative research methods were chosen over its quantitative counterpart to understand the depth and breadth of the Snowden information release in the non-fiscal context (Yin, 2014). A quantitative research method would have proved successful had fiscal impacts been examined, but not nearly so examining non-fiscal impacts to national security where the interpretation of experts lends to the understanding of the case (Stake, 1995).

A single-case, holistic case study was appropriate as a research design to answer the research question and sub-questions. Reasons included the lack of a concrete understanding of the phenomenon, the lack of scholarly examination of the phenomenon vis-à-vis its impact, and the contemporary nature of the topic (Yin, 2014). Likewise, the case study was appropriate because one was describing the impact of events and

considering information release that this event affected many different parties (Kohn, 1997).

Population

The population for the study was the unauthorized, classified intelligence documents disclosed to the media by Edward Snowden. These documents, according to published accounts, numbered in excess of 1.7 million (Johnson, 2014). The U.S. government stated that they knew exactly what documents were downloaded by Mr. Snowden, but that information remained contained within classified and controlled government channels (U.S. Defense Intelligence Agency, 2013). But, the exact number leaked to the press was known only to Mr. Snowden and the press (Price, 2014).

Sample

The sample for this study was the leaked, classified intelligence information from Edward Snowden, published by the press, (8,542 newspaper articles published between November 1, 2001 and May 2013) that significantly compromised national security. These included, but were not limited to, revealing intelligence sources, methods, capabilities, liaisons and accesses to territories essential for U.S. national security. The sample was gathered using the researcher's specialized knowledge of U.S. intelligence and national security (Berg, 2004, Creswell, 2009).

Materials/Instruments

The Northcentral University Library and other credible online websites were conduits to gather the online archival data. NCU Library databases included, but was not limited to EBSCOhost, ProQuest and LexisNexis, to access the primary data of the original leaked and published classified documents. Primary data were also gathered from

online intelligence and national security experts' websites and online news organizations to supplement database data by filling informational gaps. These gaps arose when a story was reported that was attributed to Mr. Snowden's leaks, but without the leaked primary source document. One example of such an online source was www.schneier.com, security expert Dr. Bruce Schneier's website. Dr. Schneier has gathered and made available online a number of the leaked documents from Mr. Snowden (Schneier, 2015). Similarly, the online news organization, *The Intercept*, co-founded by journalist Glenn Greenwald (2015), provides original source documents, as turned over by Mr. Snowden and ancillary documentation including intelligence and security experts' perceptions and analyses of the documents.

Secondary data gathered for triangulation included intelligence experts' assessments of intelligence damages from the leaked, published documents, and if available court records and first person accounts of the impacts to U.S. intelligence. This data were collected through the same databases as the primary data as well as queries of archival databases, archived physical records, and other declassified records within the holdings of the U.S. National Archives and Records Administration (NARA), if available (Yin, 2012, 2014).

Data Collection, Processing, Analysis

After receiving NCU Institutional Review Board approval, primary and secondary archived data were collected from online databases and credible online intelligence experts' websites, news organizations, and national databases. Secondary data included information to document the national security ramifications of publishing classified intelligence information leaked to the media. These data were supplemented with the

leaked source documents collected from the Schneier and Greenwald online websites, discussed in the materials section.

Data processing enlisted the use of QSR International's NVivo qualitative research software to build a database matrix with coding cells in which to input the data. Per standard intelligence analysis terms codes included, but were not limited to, intelligence sources, methods, liaisons, and access to territories. After initial data were inputted and coded, government assessments as to damages affecting U.S. intelligence activities and U.S. national security as a whole were input. These data were added to the matrix for triangulation to corroborate the initial analysis of information contained in the published leaked documents and news stories that didn't publish the documents but attributed information to leaked documents (Patton, 2002; Yin, 2014). Documents were analyzed for compromises in intelligence sources, methods, capabilities, and loss of liaisons and accesses to territories until saturation occurs (Eisenhardt, 1989; Mason, 2010).

Assumptions

Assumptions in this study were many, including issues relating to information accuracy and truthfulness, and issues relating to adversary access to classified intelligence information. Information gathered for the study, being of a classified nature and released by the press, was assumed to be truthful and accurate given its inherent classified nature and not classified to hide neglect, mismanagement, malfeasance, or constitutionally illegal government activities. They were, thus, assumed authentic and unaltered and satisfy any potential limitations (Stan, 2010). Further, all documents and activities examined in this research were assumed legal and vetted by appropriate

oversight mechanisms, backed by existing statutes. Finally, it was assumed, unless otherwise presented, that the nation's adversaries had no specific, factual, knowledge of the information gathered in this qualitative case study before its release by Mr. Snowden to the media.

Limitations

The limitations in this study revolved around access to, and handling, of the released information. The volume of information released by Mr. Snowden was vast, some 1.7 million documents, and highly classified (Johnson, 2014). That the media possessed this information and was releasing a portion did not declassify the information in the eyes of government. This single case study would access only a portion of those documents released by the press and other media outlets to present sufficient case documentation to answer the research questions. Due to the sensitive and still classified nature of the documents, the information was presented in a sanitized form, with identifying information removed and intelligence operation, source, or method generalized. As the information gathered was still classified, there was a duty to protect it beyond any vetting by media. A case study using archival records would be difficult due to factors including the authenticity of the archival record, the systematic collection methodology of the archival records, and the possibility of deception in order to hide levels of potential government impropriety and malfeasance (Stan, 2010). These potential limitations were mitigated due to the fact that the primary data released to and published by the press, were collected before government had the opportunity to redact information related to intelligence sources, methods, capabilities, liaisons and location accesses or modify any other content.

Delimitations

Given the large population of documents released by Mr. Snowden, the choice of examining only enough documents for single case study documentation that significantly compromised national security represented a means to manage a potentially overwhelming amount of data. Further this single study focused on a single case, the impact of the Snowden leaks, enabling the researcher to provide a more intensive, in-depth analysis than would have been possible with a multiple-case study. However, the researcher acknowledges there may well be further intelligence compromises from released documents outside of the focus of this study. Lastly, the Snowden case was selected over other cases because it represented an event in this current decade (2010-2020) of enormous magnitude in terms of the numbers of documents released that have and may continue to compromise U.S. security.

Ethical Assurances

Northcentral University's Institutional Review Board approval was obtained prior to any data collection. As the information gathered consisted of online archived documents, informed consent documents were not necessary. No data were gathered that was not already in the public domain. Given the classified nature of the information to be gathered and interpretation and publication by the press it was not anticipated that additional risk or harm will be incurred by the public.

Information gathered for this qualitative single case study was maintained in a new personal laptop computer. This computer was password protected, and files contained therein were encrypted and password protected. The computer was air-gapped, with no wires connecting to existing computer hardware. The computer and information

used in the research will be retained for 7 years to satisfy NCU IRB guidelines for retaining data. After the 7 years, the computer and its contents will be rendered inoperative, unrecognizable, and unrecoverable by any and all means currently available.

Summary

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. This method was appropriate as a research design to answer the research question and sub-questions because of the lack of a concrete understanding of the phenomenon, the lack of scholarly examination of the phenomenon vis-à-vis its impact, and the contemporary nature of the topic (Yin, 2014).

The sample for this study was the leaked, classified intelligence information from Edward Snowden, published by the press that significantly compromised national security and included, but was not limited to, revealing intelligence sources, methods, capabilities, liaisons and accesses to territories essential for U.S. national security. This sample was from an overall study population of the unauthorized documents disclosed to the media by Edward Snowden. These documents, according to published accounts, numbered in excess of 1.7 million (Johnson, 2014).

Primary data, the original leaked classified documents and the media reporting thereof, was collected from reputable online databases. These data included records and quotes to document the national security ramifications of publishing classified intelligence information leaked to the media (Patton, 2002). This data were supplemented

with the leaked source documents collected from relevant online websites. Secondary data in the form of intelligence experts' assessments were collected through the same databases as the primary data as well as queries of archival databases (Yin, 2012, 2014).

Processing included compiling and coding using a QSR International NVivo database built for the data. Compilation and coding were interlaced with government assessments as to damages affecting U.S. intelligence activities and U.S. national security as a whole. Court records and first person accounts of the impacts to U.S. intelligence were collected, if they were available, and applied the same process.

Analysis of the archival data included the building of matrices in which to categorically place the gathered evidence (Yin, 2014). The leaked documents were examined using government assessments as to damages affecting U.S. intelligence activities and U.S. national security as a whole (Yin, 2014). Similarly, court records and first person accounts of the impacts to U.S. intelligence were incorporated into the analysis. Finally, the analysis of the data would create generalizations to be used to answer the research questions (Yin, 2014).

Chapter 4: Findings

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. A single-case, holistic case study was appropriate as a research design to answer the research question and sub-questions. Reasons included the lack of a concrete understanding of the phenomenon, the lack of scholarly examination of the phenomenon vis-à-vis its impact, and the contemporary nature of the topic (Yin, 2014). This chapter presents the results of the data analysis and evaluations of the findings and concludes with a summary of the chapter.

Results

Initially, 8,542 published documents were examined relating to the Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press and its subsequent publication. The published documents reporting the classified intelligence information leaked by Mr. Snowden were acquired online from queries of the Lexis/Nexis database. The classified intelligence documents were retrieved online from the Snowden Surveillance Archive at the University of Toronto. An example of the data analysis process is illustrated (Figure 1).

<p>Leaked PowerPoint document from NSA. Source: Follorou & Greenwald, Le Monde, October 21, 2013</p> <p>PP Title: FRANCE - Last 30 Days. PowerPoint slide showing number and types of calls intercepted in France.</p> <p>Classification Unknown</p>	<p>News Article. Source: Gearan, The Washington Post, October 22, 2013</p> <p>A report Monday that the National Security Agency vacuumed up more than 70 million French phone records in one month left the Obama administration scrambling once again to explain spy practices that have angered allies and dented the United States' reputation overseas.</p>	<p>Impact on intelligence operations. Source: Gearan, The Washington Post, October 22, 2013</p> <p>A series of disclosures in the media, based on documents provided by former NSA contractor Edward Snowden, also have angered Brazil, Germany and Mexico, among other countries. Brazil canceled a visit by President Dilma Rousseff to the White House in protest of NSA electronic espionage targeting that country. It is not clear whether France intends to take any punitive action. French prosecutors already had opened a preliminary inquiry into one of the NSA's collection programs, known as Prism... In Washington, State Department spokeswoman Marie Harf acknowledged the outcry... Harf was asked whether the latest revelations would damage the United States' working relationship with France. "We certainly hope that it doesn't," she said.</p>
--	---	--

Figure 1: This figure illustrates the data triangulation analysis process of aligning each leak to published articles to the impact on U.S. intelligence which produced the themes for each sub-question.

Document Demographics. Table 1 illustrates the sources of the 8,542 news articles that spanned the timeframe June 6, 2013 through June 15, 2015. These published

articles originated from 524 classified intelligence documents spanning a date range from November 1, 2001 to May 2013 leaked by Mr. Snowden.

Table 1

Number of News Articles as Analyzed Per Newspaper Source

Source	Number of news articles
1. The Guardian	3,045
2. New York Times	1,341
3. Washington Post	4,156
Total Documents	8,542

The leaked intelligence documents ranged in classification levels from unclassified at the low level to exceptionally classified information, a level on the classification hierarchy higher than top secret, as defined in Table 2. The originating agencies' authors of the classified intelligence leaked by Mr. Snowden are presented in Table 3 and cross referenced by document classification.

Table 2

U.S. Intelligence Documents, Lowest to Highest Intelligence Classification

Document Classification	Definition
Unclassified (U)	Documents or portions of documents not containing classified information (Author definition).
Confidential (C)	“...information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe” (U.S. White House, 2009).
Secret (S)	“...information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe” (U.S. White House, 2009).
Top Secret (TS)	“...information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe” (U.S. White House, 2009).
Exceptionally Classified Information (ECI)	“...a classification above TOP Secret” (Schneier, 2014).

Table 3

Originating Agency, Number of Leaked Documents and Intelligence Classification

Intelligence Agency	C	U	S	TS	ECI	Other	Total
U.S. National Security Agency (NSA)	38	4	46	221	15	27	351
U.K. Government Communications Headquarters (GCHQ)	0	1	14	53	0	28	96
Canadian Communications Security Establishment (CSE)	1	0	0	14	0	2	17
Australian Defense Signals Directorate (DSD)	0	0	1	2	0	0	3
U.S. Central Intelligence Agency (NSA)	0	0	6	2	0	0	8
Other	3	0	17	14	0	15	49
Total	42	5	84	306	15	72	524

Note: A small number of documents, n=72, lack a classification designation. However, they were included in the analysis; as per to the researcher’s professional expertise, they contained classified information.

Q1. What are the impacts on U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press? Four sub questions pertaining to specific U.S. national security topics (impacts on U.S. intelligence sources and methods, revealed capabilities previously unknown to adversaries, revealed liaisons and access to territories in which to conduct intelligence activities, and other impacts, unknown) were asked to answer the main research question. According to press reports, Mr. Edward Snowden stole about 1.7 million documents from classified government computer systems relating to intelligence collection and associated programs conducted by U.S. and allied agencies (Appendix A: 1). He gave these documents to Mr. Glenn Greenwald, a U.S. citizen, living in Brazil and reporting initially for the British newspaper, The Guardian. He also gave the documents to documentary filmmaker Ms. Laura Poitras and Mr. Barton Gellman of the Washington Post (Appendix A: 2). These individuals, at a minimum, began publication of the information to a worldwide audience. The Guardian, when nearly forced to hand the documents back to their original owners, the intelligence agencies, shared the information with the New York Times which, in turn, began publication (Appendix A: 3).

News articles based on the leaked documents revealed significant information about proactive computer network initiatives in support of the U.S. and allied signals intelligence efforts of which the resulting themes that emerged from answers to each of the sub questions will be documented in this section. Significant to the research were the actual classified intelligence documents accompanying many of the news articles.

SQ1. What are the impacts on U.S. intelligence sources and methods? Four themes emerged from the data analysis. As shown in Table 4, three columns illustrate: 1)

the number of actual leaked documents supplementing the reported information, 2) the information reported, and, 3) the assessments and analysis of experts.

Table 4

Themes from Findings, SQ1: Impacts on U.S. Intelligence Sources and Methods

Theme	# of Leaked Documents / # of Intelligence References from Those Docs	# of Published References to Theme	# of Published Impact References/ Example of Impact Published
1. Computer network exploitation and attack methods revealed.	47/78	13	29/ Example: "A former senior U.S. official said that the material that has leaked publicly would be of limited use to China or Russia but that if Snowden also stole files that outline U.S. cyber-penetration efforts, the damage of any disclosure would be multiplied. The official, like others in this article, spoke on the condition of anonymity..." (Source, Appendix A: 4).
2. Signals intelligence (SIGINT) methods revealed.	49/56	33	34/ Example: "...there has been a "sharp drop in terrorists' use of a major communications channel" after the US press revealed American spies had intercepted messages between two senior al-Qaida commanders in the Middle East." (Source, Appendix A: 5).
3. SIGINT locations and types of facilities and sources were revealed.	31/39	31	34/ Example: "...compromise of their identities would "result in danger to the persons concerned or their close associates ... this danger includes a risk to life, both to intelligence officers and their families." (Source, Appendix A: 6).
4. Identities of SIGINT targets were revealed.	9/11	13	20/ Example: "...so that it can obtain contact details of foreign leaders for its surveillance systems. The revelation adds to diplomatic tensions between the US and its allies..." (Source, Appendix A: 7).

Theme 1: Computer Network Exploitation and Attack Methods Revealed. In addition to the example listed in the table, other reported impacts of computer network methods revealed, included published budget allocations and goals for cyber operations supporting signals intelligence. These included witting and unwitting relationships with U.S. internet service providers (ISP) and methods to exact information from these ISPs to further national intelligence collection objectives (Appendix A: 8). Efforts to infiltrate the internet's data stream were published to include exact methods and results of those methods (Appendix A: 9 & 10). Finally, efforts to modify cellular networks to facilitate signals intelligence collection were published (Appendix A: 11).

The leaked documents augmented many of the news articles relating to cyber operations supporting signals intelligence objectives reported by the press. Relating to cyber sources and methods, these documents revealed classified methods to infiltrate networks for passive signals intelligence collection (Appendix A: 12). Data were presented that “millions of webcam images” were being collected from “innocent Yahoo users” and that networks were hacked to access “worldwide mobile phone communications” (Appendix A: 13 & 14). Information on more than 61,000 CNA operations and over 21,000 computer network implants were revealed, as were CIA efforts to conduct adversary network penetration (Appendix A: 15 & 16). Budgets and expansion plans for these operations were disclosed (Appendix A: 17). Similarly, proactive signals intelligence collection methods were divulged, including documents detailing hardware, software, and firmware modifications available and in use to further intelligence collection objectives (Appendix A: 18). The methods to implant or deliver the modifications were published, as were the means to collect, process, and report the

intelligence once modifications were in place (Appendix A: 19 & 20). Many of the points discussed above were published in the form of a catalog detailing significant numbers of existing methods and sources relating to Computer Network Attack and Computer Network Exploitation (Appendix A: 21).

Theme 2. Signals Intelligence (SIGINT) methods revealed. The second emergent theme centered on U.S. and allied intelligence methods relating to signals intelligence. Press reporting of U.S and allied signals intelligence methods centered on access to telephone metadata and volumes of data gathered through “cable taps” (Appendix A: 22). The metadata program was of particular concern to reporters due to not only its scope but its expanding nature (Appendix A: 23). Privacy experts interviewed for their stories categorized this signals intelligence activity as illegal (Appendix A: 24). Similar stories relating to illegality were reported, indicating that there were “a number” of instances where U.S. intelligence analysts purposefully ignored existing privacy protections for U.S. person’s data (Appendix A: 25).

Active involvement by U.S. telecommunications companies to assist U.S. and allied signals intelligence efforts were another area of concentration by the press, with specific focus on U.S. companies being compelled by court order to turn over metadata for analysis (Appendix A: 26). Similar levels of focus were on the collaboration between the CIA and NSA in using signals intelligence data for anti-terrorist targeting in the allied drone campaign (Appendix A: 27).

By far, the leading topic relating to signals intelligence methods reported by the press due to Mr. Snowden’s leaks centered on surveillance of Americans (Appendix A: 28). The press reported on “surveillance programs that sweep up telephone call data from

millions of U.S. citizens as well as internet traffic” and that NSA was building a computer to break the encryption of “banking, medical, business and government records around the world” (Appendix A: 29 & 33). Additionally, the press revealed that, over a span of a given year, government searched for less than 300 phone records in their database containing tens of millions of phone records. These records, it was reminded, required orders from a surveillance court in which government shouldered the burden of proof that the records were germane to a foreign terrorist investigation (Appendix A: 31).

The actual leaked documents from Mr. Snowden accompanied many of the press revelations of signals intelligence methods reported above. Specific to these documents were procedures and methods to perform signals intelligence collection and included procedures for target discovery, target selection, and target development (Appendix A: 32 & 33). Documents relating to the processing and decryption of these signals were divulged by the press including knowledge of specific data points where NSA had achieved cryptologic successes (Appendix A: 34 & 35). Through publication of the actual classified documents, data storage and retention systems, procedures, and policies were revealed (Appendix A: 36).

Extensive documentation supporting government efforts to establish reasonable suspicion that an emitter – a communications link – was not a U.S. person was published (Appendix A: 37). Significant was the emphasis on commencing collection on a target when that target was known to be of foreign origin and that if a communicant was subsequently categorized as a U.S. person then collection would cease immediately (Appendix A: 38 & 39).

Theme 3. SIGINT locations and types of facilities and sources were revealed. The third theme emerging from the data in response to the sub-question concerned the revelation of locations and types of intelligence facilities and sources of U.S. and allied signals intelligence. Press reporting of the leaked classified intelligence information revealed signals intelligence collection sites in a vast number of countries and, in a number of references, the amount of data they were collecting and intelligence successes achieved (Appendix A: 40). Locations of cyber penetration were provided in the press reports, listing the physical location of the surveillance device and the system affected (Appendix A: 41, 42 & 43). Location of conventional signals intelligence facilities were divulged and were associated with a number of programs and sources (Appendix A: 44). Press reporting provided information relating to physical access to signals intelligence sources such as cables and commercial internet companies (Appendix A: 45). Details reported included whether the internet companies were witting of being used as an intelligence source and exact types of data that were sought (Appendix A: 46).

Actual documents accompanying the press reporting contained details on intelligence collection sites belonging to the United States, United Kingdom, Germany, Australia, and New Zealand (Appendix A: 47, 48, 49 & 50). Significant detail was provided on signals intelligence sources in numerous other nations (Appendix A: 51). Many of these references provided details as to the specific city in which the collection operation was based and the collection programs to which these sites contributed (Appendix A: 52). Published leaked documents provided exact locations and labels of cable entry points in which collection activity was being conducted (Appendix A: 53).

Theme 4. Identities of SIGINT targets were revealed. The revelation of the identities of U.S. and allied intelligence targets constitutes the fourth and final theme relating to the sub-question. Press reporting of the information leaked by Mr. Snowden indicated a large number of nations, their communications systems and subsystems as the targets of U.S. and allied signals intelligence collection (Appendix A: 54, 55 & 56). Press reporting was triangulated in the public eye with the actual leaked and published documents discussing details of foreign leaders and staff, by name, targeted for collection (Appendix A: 57). Specific communications systems within nations and exact methods of collection were revealed (Appendix A: 58 & 59).

SQ2. What are the impacts on U.S. intelligence if capabilities were revealed that were previously unknown to adversaries? Three themes emerged from the data analysis. As in SQ1, Table 5's three number columns illustrate: 1) the number of actual leaked documents supplementing the published information, 2) the information reported, and, 3) the impact assessments and analysis of experts.

Table 5

Themes from Findings, SQ2: Impacts on U.S. Intelligence Capabilities

Theme	# of Leaked Documents /# of Intelligence References from Those Docs	# of Published References to Theme	# of Reported Impact References and Examples of Impact Published
1. Computer network attack and exploitation capabilities revealed.	60/171	2	2/ Example: "The reaction of the tech industry to Snowden has been helpful," says Anderson, who also describes Google's engineers as "hitting the roof" at some of the Snowden revelations of backdoor access by the NSA." (Source, Appendix A: 60)
2. Depth and breadth of capabilities of SIGINT activities revealed.	63/85	6	19/ Example: "'By speculating about our capabilities, it makes it easier for people who want to evade interception but are seeking to damage our country, or kill people, it makes it easier for them to evade interception. That is something that is very, very serious, and very damaging.'" (Source, Appendix A: 61)
3. Cryptologic capabilities and successes revealed.	22/45	2	3/ Example: "The Islamic State has also studied revelations from Edward J. Snowden, the former National Security Agency contractor, about how the United States gathers information on militants. A main result is that the group's top leaders now use couriers or encrypted channels that Western analysts cannot crack to communicate, intelligence and military officials said." (Source, Appendix A: 62)

Theme 1: Computer network attack and exploitation capabilities revealed. Press reporting of Computer Network Attack (CNA)/Computer Network Exploitation

(CNE)/Computer Network Information Operations (CNIO) data indicated relationships between Britain's GCHQ and major internet service providers and search engine entities (Appendix A: 63). Der Spiegel, in extensive reporting, revealed the existence of a minimum of 81 highly classified programs at the National Security Agency relating to this theme (Appendix A: 64). Reporter Glenn Greenwald, through his website *The Intercept*, revealed the existence and details of a minimum of 136 programs tied to the cyber warfare theme conducted by GCHQ (Appendix A: 65). Along with the press reporting, the actual documents on which the reporting was based were released by *der Spiegel*, *The Intercept* and *The Guardian*. These documents provided extensive details as to systems targeted, levels of entry into a computer system, and persistence of CNA weapons (Appendix A: 63, 64 & 65).

Theme 2. Depth and breadth of capabilities of SIGINT activities revealed.

Volumes of information collected comprised the second theme associated with revelation of U.S. intelligence capabilities. Press reporting, in general, concentrated on manning and facility size when reporting on U.S. and allied SIGINT capabilities (Appendix A: 66). Aligned with this reporting were revelations, through the publication of the actual leaked documents, of significant capabilities to intercept tens, and as much as hundreds, of millions of messages daily (Appendix A: 67 & 68). U.S. and allied capabilities to process and manage that much data were similarly published (Appendix A: 69). Finally, the breadth of targeted communications systems and sub-systems were revealed (Appendix A: 70).

Theme 3. Cryptologic capabilities and successes revealed. Capabilities related to encryption and decryption efforts constitutes the final theme. Press reporting based on the

leaked Snowden documents revealed that “US and British intelligence agencies ha[d] successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails” (Appendix A: 71). Specifically, GCHQ was reported as targeting encrypted traffic on internet service providers Hotmail, Google, Yahoo and Facebook. The leaked actual documents published revealed specific decryption efforts and specific systems to which those efforts were targeted (Appendix A: 72).

SQ3. What are the impacts on U.S. intelligence if liaisons and access to territories in which to conduct intelligence activities were revealed? Two broad themes emerged from the data analysis. Table 6’s three number columns illustrate: 1) the number of actual leaked documents supplementing the reported information, 2) the information reported, and, 3) the impact assessments and analysis of experts.

Table 6

Themes from Findings, SQ3: Impacts on U.S. Liaisons and Accesses

Theme	# of Leaked Documents / # of Intelligence References from Those Docs	# of Published References to Theme	# of Reported Impact References and Examples of Impact, Published
1. Depth and breadth of inter and intra relationships, accesses and liaisons between the U.S. and its allied intelligence communities	89/111	9	5/ Example: “Ministerial claims that the publication of reports based on NSA and GCHQ documentation undermined national security prompted a scathing response from United Nations experts on freedom of expression and human rights.” “Cooperation between the two countries' spy services "is deeper than previously believed," as Der Spiegel put it. The United States and Germany are now attempting to rebuild the partnership...” (Source, Appendix A: 73 & 74)
2. International backlash resulting from U.S. intelligence accesses and liaisons being revealed.	0/0	97	143/ Example: “Indonesia has recalled its ambassador to Australia and is reviewing all co-operation with the country after revelations that Australian spy agencies attempted to listen in to the phone calls of the Indonesian president and his inner circle.” (Source, Appendix A: 75)

Theme 1: Intelligence Relationships, Liaisons and Accesses. Intelligence relationships – both internally and externally to the United States – were reported. Internally, actual leaked documents published as supplements to news stories revealed the depth and breadth of relationships between the signals intelligence agencies and their counterparts in other intelligence disciplines (Appendix A: 76). Included were the relationships and successes between the National Security Agency and the Central

Intelligence Agency, The Defense Intelligence Agency, the Federal Bureau of Investigation, and the Drug Enforcement Agency (Appendix A: 77 & 78). Externally, intelligence collection relationships were reported with a minimum of 41 nations (Appendix A: 79). Within the context of these relationships, actual documents published revealed the robustness of the intelligence relationship, the contribution each relationship made to the overall intelligence picture, the targets covered or assigned as part of the intelligence enterprise, and the locations of a number of intelligence collection sites (Appendix A: 80 & 81). Similarly, the importance that the U.S. assigns to the liaisons was discussed in depth (Appendix A: 82 & 83). Many of these relationships were sensitive due to neutralities or other issues such as nations that were traditionally each other's adversaries (Appendix A: 84). The press reported that NSA was monitoring the phone conversations of at least 35 world leaders, some of which were established intelligence sharing partners (Appendix A: 85). The named leaders included the German Chancellor and Brazilian President (Appendix A: 86 & 87).

Theme 2. Intelligence Repercussions. Press reported the depth and breadth of relationships between signals intelligence agencies and a number of private companies. Reporting included assertions that private telecommunications firms were, themselves, conducting monitoring on behalf of the signals intelligence agencies (Appendix A: 88). According to press reporting, private telecommunications and internet companies have suffered consumer backlashes (Appendix A: 89). The publication of the Snowden documents opened a reexamination of the relationship between technology and telephone companies, the government and the consumer, raising “the issue of digital human rights

and how to control a covert surveillance state. It has made the internet potentially unstable...” (Appendix A: 90).

SQ4. What emerged as other impacts on U.S. national security from Snowden’s unauthorized disclosure of classified intelligence information to the press? One theme emerged from the data analysis of SQ4 related to the impact seen as reported by media and experts, respectively. Table 7’s three number columns illustrate: 1) the number of actual leaked documents supplementing the reported information, 2) the information reported, and, 3) the impact assessments and analysis of experts.

Table 7

Theme from Findings, SQ4: Other Impacts

Theme	# of Leaked Documents / # of Intelligence References from Those Docs	# of Published References to Theme	# of Reported Impact References and Examples of Impact Published
1. The role of secrecy and the press.	96/134	46	63/ Example: “...there has been a "sharp drop in terrorists' use of a major communications channel" after the US press revealed American spies had intercepted messages between two senior al-Qaida commanders in the Middle East.” (Source, Appendix A: 91)

Theme 1: The role of secrecy and the press in press reporting. The press reported the activities of British intelligence agencies as illegal (Appendix A: 92 & 93). Press reporting evaluated intelligence agencies, the laws governing them, and mass surveillance as requiring an overhaul so as to be more accountable to the people they serve (Appendix A: 94, 95, 96 & 97). Key to this argument was that a leak of Snowden’s caliber required a

different style of reporting to deal with the sheer volume (Appendix A: 98). Secrecy, as evaluated by the press, was dismissed as ineffective because those with similar security clearances and access to Snowden numbered nearly half a million persons (Appendix A: 98). Questioned was whether a piece of information known by that many people was really a secret at all (Appendix A: 99). Similarly, the press questioned whether, after the leak, the information leaked was still classified (Appendix A: 100).

Evaluation of Findings

The main research question--what are the impacts on U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press--utilized four sub questions to guide data collection and analysis. The evaluation of findings that answered the sub-questions, are discussed in this section. The study topics pertaining to specific U.S. national security topics are: impacts on U.S. intelligence sources and methods, revealed capabilities previously unknown to adversaries, revealed liaisons and access to territories in which to conduct intelligence activities, and other impacts, unknown. Specific to the research was an overwhelming lack of government officials discussing, or willing to discuss, the specifics of the Snowden revelations and their subsequent publication in other than a very generic sense. Details related to damages that the publication of the Snowden leaks may have caused are, largely, dependent on the assumption that an adversary, if having a knowledge that U.S. and allied intelligence services were monitoring their communications, knew so, in the most basic of senses.

Impacts on U.S. intelligence sources and methods (SQ1). Findings discussed in the results section included thirteen published newspaper articles and a catalog cited as

specific findings of Theme 1, Computer Network Exploitation and Attack Methods Revealed (Appendix A, 4; 8-21). The Director of GCHQ, Sir Iain Lobban, in considering the technological challenges that his agency – and by default, NSA – faces, said, “Our challenges come from the explosion in the volume of communications as well as the relentless increase in new ways of accessing and processing that volume...today, the challenge can simply be to cope with the number of different communications options” (Hopkins, 2013c). Christopher Soghoian, principal technologist and senior policy analyst at the American Civil Liberties Union assessed that NSA manipulation of encryption algorithms were “fundamentally in conflict with good security” (Guardian, 2013b; Hopkins, 2013c).

Concerns arose from privacy advocates, specifically Privacy International, relating to NSA’s and allied abilities to surveil internet and mobile phone networks and to defeat and control international encryption standards. The press included these privacy advocates in their expert pool, keying on their assessment of government cyber efforts in support of intelligence collection objectives as illegal (Boycott, 2014). Implications by Mr. Snowden were that NSA “could tap into any American’s communications” (Cole, 2014). However, in a juxtaposition worth noting, one former U.S. official, as reported by Nakashima and Miller (2013), downplayed damages caused by the publication of this leaked information, but warned that if adversaries had the actual files, damages would be multiplied.

For Theme 2, Signals Intelligence Methods Revealed, 33 published newspaper articles were cited as findings of compromised U.S. Signals Intelligence (Appendix A, 5; 22-39). Expert assessments of the material leaked by Mr. Snowden and reported by the

press relating to signals intelligence methods centered on adversary reactions and legalities (Booth 2013; Hopkins, 2013b). Oliver Robbins, deputy national security adviser in the U.K. Cabinet Office argued that the published revelations of tradecraft, methods, and methodologies were valuable to adversaries and could risk U.S. and foreign intelligence lives (Booth, 2013). Dr. Bruce Schneier noted that there had been a “sharp drop in terrorists’ use of a major communication channel” following press reporting of the leaked information (Hopkins, 2013b). Similarly, Admiral Michael Rogers, Director of the National Security Agency, reported that terrorists had been overheard making references to the reported information (MacAskill, 2014).

However, debate sparked as a result of the revelations and reporting specific to signals intelligence methods center on proprieties of digital data (Guardian, 2013b). Much of the reporting keyed on the volume and type of information being collected as well as the disposition of that material. Interestingly, press reporting also indicated that some U.S. companies have lost business as result of the revelations that intelligence agencies had access to and were exploiting their digital infrastructure (Liacas, 2015).

Relating to SIGINT locations and types of facilities and sources revealed, Theme 3 was derived from 31 published newspaper articles cited as findings of compromised U.S. Signals Intelligence (Appendix A, 6; 40-53). Government hearings in both the United States and the United Kingdom, had called into question their respective intelligence agencies sources and methods resulting from the leaks and their publications (Mason, 2013; Nakashima, 2013c). Revelations of locational data on signals intelligence collection facilities and source information were assessed, in testimony from Oliver Robbins, U.K. Cabinet Office deputy national security adviser, as a significant

intelligence breach that now compromises staff safety (Booth, 2013; Halliday, 2013). These assertions, at times, were challenged as lacking credibility on the basis that government was unable or unwilling to provide classified details of the damages in open court (Booth, 2013). Additional impacts or damages were assessed by the press as to the credibility of technology sector companies for allowing access to their systems from the intelligence agencies (Liacas, 2015).

Thirteen articles contributed to Theme 4, revelations concerning the identities of SIGINT targets (Appendix A: 7; 54-59). An unnamed U.S. congressional aide assessed the press revelation of SIGINT targets as potentially affecting the U.S. by “losing collection, but also of harming relationships” (Nakashima, 2013b). These relationships were addressed by the White House Press Secretary, including "some of the very specific things with regard to intelligence gathered, including matters that deal with heads of states and other governments" (Lewis, 2013a). The reported impact of these disclosures, at a minimum, included a call for a European Union-wide privacy law in order to restore “trust in the digital economy”, according to the British Information Commissioner (Travis, 2013).

Impacts on U.S. intelligence if capabilities were revealed that were previously unknown to adversaries (SQ2). Findings discussed in the results section included two published newspaper articles cited as specific findings of Theme 1, Computer Network Attack and Exploitation Capabilities Revealed (Appendix A: 60; 63-65). Press reporting of Computer Network Attack (CNA)/Computer Network Exploitation (CNE)/Computer Network Information Operations (CNIO) capabilities were scantily covered, but included anger from entities at Google and Yahoo when accesses to their systems were revealed

(Dredge, 2014). Government reaction abroad was predictable, the German Justice Minister equating some intelligence practices to their Cold War equivalents (MacAskill, 2013a). A senior British official within the European commission countered the German reaction, alleging that EU negotiators always assumed that their communications were being monitored (Traynor, 2013b).

For Theme 2, given the depth and breadth of capabilities of SIGINT activities that were revealed, six articles were germane (Appendix A: 61; 66-70). Expert assessments published, specifically a report originated in the U.S. Department of Defense, categorized the damage associated with the Snowden leak on U.S. intelligence capabilities as “staggering” and the greatest damage that has ever been suffered to U.S. and allied intelligence collection systems (Leopold, 2014). U.S. intelligence agencies noted drops in terrorist uses of communications channels and conversations directly referencing the leaked Snowden documents (Hopkins, 2013b). Balancing this view was that of a former member of the British Intelligence organization, MI-6, who “sense[d] that those most interested in the activities of the NSA and GCHQ have not been told very much they didn't know already or could have inferred.” The same official continued, saying that, “Al-Qaida leaders in the tribal areas of Pakistan had been "in the dark" for some time - in the sense that they had not used any form of electronic media that would "illuminate" their whereabouts” and that “other "serious actors" were equally aware of the risks to their security from NSA and GCHQ eavesdroppers.” This official further surmised that “the reality was that any government with a national communications system also had a national signal intelligence capability” (Norton-Taylor & Rushe, 2013).

For Theme 3, Cryptologic Capabilities and Successes Revealed, two published newspaper articles were cited as findings of compromised capabilities (Appendix A, 62; 71-73). Expert assessments relating to these revelations centered around the capability to decrypt commercial codes and the impact on privacy of business transactions. The U.K. information commissioner empaneled a group of experts in academia and industry, chaired by the information commission's policy adviser on technology, to examine privacy issues as a result of the Snowden documents' publication. At question was the ability to crack commercial encryption codes, specifically credit card transactions and commercial banking, the impact of which was assessed as intrusive and as destroying the public trust in digital transactions (Travis, 2013). Intelligence agencies asked the press to refrain from publishing articles on cryptologic capabilities because adversaries could modify their encryption or communications, increasing collection and exploitation difficulty. (Ball, Borger & Greenwald, 2013). Not surprisingly, intelligence officials also confessed that the Islamic State (IS) had studied the published Snowden information, specifically how the United States gathers information on militants, with the result being that IS leaders now use couriers or encrypted channels to communicate that cannot be decrypted (Schmitt & Hubbard, 2015).

Impacts on U.S. intelligence when liaisons and access to territories in which to conduct intelligence activities were revealed (SQ3). Nine published newspaper articles are cited as specific findings of Theme 1, discussing the depth and breadth of inter and intra relationships, accesses and liaisons between the U.S. and its allied intelligence communities (Appendix A: 73 & 74; 76-87). Capitals throughout Europe insisted that Washington account for the disclosures on the scale of spying on its allies.

German and French leaders were to undertake efforts to instill rules on spying within Europe (Traynor, 2013a). There were calls from ministers within the European Parliament for the president of the European council and the president of the European commission to explain what steps they were taking in response to the leaked and published intelligence documents. A former Belgian prime minister stated: "This is absolutely unacceptable and must be stopped immediately. The American data collection mania has achieved another quality by spying on EU officials and their meetings. Our trust is at stake". A similar call echoed from Luxembourg's Foreign Minister. The European parliament demanded information-sharing between the EU and the US aimed at tracking terrorism funding be stopped (Traynor, 2013b). Behind the scenes in Europe calls for change were reluctant, at best, probably due to the revelation that at least six European member states, the UK, Denmark, the Netherlands, France, Germany, Spain, and Italy have shared, through formal agreements, personal communications data with NSA and that, as press has reported, many of these nations had "well-developed electronic intelligence capabilities of their own" (Traynor, 2013b).

Ninety-seven articles contributed to Theme 2 relating to the international backlash resulting from U.S. intelligence accesses and liaisons being revealed (Appendix A: 75; 88-90). U.S. relations with France were affected by the revelations that included a popular backlash against the U.S. and the summoning of the U.S. ambassador to France to answer questions relating to the reported "widespread phone and internet surveillance of French citizens" (Chrisafis & Lewis, 2013; Washington Post, 2013a). A similar diplomatic summoning occurred in Spain, where not only was the ambassador called to answer questions but ordered to bring with him all information regarding intelligence

monitoring activities against Spain (Lewis, 2013b). Turkey, a key U.S. ally, reacted to revelations of GCHQ documents showing the UK had spied on a Turkish delegation, in Britain for G20 meetings in 2009, labeling the activity as scandalous (Borger, 2013).

Of the reported reactions from leaked, published documents, none perhaps was stronger than that of Germany, which involved face-to-face discussions between the German Chancellor and the American President (Oltermann, 2014). The German federal data protection commissioner considered the fact that U.S. authorities had access to European citizens' data unacceptable "and [that] the level of protection is lower than what is guaranteed for US citizens" (Travis & Roberts, 2013). The German Interior Minister said, "Whoever fears their communication is being intercepted in any way should use services that don't go through American servers" (Greenwald, 2013a). Finally, a German Justice Minister, called for a boycott of US companies (Greenwald, 2013b). The reaction culminated when the German Chancellor expelled the CIA's station chief from the country and implemented intelligence cooperation limits with the U.S. (Guardian, 2014b; Miller & Kirchner, 2014; Smale, 2015).

Relating to South America, the Snowden documents and press reporting thereof revealed the US had monitored Brazilian communications, specifically Brazilian diplomats and companies. The Brazilian President, as a result, cancelled a diplomatic trip to Washington and, instead, denounced US surveillance in front of the UN general assembly (Borger, 2013; MacAskill, 2015). In Bolivia, reaction was as tangible, its President stating, "Those US intelligence agents have accessed the emails of our most senior authorities in Bolivia... It was recommended to me that I not use email, and I've followed suit and shut it down" (Guardian, 2013b). A result of Mr. Snowden's request for

asylum in Ecuador and U.S. pressure against such an act, Ecuador renounced the Andean Trade Promotion and Drug Eradication Act (Carroll & Collyns, 2013). The renunciation revealed divisions within Ecuador's government between leftists who “embraced Snowden as an anti-imperialist symbol and centrists who fear diplomatic and economic damage”. Ecuador continued its defiance by waiving preferential trade rights with the U.S. as Mr. Snowden’s chances for asylum waned (Carroll, 2013).

In Asia, Indonesia specifically, after the Australians were revealed to have monitored the communications of the Indonesian president and his advisors, recalled its ambassador to Australia and reviewed all co-operation with the country (Laughland, 2013). A function of the press reporting of the leaked classified intelligence information, the Obama administration ordered NSA to cease the monitoring of a number of world leaders (Lewis, 2013a).

Other impacts on U.S. national security from Mr. Snowden’s unauthorized disclosure of classified intelligence information to the press (SQ4). Forty-six published newspaper articles were cited as findings which constituted Theme 1, the role of secrecy and the press (Appendix A: 91-100). When the press reported on the impact of the leak, they in general reported on the leak itself, versus the impact of the presses reporting of the leak and their resultant analysis of the data and the mosaic-making efforts (Hopkins, 2013b). This is important because the classified information, when initially leaked, was only given to a few select individuals. These individuals, knowing they had received stolen and – more so – classified intelligence documents chose to broadcast those mosaic-like pieces, in their assembled form, to hundreds of millions of persons under the guise of journalism. Thus, a large share of other impacts reported in this section

center on the press making themselves the news versus the leaked documents (Bell, 2013).

Less accusations of aiding and abetting the enemy, the UK Daily Mail's assessment of the Guardian newspaper's publication of the leaked classified intelligence information, the vast majority of the media's views of publication were supportive (Guardian, 2013c). The media's self-assessment was that of a body that verified and fact-checked their information, was in consultation with their lawyers and government officials regarding security concerns, and that no harm was done in the publication of the Snowden documents (Fahri, 2014; Quinn, 2013). The argument that intelligence professionals knew better what information should be suppressed was dismissed as superficial (Guardian, 2013c). Some experts within the British defense establishment accused the Guardian as producing a handbook for terrorists (Greenslade, 2014). The Guardian's self-assessment of its behavior was remarkable, it noting that at a point it had only published 26 of more than 58,000 documents. Further, The Guardian believed it had saved the intelligence agencies further damage as itself was the target of foreign intelligence services trying to access the leaked documents in their possession (Huppert, 2013). Journalistic paranoia and sense of self-importance extended to fully 2/3s of polled journalists believing that agencies within the U.S. government were specifically monitoring their communications (Dredge, 2015). Similarly, a function of increased whistleblower prosecutions was that select members of the press felt there was a war being waged against journalism (Moss, 2013). Some assessments had gone as far as turning the burden onto NSA for allowing Snowden, a contractor, access to the data in the first place due to inadequate security measures (Norton-Taylor, 2013b).

The New York Times considered the reporting of the information as causing less damage than other historic leaks (Hopkins, 2013b). Other individuals including Daniel Ellsberg, leaker of the Pentagon Papers, labeled the leaks as significant while still others, including anonymous former intelligence officials, assessed the damage as overly exaggerated and symbolic (Norton-Taylor, 2013a; Roberts, 2013). As would be expected, the government invoked “national security” as a method of quashing debate or discussion, while the press was quick to provide their assessment and denunciation of the government (Norton-Taylor & Cobain, 2013).

Among Snowden’s choice of conduit to the public was Glenn Greenwald of the Guardian. Reporter Greenwald, a proponent of “independent adversarial journalism,” initially broke the story in the Guardian and has continued to be lead on much of the coverage (Cardew, 2014). On June 6, 2013 Greenwald, an American living in Brazil and working for a British newspaper, The Guardian, published the first of a number of stories relating to mass collection of communications by NSA (Bell, 2013). Greenwald and a number of other reporters functioned as the “mosaic makers” in assembling and providing their perspective on the leaked information (Pozen, 2005). Press and expert assessments agree that the Snowden documents and their publication have increased public debate on government surveillance and the powers of the state in protecting its citizens (Hopkins, 2013a; Shane, 2013b). They have inspired congressional and parliamentary legislation, investigations, a Presidential review, and a general rethinking of the role of government surveillance agencies, opening a window in which to view these entities (Nyst, 2015).

On whether to label Mr. Snowden as a traitor, leaker, or whistleblower, received significant press. Although seemingly intending to “alert the world to the unprecedented and industrial scale” of espionage, Snowden was assessed by experts as not having the right nor the knowledge to determine what information needed to be in the public domain (Cohen, 2013; Guardian, 2013a). Given that Mr. Snowden leaked classified information about operations relating to Russian and Chinese intelligence targets, but lacked a level of intent, debate on his status is ongoing (Cohen, 2013).

Significant to the whistleblower debate was the fact that most, if not all, government institutions had available to them vehicles by which an employee could discuss a concern or air a grievance. Snowden, apparently, did not utilize these vehicles to their full potential (Gellman, 2013). An important element in the leaker/whistleblower debate was an observation that “one reports a crime; and one commits a crime” (Cohen, 2013). In that sense, Mr. Snowden stole in excess of 1.7 million classified documents relating to sources and methods on allied intelligence collection efforts (Pincus, 2013). These documents included tasking relating to intelligence collection – exactly what allied governments were interested in. This led to espionage charges being levied – specifically violations of the Espionage Act of 1917 – against Mr. Snowden, another much debated issue (Shane, 2013a).

Press reporting characterized the United States as having “the only intelligence services on the planet that are under siege from both its adversaries and from its internal support system, the citizens of the United States” (Rogers, 2013). The National Security Agency was vilified and yet defended in the press. The public was made to believe that “they” were the target of surveillance and not bycatch in the surveillance dragnet, given

technological advances (Greenwald, 2013c). Press reporting indicated that the government was building an intelligence collection apparatus to collect on not only U.S. but all citizens worldwide (Risen & Poitras, 2013). The Big Brother concept was prevalent throughout the data and the implication was that the world power balance was being altered (Greenwald, 2013e). The metadata collection was reported as NSA collecting phone call data on tens of millions of U.S. customers with phone and internet companies complicit in the act and occupied most of the discussion in the U.S. (Nakashima, 2013a). Discussions in Europe centered on the privacy of citizens vis-à-vis bulk data collection (MacAskill & Ball, 2013).

The volume of data collection was characterized as government overreach, lacking oversight, and eroding citizens' privacy (Jarvis, 2013). Much press reporting concentrated on the potential to infringe on the privacy of Americans versus an actual violation of privacy (Nakashima, 2013a). No evidence existed, according to some press estimates, that any laws were violated (Risen & Lichtblau, 2013). While counter accusations arose arguing that other nations possessed similar mass surveillance apparatus the press dismissed these accusations, based on their knowledge of the scope and indiscriminate nature of the surveillance, as baseless (Greenwald, 2013e). The nature of secrets and secrecy was of particular import, with the argument being that American interests were, as Jacob Weisberg of the Slate Group stated, poorly "served by secrecy", a thought closely tied into misjudgment and abuse of power by government and bad policymaking (Guardian, 2013c). NSA was drawn into the conversation, implying that it was listening to every phone call and the government would possibly misuse the information that NSA collected (Guardian, 2013c; Samuelson, 2014).

Summary

A small fraction of the classified intelligence documents that Mr. Edward Snowden leaked to three members of the press – 524 out of over 1.7 million – yielded thousands of published accounts of the intelligence activities of the United States and her allies (Gellman, 2013). Relating to signals intelligence, these published stories revealed, 1) exact methods by which to exploit computer networks, 2) exact targets of intelligence collection efforts, 3) the location of numerous signals intelligence facilities and their targets, 4) the sources and methods reported, 5) the actual capabilities of facilities, 6) the depth and breadth of computer network activities, 7) successes and failures relating to cryptology were revealed, 8) inter- and intra-relationships within the intelligence community, and 9) the depths of relationships, targets, and intelligence successes (Appendix A: 4-7, 60-62, 73-75, 91). Impacts resulting from these revelations were difficult to assess due to government's unwillingness or inability to discuss classified issues in an open forum, the media (Booth, 2013). At a minimum, according to officials, intelligence personnel were placed in danger of compromise, adversaries modified or ceased their traditional methods of communication, and companies that traditionally cooperated with the intelligence services reduced and/or eliminated such cooperation (Booth, 2013; Schmitt & Hubbard, 2015). On the surface, intelligence and diplomatic relationships with long-standing allies were degraded upon revelation of their activities with U.S. and allied intelligence services or revelations that they themselves were the target of U.S. and allied intelligence collection (Leopold, 2014).

Chapter 5: Implications, Recommendations, and Conclusions

The problem addressed in this study was what are the impacts to U.S. intelligence from the unauthorized bulk disclosure of classified intelligence information from Edward Snowden to the press including, but not limited to, revealing intelligence sources and methods, capabilities, loss of intelligence liaisons and accesses to territories essential for U.S. national security (Ross, 2011; Schoenfeld, 2011; Johnson, 2014). An estimated 1.7 million documents were given by Edward Snowden to the Guardian newspaper and other media entities (Heemsbergen, 2013; Lears, 2013; Johnson, 2014). Though most damage assessments were concerned with leaks of single documents or issues (Richelson, 2012), this event represented a paradigm shift, unexplored, and when addressed in this study would contribute to Mosaic Theory (Pozen, 2005; Pozen, 2013). The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. The sample for this study was a selected sample of the leaked, classified intelligence information from Edward Snowden, published by the press. Findings from this study document that specific intelligence information leaked by Snowden, and published by the press significantly compromised national security that included, but was not limited to, revealing intelligence sources, methods, capabilities, liaisons and accesses to territories essential for U.S. national security.

The study was conducted utilizing a single-case, holistic case study method. The single-case, holistic case study was appropriate as a research design due to the lack of a concrete understanding of the phenomenon, the lack of scholarly examination of the phenomenon vis-à-vis its impact, and the contemporary nature of the topic (Yin, 2014). The researcher utilized QSR International's NVivo10 qualitative research software to perform a qualitative data analysis.

The limitations in this study revolved around access to, and handling, of the released information. The volume of information released by Mr. Snowden was vast, some 1.7 million documents, and highly classified (Johnson, 2014). That the media possessed this information and was releasing a portion did not declassify the information in the eyes of government. This single sample includes only a portion of those documents released by the press and other media outlets to document and analyze to answer the research questions. Due to the sensitive and still classified nature of the documents, the information was presented in a sanitized form, with identifying information removed and intelligence operation, source, or method generalized. As the information gathered was still classified, there was a duty to protect it beyond any vetting by media. A case study using archival records would be difficult due to factors including the authenticity of the archival record, the systematic collection methodology of the archival records, and the possibility of deception in order to hide levels of potential government impropriety and malfeasance (Stan, 2010). These potential limitations were mitigated due to the fact that the primary data released to and published by the press, were collected before government had the opportunity to redact information related to intelligence sources, methods, capabilities, liaisons and location accesses or modify any other content.

Northcentral University's Institutional Review Board approval was obtained prior to any data collection. As the information gathered consisted of online archived documents, informed consent documents were not necessary. No data were gathered that was not already in the public domain. Given the classified nature of the information to be gathered and interpretation and publication by the press it was not anticipated that additional risk or harm will be incurred by the public.

Information gathered for this qualitative single case study was maintained in a new personal laptop computer. This computer was password protected, and files contained therein were encrypted and password protected. The computer was air-gapped, with no wires connecting to existing computer hardware. The computer and information used in the research will be retained for 7 years to satisfy NCU IRB guidelines for retaining data. After the 7 years, the computer and its contents will be rendered inoperative, unrecognizable, and unrecoverable by any and all means currently available.

This chapter presents the logical conclusions, interpretations, and implications of the data that addressed each research question. Each research question is discussed in context of how the results respond to the study problem and fit with the study purpose. Implications of the study are addressed in light of the findings, evaluation of findings, and the scant existing published literature on the topic presented in Chapter Two. Implications and conclusions also reflect the researcher's over two decades of work experience in the intelligence and national security arena, per the study findings. Based on the results of the study, recommendations for practical application and future, and conclusions are presented.

Implications

Four sub questions pertaining to specific U.S. national security topics (impacts on U.S. intelligence sources and methods, revealed capabilities previously unknown to adversaries, revealed liaisons and access to territories in which to conduct intelligence activities, and other impacts, unknown) were asked to answer the main research question. According to press reports, Mr. Edward Snowden stole about 1.7 million documents from classified government computer systems relating to intelligence collection and associated programs conducted by U.S. and allied agencies (Appendix A: 1). He gave these documents to Mr. Glenn Greenwald, a U.S. citizen, living in Brazil and reporting initially for the British newspaper, *The Guardian*. He also gave the documents to documentary filmmaker Ms. Laura Poitras and Mr. Barton Gellman of the Washington Post (Appendix A: 2). These individuals, at a minimum, began publication of the information to a worldwide audience. The Guardian, when nearly forced to hand the documents back to their original owners, the intelligence agencies, shared the information with the New York Times which, in turn, began publication (Appendix A: 3).

News articles based on the leaked documents revealed significant information about proactive computer network initiatives in support of the U.S. and allied signals intelligence efforts of which the resulting themes that emerged from answers to each of the sub questions will be documented in this section. Significant to the research were the actual classified intelligence documents accompanying many of the news articles.

Impacts on U.S. intelligence sources and methods. Four themes emerged from the data analysis, illustrating: 1) Computer Network Exploitation and Attack Methods, 2) Signals Intelligence (SIGINT) methods, 3) SIGINT locations and types of facilities and

sources, and 4) Identities of SIGINT targets. The researcher expected, when initiating the research, that only a small amount of the actual leaked classified intelligence documents would be published. And then, only in redacted form. Such was not the case with the vast majority of the documents – the pieces of the mosaic – published in their raw and un-redacted form. This phenomenon was prevalent throughout the analysis of the sample.

Computer network exploitation and attack methods revealed. U.S. intelligence budget allocations and goals for cyber operations supporting signals intelligence were published, as were relationships between commercial firms and the intelligence community (Appendix A: 8-17). Much of these relationships concerned exact methods to modify internet and cellular networks to facilitate signals intelligence collection. The implication of this revelation could be the reduction or cessation of existing relationships with commercial firms due to backlash from users and/or customers. This implication has already been realized, as U.S. companies lost customers as result of the revelations that intelligence agencies had access to and were exploiting their digital infrastructure (Liacas, 2015). Similarly, adversaries using given networks will change or cease using these networks, thus rendering intelligence collection against these networks considerable more difficult (Schmitt & Hubbard, 2015).

Published documents also revealed classified methods and expansion aims toward the infiltration of networks for passive signals intelligence collection, much through what is considered to be normal social media (Appendix A: 72). Because proactive signals intelligence collection methods were divulged, including documents detailing hardware, software, and firmware modifications available and in use to further intelligence collection objectives, implications are that adversaries of intelligence targets potentially

can inspect their computers so as to seek out and either remove or replace systems compromised. This, like other implications that seem prevalent in this text, would deny U.S. and allied intelligence collection on targets of interest. In Chapter Four, Nakashima and Miller (2013) quoted a former U.S. official as downplaying damages caused by the publication of Snowden's leaks, but warned that if adversaries had the actual files, damages would be multiplied. Adversaries, through the press, now have detailed files that can be interpreted by their experts so as to develop countermeasures to thwart U.S. and allied intelligence collection (Hopkins, 2013b).

Signals Intelligence (SIGINT) methods revealed. The press reported that U.S and allied signals intelligence methods revealed sources by which intelligence was gathered. Reporting also revealed procedures and methods for signals intelligence collection including target discovery, selection, development, and cryptologic success points. Implications from these findings include the cessation of adversaries to communicate along these channels or, should they choose to continue communicating along established paths, to insert deceptive information into those paths so as to mislead, gauge the level of U.S. and allied monitoring, and response (Hopkins, 2013b).

Although establishing reasonable suspicion that an emitter – a communications link – was not a U.S. person was reported, the reporting leaned toward the assumption that the signals intelligence agencies were targeting Americans (Appendix A: 28 & 37). Privacy experts categorized signals intelligence, based on the reporting, as illegal as did others when alleging willful violation of existing privacy laws. The implication of privacy experts and others alleging illegality created a level of paranoia and anger toward

the intelligence communities working on behalf of citizen safety (Borger, 2013; Dredge, 2014).

As in the cyber theme above, the press reported on active involvement, court ordered, between U.S. telecommunications companies and the intelligence community (Appendix A: 26). As is the recurring implication in this sub-question, cessation of adversaries to utilize a given communication or introduce misleading information into the link remains threatening. This implication, as others, is being realized as some terrorists have already changed communication paths and others, in communications, have referenced the published information leaked by Mr. Snowden (Appendix A: 61 & 62; Hopkins, 2013b; Schneier, 2014).

SIGINT locations and types of facilities and sources were revealed. The press published identified conventional and special signals intelligence collection sites in the United States, United Kingdom, Germany, Australia, and New Zealand (Appendix A: 47, 48, 49 & 50). The publications included the amount of data the sites were collecting, surveillance devices, their exact location and levels of successes. Once the location of a device or intelligence collection site is confirmed, adversary measures to avoid a given link or device can be implemented. Similarly, the physical location could be threatened as well as the personnel associated. This implication has already been acknowledged by numerous officials, citing increased staff risk (Booth, 2013; Halliday, 2013).

Significant detail was also provided on the signals intelligence sources of numerous other nations (Appendix A: 6, 40-53). Implications of this revelation are the safety of foreign partners and the credibility of governments or companies when cooperating with the United States and allied governments. Waning cooperation, a

function of reacting to press reports and given political environments with other nations could destabilize regions and governments in areas where cooperation is critical to accessing adversary communications (Sanger & Smale, 2013).

Identities of SIGINT targets were revealed. Press reporting of the actual leaked documents by Mr. Snowden revealed a significant number of SIGINT targets. These included the nations and their leaders, communications systems and subsystems that were targeted, and the methods used for collecting intelligence against them (Appendix A: 54, 55, 56 & 57). Implications of these revelations include a backlash against the U.S. and allies, losses of intelligence cooperation, and access to foreign information sources when these potential sources have reason to believe that, if they cooperate with U.S. and allied intelligence services, the relationship will be revealed in the press (Nakashima, 2013b).

Impacts on U.S. intelligence of capabilities revealed that were previously unknown to adversaries. Three themes emerged from the data analysis, illustrating: 1) computer network attack and exploitation capabilities, 2) the depth and breadth of capabilities of SIGINT activities, and, 3) cryptology capabilities and successes.

Computer network attack and exploitation capabilities revealed. Press reporting of Computer Network Attack (CNA)/Computer Network Exploitation (CNE)/Computer Network Information Operations (CNIO) data indicated relationships between intelligence organizations and commercial interests that included systems targeted, levels of entry into computer systems, and persistence of CNA weapons (Appendix A: 63, 64 & 65). Implications from the publication of these relationships are twofold and included: 1) reduction or termination of business between the subject and the intelligence organization and 2) backlash from consumers who believe that their data is being collected and

analyzed the government courtesy of the commercial firm. Two specific entities, der Spiegel and reporter Glenn Greenwald through his website *The Intercept* (2015) revealed a total of 227 highly classified programs relating to this theme, with no repercussion from government. Implications here include that some press may now have new beliefs that they may publish, unchecked, the affairs of governments even if those reports contribute negatively toward the national security interests of the state (Appendix A: 64 & 65). Even though many adversaries, such as al Qaeda, assumed that their communications were being monitored, publication of the details and actual documents to reinforce reporting confirmed assumptions and potentially paved the way for countermeasures and stratagem to foil U.S. and allied intelligence (Norton-Taylor & Rushe, 2013).

Depth and breadth of capabilities of SIGINT activities revealed. Press reporting, in general, concentrated on personnel and physical size when reporting on U.S. and allied SIGINT capabilities. Publication of the actual leaked documents revealed significant capabilities to intercept and process staggering numbers of messages daily from a broad number of communication systems (Appendix A: 66-69). Given the mass of documents leaked, experts assessed the damage associated with the Snowden leak as the greatest damage that has ever been suffered to U.S. and allied intelligence collection systems (Leopold, 2014). Terrorists ceased using normal communications channels, realizing the implications stated in previous findings. Opined was the thought that adversaries probably knew much of the data that was leaked (Norton-Taylor & Rushe, 2013).

Cryptologic capabilities and successes revealed. Press reporting based on the leaked Snowden documents revealed that U.S. and allied intelligence had successfully exploited encryption used by Hotmail, Google, Yahoo and Facebook users (Appendix A:

72). The capability to decrypt commercial codes was implied to impact the privacy of business transactions. Questioned was the level of intrusiveness and violation of public trust as a result of government's ability to crack commercial encryption codes, specifically credit card transactions and commercial banking. The implications of revealing to the world U.S. and allied capabilities to decrypt enciphered communications is significant, as evidenced by elements associated with the Islamic State now using couriers or encrypted channels that cannot, theoretically, be readily decrypted (Schmitt & Hubbard, 2015).

Impacts on U.S. intelligence when liaisons and access to territories in which to conduct intelligence activities are revealed. Two findings emerged illustrating: 1) Intelligence relationships, liaisons and accesses, and 2) Intelligence repercussions.

Intelligence Relationships, Liaisons and Accesses. Intelligence relationships were reported by the press revealing the depth and breadth of relationships between the signals intelligence agencies internally with counterparts in other intelligence disciplines and externally with a minimum of 41 nations (Appendix A: 79). Internal relationships have been common knowledge in the literature for decades but the confirmation of relationships externally have significant implications. These implications include backlash from cooperating with countries that have neutralities which need to be preserved, such as Sweden and countries with political ramifications, such as Israel (Appendix A: 82 & 84). These relationships were sensitive due to neutralities or other issues such as nations that were traditionally each other's adversaries.

Among a number of world leaders subject to NSA monitoring were the German Chancellor and Brazilian President (Appendix A: 86 & 87). Diplomatic fallout from the

revelations were significant as capitals throughout Europe called on the U.S. to account for the disclosures, calling upon U.S. Ambassadors to explain the U.S. intelligence community's actions and some even calling personally upon the U.S. President. Similar activity was noted in Southeast Asia in the form of diplomatic tensions between Indonesia and U.S. intelligence partner, Australia (Laughland, 2013). Demands were made to instill rules on spying within Europe and the European Parliament demanded response to the leaked and published intelligence documents. Implications in this arena include a dissolving level of trust and cooperation between the U.S. and its European allies. The dichotomy here is that Europe and many of the European nations have been strong partners with the U.S. vis-s-vis intelligence collection and sharing. One significant implication is that a declining level of cooperation could result from the revelations and an internal European want to limit domestic backlash (Traynor, 2013c).

Intelligence repercussions. The press reported relationships between signals intelligence agencies and a number of private companies (Appendix A: 88). Reporting included assertions that these firms were conducting monitoring activities on behalf of the signals intelligence agencies. Implications could be fallout exacted on these companies from consumer retribution and on the intelligence community when the association is revealed. Indeed, the former has been realized, the former with consumers reacting to the revelations and the latter with the German government expelling the U.S. CIA station chief (Guardian, 2014b; Miller & Kirchner, 2014; Smale, 2015). Further implications could result from potential intelligence cooperation, should that cooperation be required, occurring at a slowed pace. Given that intelligence collection against foreign governments is a fundamental element of statecraft, implications further, a result of the

revelations and their publication could include a changing communications method by foreign government entities. Again, this implication has been realized by foreign leaders, Bolivia for example, changing their communications methods (Guardian, 2013b).

Other impacts on U.S. national security from Snowden's unauthorized disclosure of classified intelligence information to the press. One finding that emerged from the data analysis illustrated the role of secrecy and the press in press reporting.

Secrecy in press reporting. The press evaluated the intelligence agencies, assessed the laws governing them, and determined that mass surveillance was illegal (Appendix A: 92 & 93). Implications relating to this thought included a popular backlash from society due to the publication of misleading information (Taylor, 2014). Consider that surveillance of the scale reported in the press would imply that potentially tens of thousands of individuals were witting of the illegal activity. It also implies that these individuals participated in the illegal activity and, until the Snowden leak, maintained their obligations to their signed secrecy oath. Secrecy was judged ineffective by the press because nearly half a million persons possessed similar security clearance to Mr. Snowden. The press also questioned whether the information was still classified, post leak and publication. Implications relating to the classification thought are many and echo those found in the literature, specifically relating to the press' qualifications to determine what is or is not a secret (Ross, 2011; Sedler, 2007). If unchecked, the press could summarily publish everything that come to their desks stamped secret by government. Greenwald, and his reporting of clearly sensitive U.S. and allied intelligence collection systems, methods, and capabilities evidences the impact a reporter sans editor can inflict (Cardew, 2014; Nyst, 2015).

The Guardian initially published the stories relating to mass collection of communications by the NSA (Guardian, 2014a). Greenwald and a number of other reporters functioned as the “mosaic makers” in assembling and providing their perspective on the leaked information. When the press reported on the impact of the leak, they in general reported on the leak itself, versus the impact of the press’ reporting of the leak and their resultant analysis of the data and the mosaic-making efforts. This is important because the classified information, when initially leaked, was only given to a few select individuals. These individuals, knowing they had received stolen and – more so – classified intelligence documents chose to broadcast those mosaic-like pieces, in their assembled form, to hundreds of millions of persons under the guise of journalism. The implications of the press being the mosaic-makers are important because they build the picture from pieces of information from which they have no practical knowledge. Their analysis could be flawed and, more importantly, based on their own personal biases – as was the case with Mr. Greenwald – the information that was reported to the reader on the printed page resembled a personal vendetta against the U.S. (Cole, 2014).

Interestingly, the media claimed they verified and fact-checked the leaked information and that government was consulted and, as a result, no harm was done in the publication of the Snowden documents (Fahri, 2014; Quinn, 2013). The argument that intelligence professionals knew better what information should be suppressed was dismissed as superficial. Experts in the British defense establishment accused the media of producing a handbook for terrorists (Greenslade, 2014). The Guardian’s self-assessment of its behavior was remarkable, noting that at a point it had only published 26 of more than 58,000 documents. Guardian leadership also believed they had saved the

intelligence agencies further damage, and that the newspaper itself was the target of foreign intelligence services trying to access the leaked documents in their possession (Huppert, 2013). Implications relating to the press believing that they were saving further damage extend to the thought that the press is not only the arbiter of what is or is not classified, but implies that government, in its attempt to protect information in the national security interest, is wrong or covering up wrongdoing in their requests to the press to refrain publication. This thought is not only mentioned in the press articles on the Snowden but echoed in the literature (Gup, 2003; Risen, 2009; Etzioni, 2014).

Press considered their reporting as causing less damage than other historic leaks, despite Daniel Ellsberg, leaker of the Pentagon Papers, considering the leaks significant (Norton-Taylor, 2013a; Roberts, 2013). However, some anonymous former intelligence officials assessed the damage as overly exaggerated. Implications of downplaying the leak and its subsequent publication for adversaries to peruse seems to indicate a lack of understanding of the material and of the subject matter in general. When “anonymous former intelligence officials” were quoted, these individuals should have recognized the gravity of the information at hand. From the study findings documented in this study, it is apparent that downplaying the information and its impact was akin to pandering to the media and joining the anti-government bandwagon in condemning the information contained within the leaked documents.

The Snowden documents and their publication increased public debate, inspiring congressional and parliamentary legislation, investigations, a Presidential review, and a general rethinking of the role of government surveillance agencies (Nyst, 2015). The implications of this public debate is based on how the press reports the information

versus what, exactly, the leaked information contains (Hopkins, 2013a; Shane, 2013b). In this case, reporting of the capabilities of NSA to monitor American citizens' communications while not overblown, led much of the American public to believe that they were the primary targets of surveillance rather than adversaries.

Recommendations

Recommendations for practical application. Mr. Snowden turned over in excess of 1.7 million documents to the media dealing with U.S. and allied intelligence collection sources and methods. A small portion of the overall number of compromised documents have been released in press reporting with the major document holder, Mr. Greenwald – now operating as an independent journalist – promising the release of more at his discretion (Nakashima, 2013d). The intelligence community had divided the Snowden material, by June 2014, into three levels: a) documents that were published, many with redactions, numbering about 300; b) 200,000 additional documents given to the media, and; c) documents of unknown status or disposition, numbering about 1.5 million, according to unnamed senior U.S. officials. (Ignatius, 2014). Mr. Snowden claimed that no one other than journalists he met in Hong Kong had received the documents (Risen, 2013). It is recommended for practical application that U.S. and allied intelligence agencies assume that all of the sources, methods, and systems turned over to Mr. Greenwald and his associates by Mr. Snowden have been compromised in their entirety to potentially adversarial nations such as China and Russia. These potential adversaries, although not claiming knowledge or possession of the leaked classified intelligence documents can, in the worst case scenario, change tactics, techniques, and procedures at a time of their choosing so as to avoid U.S. and allied intelligence

collection. Therefore, U.S. intelligence should work immediately to invoke new tactics, techniques, and procedures for intelligence collection. Further the U.S. Attorney General working with the Secretary of State on behalf of the United States need to do everything in their power, within the law, working with the Government of Brazil – where Greenwald resides – to see that all the remaining and unpublished leaked documents in Greenwald’s possession are returned to the United States.

Practical application extends to a smaller threat subsection, so equally to be assumed, is acquisition of the leaked classified material, through the press, by smaller and relatively less technologically advanced non-state groups to include those labeled as terrorists or hackers by U.S. or allied governments. Due to the leaks of Mr. Snowden and the scrupulous publication of the nation’s intelligence sources and methods by reporters like Mr. Greenwald, societies will increase their vulnerabilities to attack due to, as Pozen (2005) states, “the dangers of adversarial mosaic-making” (p. 650). This has been evident in recent events such as multipronged attacks in Paris in November, 2015. Former U.S. Director of Central Intelligence, James Woolsey, directly attributed these attacks to adversaries studying the published material from Mr. Snowden’s leaks (Glum, 2015).

To assert that U.S. and allied intelligence services were conducting illegal activity in their intelligence collecting efforts implies that thousands of individuals were witting and approving of the illegal activity with only one, Mr. Snowden willing to speak out in public. Such is not the case. Similarly, to imply that effective oversight mechanisms were lacking is misleading. That the American people should be informed as to the activities of their intelligence services is not in doubt (Quinn, 2013). But informing the American citizens also, by proxy, informs adversaries or potential adversaries. From the results of

this study, practical application should be that the U.S. Intelligence effectively informs the Congress as to the activities of the Intelligence Community. As representatives of American citizens, they become the population – the people – as a whole, staying informed, and keeping classified information within its controlled channels.

Much of the reporting based on the documents that Mr. Snowden released was misleading in that they implied U.S. and allied intelligence services were monitoring and misusing information gathered from their own citizens. The evidence in this research indicates that such was not the case (Risen & Lichtblau, 2013). Practical application extends here to government effectively informing its own citizens when those citizens are misinformed by the press. Similarly, much has been made given the press' primary role, whether that role is called selling air, selling advertising, comforting the afflicted, or afflicting the comfortable (Kovach & Rosenstiel, 2007). The press must be accountable for the information that they report if they are to consider themselves the “fourth” branch of government (Kovach & Rosenstiel, 2007). Practical application is that checks and balances regarding press reporting of issues of U.S. national security should be a two-way street so truth can be reported without increasing vulnerabilities to the citizenry.

Due to Mr. Snowden's former employment with the NSA, he had an extensive knowledge of encryption and advanced data storage and transmission methods. This was due, in part, to an increased level of intelligence sharing in the wake of the September 11th, 2001 terrorist attacks and contributed to Mr. Snowden's theft and subsequent compromise of millions of intelligence community documents (MacAskill, 2013b). Practical application, based on study findings, means changing access, process, and

safeguards to access classified material. Further, audit trails should be established to track patterns of data access so as to identify individuals with no reasonable need-to-know.

Due to study findings documenting the significant damage done to U.S. and allied intelligence by the leaked and published documents, this researcher feels he must also make a further comment regarding a practical application needed regarding the Mr. Greenwald, the lead journalist of the Snowden event. As early as July, 2013, U.S. officials were uncertain as to whether Russia or China had obtained the Snowden documents (Washington Post, 2013c). Officials from the British Prime Minister's office, the British interior ministry, and security services had confirmed that by June, 2015, Britain had removed intelligence agents from a number of countries due to "...agents and assets being targeted", a direct function of the Snowden leak and publication of its contents (Reuters, 2015). With significant assistance from supporters, Mr. Snowden was able to evade capture by fleeing the United States to Hong Kong and, subsequently, Russia where he sought asylum and remains as of the publication date of this research. Mr. Greenwald's courier stated that he was unable to open the files he was carrying. A British court, in admonishing Mr. Greenwald, assessed that neither he – Mr. Greenwald – nor his courier were in "a position to form an accurate judgment on the matter because they would depend on knowing the whole "jigsaw" of disparate pieces of intelligence" – the mosaic effect (Travis, 2014). Given Mr. Greenwald's anti-U.S. rhetoric, this researcher recommends the practical application toward investigating whether Mr. Greenwald and his associates had as their target audience adversary nations and their intelligence services.

Significant to this research was the predominance the press placed on making themselves the news versus the stolen and leaked information (Bell, 2013). An examination of the press role reveals a level of espionage tradecraft in acquiring, moving, and protecting the Snowden documents. In fact, given the behavior of the three initial reporters in secreting the information from the source, Mr. Snowden, the only legal roadblock between what these reporters considered journalism and what the government considered espionage is the First Amendment of the U.S. Constitution (U.S. Const. amend. I). Normally a criminal offense under Section 798 of the Espionage Act, this activity was shielded under protections afforded by the First Amendment of the Constitution of the United States. It is this researcher's opinion, based on study findings that practical application should include enforcing the Espionage Act of 1917 by the U.S. Congress and Attorney General. This Act and specifically the COMINT Statutes contained therein, if aggressively enforced, could deter future leaks of classified intelligence sources and methods. The historical record of inactivity and ambivalence toward enforcement under this statute should be reversed (Bruce, 2003; Schoenfeld, 2011, 2013). The inherent tension between Section 798 of the Espionage Act and the First Amendment of the U.S. Constitution should be tested and modified, if necessary, according to the opinions of the courts.

Recommendations for future research. Given advances in technology, specifically data storage and transmission speeds, one must ask the question of whether the press is, in their mosaic-making efforts of the government's intelligence sources and methods, functioning as the intelligence collection and analysis apparatus for the nation's adversaries? While their claims that adversaries knew the information already is dubious

at best, one must consider if that is indeed the case – did adversaries already know this data at this level of detail? If the answer is no, one has a case for the press providing aid and comfort to the enemy. If the answer is yes, the U.S. and her allies have grossly overestimated their counterintelligence success. Future academic study is recommended to research the press' role, if any, as an adversary intelligence collection and propaganda apparatus.

Press publication of the leaked, classified intelligence information sparked two-pronged reaction. Once the first leaked intelligence information was published, the press was criticized within its own press circles and externally from experts familiar with mass surveillance (Guardian, 2013c). The Director of the National Security Agency, the Director of National Intelligence, and a Conservative Member of the British Parliament all criticized the press' publication of the leaked classified intelligence information, saying that the information published had been misleading (Lewis, 2013c). A British former foreign secretary labeled the press as naïve and arrogant when the press published articles based on the leaked information (Watt, 2013). Cabinet Secretaries went as far as cautioning newspaper editors to consider national security before rushing to publication (Somaiya, 2013). The editor of the New York Times, speaking on behalf of her newspaper and The Guardian, said that government prior restraint requests receive consideration but a greater weight is given the task of informing the public (Guardian, 2013c; Pilkington, 2013). A Washington Post reader opined that journalists were not in a position to declassify information and that given a “Free Flow of Information Act” journalists, that come to possess classified material, should be held to the same standards of safeguarding as those with a security clearance (Washington Post, 2013b). Future

research should be conducted on whether a “Free Flow of Information Act” would be a viable option to meter leaked, classified information to the public given secrecy concerns and adversary use of government information for their benefit. Similarly, given the rapid advances in data transmission, a version of Britain’s “Official Secrets Act” should be tested in the United States.

Finally, based on this study’s findings, this researcher recommends investigating the fiscal impact of the leaks and their publication. Given the significant capabilities that were compromised and certain adversarial countermeasures that have been or will occur, costs for research and development of capabilities have been incurred as well as future costs for development of new capabilities. External to government, costs to society resulting from adversarial actions, such as the Paris attacks, could be substantial.

Conclusions

This study investigated and documented significant impacts to U.S. intelligence from the unauthorized bulk disclosure of classified intelligence information from Edward Snowden and publication by the press. The research findings then also provided greater insight into Mosaic Theory. Previous research, although sparse, found that Mosaic Theory traditionally applied to Fourth Amendment law (Kerr, 2012), was oft cited by government (Slobogin, 2012), and was synergistic, but lacked theoretical development (Pozen, 2005). Additionally, Mosaic Theory was used as a defense by government so as not to publically divulge information and as a theory of intelligence analysis by ally and adversary alike (McQueen, 2007; Pozen, 2005, 2010; Schulhofer, 2013; Setty, 2012). Pozen (2010) and Ross (2011) introduced the concept that the press can be mosaic makers, filling in voids in adversarial intelligence gathering.

The purpose of this single-case, holistic study was to examine the impacts to U.S. intelligence from Edward Snowden's unauthorized bulk disclosure of classified intelligence information to the press that may have included, but may not have been limited to, U.S. Intelligence sources and methods, capabilities, liaisons, and accesses to territories essential for U.S national security. The population for the study was the unauthorized documents disclosed to the press. The sample for the study was the published documents that compromised national security. Implications for the study were derived from the sub-questions, the triangulated data, and the referenced literature.

The study findings revealed significant impacts to U.S. intelligence sources and methods due to the previously unpublished knowledge of, at a minimum, computer network exploitation and attack methods, SIGINT methods, locations, types of facilities and sources, and targets (Appendix A: 4-59). The study findings further showed impacts on U.S. intelligence due to the revelation of its capabilities which included previously unpublished knowledge of computer network attack and exploitation capabilities, the depth and breadth of capabilities of SIGINT activities, and cryptologic capabilities and successes (Appendix A: 60-73).

Additionally, study findings revealed impacts to U.S. intelligence liaisons and access to territories due to the publication of the leaked and classified intelligence information (Appendix A: 73-90). This information included themes relating to intelligence relationships, liaisons and accesses and intelligence repercussions. Finally, the study findings revealed other impacts to U.S. national security from Snowden's unauthorized disclosure of classified intelligence information to the press. The overriding

theme emerging related to the role of secrecy and the press in press reporting (Appendix A: 91-100).

The press began publication of the information to a worldwide audience to include classified intelligence information revealing sources and methods of U.S. and allies' intelligence gathering (Appendix A: 4; 8-21). Significant were the actual classified intelligence documents accompanying many of the news articles. Information migration between themes, an unexpected and unintended benefit of the data coding helped to more fully answer the sub-questions. A fuller explanation of the results of the documents analysis were illustrated and reported for each sub-question.

By placing the data side by side – the actual compromised classified intelligence information and the press reporting thereof – it was possible to build an accurate mosaic of U.S. and allied intelligence strengths and weaknesses. Simply, the press functioned as the mosaic maker. Their reporting allowed ordinary citizens and adversaries alike to create their own mosaics and act upon the data. The result, at a minimum, was that citizens built a healthy distrust in the government's ability to conduct intelligence activities and adversaries changed methods of communicating, aiding their effectiveness and rendering themselves all but invisible to intelligence collection as evidenced in the Paris terrorist attacks of November, 2015 (Glum, 2015). Citizens and adversaries could have been aided in their mosaic-making efforts by the press reporting the classified data and providing context to that data. More so, the mosaic-makers were assisted by being able to access the actual documents that accompanied most of the press reporting.

After the leaks were made public, significant criticism was aimed at one of the initial reporters of the leaks, Glenn Greenwald, a self-described activist and advocate.

Professor David Cole, writing in the Washington Post (2014), stated that Mr. Greenwald did not know the difference between “justified and unjustified leaks,” that some of Mr. Greenwald’s reporting had been misleading, and that overstating a problem weakened his credibility as a journalist. Greenwald, in rebuttal, criticized traditional media for consulting with government when faced with leaked classified material of the nature that he received (Greenwald, 2013c). Importantly, the New York Times revealed that in much of his reporting, Mr. Greenwald did not report to an editor, but rather published through a direct link without editor preapproval (Cohen & Kaufman, 2013).

The National Security Agency was vilified as the public was led to believe that “they” were the target of government surveillance and not “by catch” in the surveillance dragnet, given technological advances. Press reporting indicated that the government – Big Brother – was building an intelligence collection apparatus to collect on not only U.S. but all citizens worldwide (Risen & Poitras, 2013). The volume of data collection was assessed as infringing on the privacy of citizens and that NSA was listening to every phone call and the government would possibly misuse the information that was collected. No evidence existed though, according to some press estimates, that any laws were violated (Risen & Lichtblau, 2013). Accusations that NSA is operating as Big Brother must be addressed by NSA in open public forums. A challenge to NSA being heard and believed will occur when trying to counter a vocal minority, and the press, that outshouts government in the debate.

In this leaked and published documents case, the press responded to government and citizen criticism in both a traditional and contemporary manner. Unless the issue is addressed, the later manner, based on study findings, will affect future leaks of this type

and volume. Traditionally, the First Amendment of the Constitution was invoked as was the press' duty to "irritate the powerful" (Guardian, 2013c; McCarthy, 2013). The duty to expose abuses of power, challenge government, and write about what exists was a portion of the duties and responsibilities of a journalist described by editors of prominent newspapers in defense of publishing the leaked documents (Guardian, 2013c). A contemporary view was that of the adversarial journalist, some noting that, at a minimum, anti-American activists had controlled the story line (Bolton, 2014; Dredge, 2014). At question was the relevance of the objective journalist versus the activist journalist, one that is "objective, neutral, impartial" and one that is "subjective, activist, adversarial" (Greenslade, 2013). Perhaps the latter role was best reasoned by Seymour Hersh who, in referencing government at a symposium on secrecy, surveillance, and censorship stated "We are here to keep them in check, to keep the powers that be in check. That's the only thing between them, and chaos - fascism if you like. Because they lie. They are frigging liars, because it's so easy to lie... We have a role to play. We can at least keep them afraid of us" (Dredge, 2014).

Mr. Snowden stole and provided to the media in excess of 1.7 million classified documents relating to sources and methods on allied intelligence collection efforts, ostensibly intending to "alert the world to the unprecedented and industrial scale" of espionage, including operations against Russian and Chinese intelligence targets (Caplan, 2013; Johnson, 2014; Meyer, 2014; Papandrea, 2014). In doing so, he violated the Espionage Act of 1917 (Espionage Act of 1917). It is evident from this study's findings that he did not have the knowledge (or right) to determine what information needed to be in the public domain nor did he, apparently, avail himself to existing government entities or

programs, such as standing Inspector General, for employees with ethical or legal concerns (Check & Radsan, 2010; Vladeck, 2008).

Implications relating to this issue include monitoring government action related to prosecution of Mr. Snowden and his accomplices, should there be any. Should government not maintain their level of effort to render Mr. Snowden to the United States and prosecute the case, they will maintain the status quo when considering the Espionage Act and governments dearth to prosecute under the same. Implications relating to a lack of prosecution could include giving license, by proxy, to anyone with a security clearance, a thumb drive, and a crisis of conscience and an unwillingness to utilize systems in place to air and rectify grievances.

The collaboration between Mr. Snowden and Mr. Greenwald, one of three reporters given initial access to the Snowden horde, included the use of clandestine communications methods, military-grade encryption, couriers to move documents between countries – elements associated with traditional espionage (Kakutani, 2014). Initially, for Mr. Greenwald, the communications logistics posed a challenge, but was overcome by “installing encrypted instant chat and e-mail programs” on his computer. In at least one instance of record, one of Mr. Greenwald’s couriers was detained in London with 58,000 encrypted and highly classified intelligence documents leaked from Mr. Snowden that revealed, in part, the identities of U.K. intelligence officers both within the U.K. and abroad (Booth, 2013). These documents in the courier’s possession included passwords that would allow a user to decrypt the documents.

Where Mr. Snowden metaphorically broadcast the stolen classified intelligence information to a group of three, the press actually broadcast to billions of individuals the

infrastructure and capabilities of U.S. and allied nations. The direct impact of these revelations was instant and dramatic, as revealed in the answers to sub-questions, per the study findings. Just as significant to what was revealed is what was not. Due to an overstatement of the actual contents of the leaked classified intelligence documents, citizens were led to believe that the intelligence apparatus of the U.S. and allied countries were turning inward to actively and illegally monitor their own citizens (Greenwald, 2013c; Risen & Poitras, 2013). Given the analysis in this study of the 524 actual documents released by the press to supplement their reporting, no evidence indicated such an activity – the United States spying on its own citizens – was taking place. Mosaic making, thus, depends on the truthfulness of the mosaic-maker. The U.S. Government, in their mosaic-making efforts to inform decision-makers, i.e., Congress, for the purposes of investigating and prosecuting criminals or providing intelligence, seek to deliver truth to power (Marrin, 2013; McGruddy, 2013). These study findings show that the press, in the Snowden event, did not hold themselves to as stringent a standard.

References

- Aftergood, S. (2010). National Security Secrecy: How the Limits Change. *Social Research*, 77(3), 839-852.
- Alson, M. (2008). Someone Talked! The Necessity of Prohibitions against Publishing Classified Financial Intelligence Information. *Valparaiso University Law Review*, 42(4), 1277-1317.
- Ball, J., Borger, J. & Greenwald, G. (2013, September 6). Front: Exclusive: how US and Britain unlock privacy on the internet: Elaborate safeguards broken by NSA and GCHQ: Encryption meant to protect emails, bank and medical records: New Snowden revelations certain to cause political row. *The Guardian*. Retrieved from Lexis/Nexis.
- Baxter, P. & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report* 13(4), 544-559.
- Bell, E. (2013, December 16). Media: A year of fireworks for the NSA and BBC: Austerity and the digital era have forced big changes on to the media, with new partnerships and bold decisions the keys to delivering quality journalism in the new world. *The Guardian*. Retrieved from Lexis/Nexis.
- Berg, B. L. (2004). *Qualitative research methods for the social sciences*. Boston, Mass: Pearson.
- Bolton, J. (2013, June 18). Edward Snowden's leaks are a grave threat to US national security. *The Guardian*. Retrieved from Lexis/Nexis.
- Booth, R. (2013, August 13). David Miranda: police win wider powers to investigate seized data. *The Guardian*. Retrieved from Lexis/Nexis.
- Borger, J. (2013, October 22). Surveillance: French anger widens diplomatic difficulties over Snowden revelations for US and Britain: Signs that US and UK losing 'soft power' in controversy over intelligence agencies. *The Guardian*. Retrieved from Lexis/Nexis.
- Boycott, O. (2014, May 14). GCHQ spying programs face legal challenge. *The Guardian*. Retrieved from Lexis/Nexis.
- Bruce, J. (2003). The Consequences of Permissive Neglect: Laws and Leaks of Classified Information. *Studies in Intelligence*, 47(1). Washington, DC: Central Intelligence Agency. Retrieved from <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/index.html>

- Bryman, A. (2002). *Triangulation*. Retrieved from www.referenceworld.com/sage/socialscience/triangulation.pdf
- Caplan, L. (2013). Leaks and Consequences: Why treating leakers as spies puts journalists at legal risk. *American Scholar*, 82(4), 20-31. Retrieved from <http://theamericanscholar.org/leaks-and-consequences/#.VGdrRst0zA4>
- Cardew, B. (2014, March 3). Media: Can Greenwald's Intercept help reinvent journalism?: Collaboration is the key for First Look's online magazine. *The Guardian*. Retrieved from Lexis/Nexis.
- Carroll, R. (2013, June 27). Ecuador breaks US trade pact to thwart 'blackmail' over Snowden asylum. *The Guardian*. Retrieved from Lexis/Nexis.
- Carroll, R. & Collins, D. (2013, June 28). Edward Snowden: Correa shoots first in Ecuadorean stand-off: Leftist leader renounces bilateral deal with US 'We do not trade principles for mercantile interests'. *The Guardian*. Retrieved from Lexis/Nexis.
- Check, R.M. & Radsan, A.J. (2010). One lantern in the darkest night: The CIA's inspector general. *Journal of National Security Law & Policy*, 4(2), 247-294. Retrieved from <http://proxy1.ncu.edu/docview/872471642?accountid=28180>
- Chrisafis, A. & Lewis, P. (2013, October 22). Front: Obama tries to calm French fury over mass surveillance. *The Guardian*. Retrieved from Lexis/Nexis.
- Cohen, H. (2009). Freedom of speech and press: Exceptions to the First Amendment. *CRS Report for Congress*. Washington, D.C.: Congressional Research Service. Retrieved from www.crs.gov
- Cohen, M. (2013, June 21). Is Obama presiding over a national security state gone rogue? *The Guardian*. Retrieved from Lexis/Nexis.
- Cohen, N. & Kaufman, L. (2013, June 7). Blogger, With Focus on Surveillance, Is at Center of a Debate. *The New York Times*. Retrieved from Lexis/Nexis.
- Cole, D. (2014, May 18). NSA mantra: 'Collect it all . . . know it all'. *The Washington Post*. Retrieved from Lexis/Nexis.
- Creswell, J.W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, Ca: SAGE Publications
- Danielson, E. S. (2011). Secret Sharers. *The American Scholar*, 80(4), 39-46. Retrieved from ProQuest.

- Divoll, V. (2011). The "full access doctrine": Congress's constitutional entitlement to national security information from the executive. *Harvard Journal of Law and Public Policy*, 34(2), 493-542. Retrieved from <http://proxy1.ncu.edu/docview/868927008?accountid=28180>
- Doorey, T. J. (2007). Intelligence Secrecy and Transparency: Finding the Proper Balance from the War of Independence to the War on Terror. *Strategic Insights*, VI(3). Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484534
- Dredge, S. (2015, February 6). How have journalists responded to revelations of mass surveillance?; Edward Snowden's NSA whistleblowing has led more journalists to protect their data and sources, but they're not giving up on stories. *The Guardian*. Retrieved from Lexis/Nexis.
- Dredge, S. (2014, December 5). Live from The Logan Symposium: secrecy, surveillance and censorship; From Wikileaks and Edward Snowden to investigative journalism and the future of hacking, London event gets underway. *The Guardian*. Retrieved from Lexis/Nexis.
- Dulles, A. (1963). *The Craft of Intelligence*. New York: Harper & Row.
- Eisenhardt, K.M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, 14(4), 532-550. Retrieved from <http://www.jstor.org/stable/258557>
- Ellsberg, D. (2010). Secrecy and National Security Whistleblowing. *Social Research*, 77(3), 773-804.
- Elsa, J. (2011). Criminal Prohibitions on the Publication of Classified Defense Information. *CRS Report for Congress*. Washington DC: Congressional Research Service. Retrieved from www.fas.org/sgp/crs/secrecy/R41404.pdf
- Espionage Act of 1917, Act of October 6, 1917, ch. 106, §10(i), 40 Stat. 422, codified at 18 U.S.C. §§ 793-98
- Etzioni, A. (2014). A Liberal Communitarian Approach to Security Limitations on the Freedom of the Press. *William & Mary Bill of Rights Journal* 22(4), 1141-1181. Retrieved from <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1697&context=wmborj>
- Fahri, P. (2014, March 22). Slow leak: Why NSA articles trickle out. *The Washington Post*. Retrieved from Lexis/Nexis.
- Fenster, M. (2012). Disclosure's Effects: WikiLeaks and Transparency. *Iowa Law Review* 97, 753-807. Retrieved from www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf

- Follorou J. & Greenwald, G. (2013, October 21). France in the NSA's crosshair: phone networks under surveillance. *Le Monde*. Retrieved from http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html
- Freivogel, W. H. (2009). Publishing National Security Secrets: The Case for “Benign Indeterminacy”. *Journal of National Security Law & Policy* 3(3), 95-119. Retrieved from http://jnslp.com/wp-content/uploads/2010/08/03-Freivogel_ver_16_9-21-09.pdf
- Gearan, A. (2013, October 22). Report: NSA netted 70 million French phone records in month. *The Washington Post*. Retrieved from Lexis/Nexis.
- Gellman, B. (2013, December 24). Edward Snowden, after months of NSA revelations, says his mission's accomplished. *The Washington Post*. Retrieved from Lexis/Nexis.
- Glum, J. (2015, November 20). After Paris Attacks, Edward Snowden Should Be “Hanged by the Neck”, Former CIA Director James Woolsey Says. *IBTimes*. Retrieved from <http://www.ibtimes.com/after-paris-attack-edward-snowden-should-be-hanged-neck-former-cia-director-james-2193697>
- Goodwin, M.P. (2010). A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts. *Hastings Communications and Entertainment Law Journal* 32(2), 179-207. Retrieved from LexisNexis Academic.
- Graber, D. (2002, August). *Terrorism, the 1st Amendment and Formal and Informal Censorship: In Search of Public Policy Guidelines*. Paper presented at the annual meeting of the American Political Science Association, Boston, MA. Retrieved from http://www.allacademic.com/meta/p66714_index.html
- Grabo, C. (2004). *Anticipating Surprise: Analysis for Strategic Warning*. Lanham, MD: University Press of America.
- Green, A. (2005). *It's mine!: Why the US Intelligence Community does not share information*. Maxwell Air Force Base, AL: Air University.
- Greenslade, R. (2013, October 29). Greenwald vs Keller - adversarial journalism vs mainstream journalism. *The Guardian*. Retrieved from Lexis/Nexis.
- Greenslade, R. (2014, May 13). Media academic attacks press campaign against The Guardian over Snowden leaks. *The Guardian*. Retrieved from Lexis/Nexis.
- Greenwald, G. (2015). *About The Intercept*. Retrieved from <https://firstlook.org/theintercept/about/>

- Greenwald, G. (2013a, August 10). Comment: What would Google do?: Lavabit, the encrypted email service, has closed rather than betray users. Others should do so too. *The Guardian*. Retrieved from Lexis/Nexis.
- Greenwald, G. (2013b, August 9). Email service used by Snowden shuts itself down, warns against using US-based companies. *The Guardian*. Retrieved from Lexis/Nexis.
- Greenwald, G. (2013c, June 14). On PRISM, partisanship and propaganda. *The Guardian*. Retrieved from Lexis/Nexis. *The Guardian*. Retrieved from Lexis/Nexis.
- Greenwald, G. (2013, July 10). The journalistic practices of the Washington Post and Walter Pincus. *The Guardian*. Retrieved from Lexis/Nexis.
- Greenwald (2013e, July 7). The NSA's mass and indiscriminate spying on Brazilians. *The Guardian*. Retrieved from Lexis/Nexis.
- Guardian. (2013a, July 3). Leading Article: Edward Snowden: A whistleblower, not a spy. Retrieved from Lexis/Nexis.
- Guardian. (2013b, October 11). The Snowden files: The debate: Surveillance, democracy, transparency - a global view. Retrieved from Lexis/Nexis.
- Guardian. (2013c, October 11). The Snowden files: Yesterday, the Daily Mail described the Guardian as 'The paper that helps Britain's enemies'. We showed that article to many of the world's leading editors. This is what they said. *The Guardian*. Retrieved from Lexis/Nexis.
- Guardian. (2014a, February 1). Weekend: 'I have some stuff you might be interested in ...': Edward Snowden was an unlikely whistleblower: politically conservative, a gun owner, a geek - and for several years a loyal NSA contractor. What changed? Luke Harding uncovers the man behind the most explosive intelligence leak in history. *The Guardian*. Retrieved from Lexis/Nexis.
- Guardian. (2014, July 19). Weekend: I, spy: He doesn't drink, he's reading Dostoevsky and, no, he doesn't wear a disguise. A year after blowing the whistle on the NSA, Edward Snowden talks to Alan Rusbridger and Ewen MacAskill about his life as a hero-pariah - and why the world remains 'more dangerous than Orwell imagined'. *The Guardian*. Retrieved from Lexis/Nexis.
- Gup, T. (2004). Covering the CIA in times of crisis: Obstacles and Strategies. *Working Paper Series #2004-3*. Cambridge, MA: Harvard University. Retrieved from <http://www.hks.harvard.edu/presspol/publications/papers.html>

- Gup, T. (2003). Useful Secrets: In a Run-Up to War, How Do We Report Intelligently on Intelligence? *Columbia Journalism Review*, 41(6), 14-16.
- Halliday, J. (2013, June 18). Covert surveillance: Media: MoD serves news outlets with D notice over surveillance leaks. *The Guardian*. Retrieved from Lexis/Nexis
- Heemsbergen, L.J. (2013). Radical Transparency in Journalism: Digital Evolutions from Historic Precedents. *Global Media Journal* 6(1), 45-65. Retrieved from www.gmj.uottawa.ca/1301/v6i1_heemsbergen.pdf
- Hillebrand, C. (2012). The Role of News Media in Intelligence Oversight. *Intelligence and National Security*, 27(5), 689-706.
- Hoekstra, P. (2005). Secrets and leaks: The costs and consequences for national security. *Heritage Lectures No. 897*. Retrieved from www.heritage.org/research/national-security/hl897.cfm
- Hopkins, N. (2013a, December 3). Guardian will not be intimidated over NSA leaks, Alan Rusbridger tells MPs. *The Guardian*. Retrieved from Lexis/Nexis.
- Hopkins, N. (2013b, October 9). MI5 chief's criticism of Snowden and the Guardian is hardly unexpected. *The Guardian*. Retrieved from Lexis/Nexis.
- Hopkins, N. (2013c, December 2). The Snowden files: Inside the surveillance state: From: Turing to Tempora: The US-UK intelligence pact, forged in the second world war, has evolved beyond the two governments' control - and perhaps even their understanding. *The Guardian*. Retrieved from Lexis/Nexis.
- Huppert, J. (2013, December 4). Comment: It's not about the Guardian: On GCHQ surveillance, Britain has missed the point. The real issue is ensuring proper oversight. *The Guardian*. Retrieved from Lexis/Nexis.
- Ignatius, D. (2014, June 8). The Snowden side effect: Transparency. *The Washington Post*. Retrieved from Lexis/Nexis.
- Inkster, N. (2014). The Snowden Revelations: Myths and Misapprehensions. *Survival: Global Tactics and Strategy* 56(1), 51-60. DOI: 10.1080/00396338.2014.882151
- Jarvis, J. (2013, December 30). The primary NSA issue isn't privacy, it's authority. *The Guardian*. Retrieved from Lexis/Nexis.
- Johnson, L. (2014). An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security* 29(6), 793-810.
- Kakutani, M. (2014, February 5). Tales from Within the N.S.A.'s Monumental Haystack. *The New York Times*. Retrieved from Lexis/Nexis.

- Kerr, O.S. (2012). The Mosaic Theory of the Fourth Amendment. *Michigan Law Review* 111, 311-354. Retrieved from <http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1079&context=mlr>
- Kessler, R. (2008). The new spies. *SAIS Review*, 28(1), 147-156. Retrieved from <http://search.proquest.com/docview/231330519?accountid=28180>
- Kitrosser, H. (2007a). “Macro-Transparency” as Structural Directive: A Look at the NSA Surveillance Controversy. *Minnesota Law Review*, 91(5), 1163-1208.
- Kitrosser, H. (2007b). *Classified information leaks and free speech*. Rochester, MN: University of Minnesota. Retrieved from <http://search.proquest.com/docview/189890563?accountid=28180>
- Kitrosser, H. (2013). Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information. *Journal of National Security Law & Policy* 6(2), 409-446. Retrieved from <http://jnslp.com/wp-content/uploads/2013/04/Free-Speech-Aboard-the-Leaky-Ship-of-State.pdf>
- Klarevas, L. (2006). The Law: The CIA Leak Case Indicting Vice President Cheney’s Chief of Staff. *Presidential Studies Quarterly* 36(2), 309-322.
- Kohn, L. T. (1997). Methods in Case Study Analysis. *Center for Studying Health System Change: Technical Paper No. 2*. June, 1997. Retrieved from www.hschange.com/CONTENT/158/158.pdf
- Kosar, K.R. (2009). Security Classification Policy and Procedure: E.O. 12958, as Amended. *CRS Report for Congress*. Washington DC: Congressional Research Service. Retrieved from http://assets.opencrs.com/rpts/97-771_20090604.pdf
- Kovach, B., & Rosenstiel, T. (2007). *The elements of journalism: What newspeople should know and the public should expect*. New York: Three Rivers Press.
- Laqueur, W. (1998). The future of intelligence. *Society*, 35(2), 301-311. Retrieved from <http://proxy1.ncu.edu/docview/206714576?accountid=28180>
- Laughland, O. (2013, November 19). Intelligence gathering: Indonesia: Ambassador recalled over Australian attempts to listen to leaders' calls. *The Guardian*. Retrieved from Lexis/Nexis.
- Lears, J. (2013). Editor’s Note. *Raritan*, 33(1), 0-5. Retrieved from ProQuest Research Library.

- Lee, W. (2008). Deep Background: Journalists, Sources, and the Perils of Leaking. *American University Law Review*, 57(5), 1453-1529.
- Leopold, J. (2014, May 23). Snowden leaks 'staggering' in scope Pentagon report finds. *The Guardian*. Retrieved from Lexis/Nexis.
- Lewis, P. (2013a, October 29). Experts to present Obama with suggested surveillance reforms. *The Guardian*. Retrieved from Lexis/Nexis.
- Lewis, P. (2013b, October 28). NSA review panel to present Obama with dossier on surveillance reforms. *The Guardian*. Retrieved from Lexis/Nexis.
- Lewis, P. (2013c, September 26). US intelligence chiefs urge Congress to preserve surveillance programs. *The Guardian*. Retrieved from Lexis/Nexis.
- Liacas, T. (2015, May 8). Why Google and other tech giants are creating tools for political dissidents; After taking fire for caving to repressive regimes on data privacy, can the tech industry rehabilitate its reputation? *The Guardian*. Retrieved from Lexis/Nexis.
- Lowe, D. (2014). Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty. *Terrorism and Political Violence* 0, 1-21. DOI: 10.1080/09546553.2014.918880
- Lumbaca, S. & Gray, D.H. (2011). The Media as an Enabler for Acts of Terrorism. *Global Security Studies* 2(1), 45-54. Retrieved from globalsecuritystudies.com/media.pdf
- Lunev, S., & Winkler, I. (1998). *Through the eyes of the enemy: Russia's highest ranking military defector reveals why Russia is more dangerous than ever*. Washington, DC: Regnery Pub.
- MacAskill, E. (2015, March 28). UN sets up privacy rapporteur role in wake of Snowden leaks; Landmark decision in response to US and UK monitoring is attempt to establish idea that freedom from excessive surveillance is a basic right. *The Guardian*. Retrieved from Lexis/Nexis.
- MacAskill, E. (2013a, June 30). New NSA leaks show how US is bugging its European allies. *The Guardian*. Retrieved from Lexis/Nexis.
- MacAskill, E. (2014, July 1). NSA chief plays down damage done to intelligence by Snowden leaks. *The Guardian*. Retrieved from Lexis/Nexis.
- MacAskill, E. (2013b, June 6). The National Security Agency: surveillance giant with eyes on America. *The Guardian*. Retrieved from Lexis/Nexis.

- MacAskill, E. & Ball, J. (2013, November 22). Allies foiled over UN snooping resolution. *The Guardian*. Retrieved from Lexis/Nexis.
- Marrin, S. (2013). Revisiting Intelligence and Policy: Problems with Politicization and Receptivity. *Intelligence and National Security*, 28(1), 1-4. DOI:10.1080/02684527.2012.749063
- Mascolo, G. & Scott, B. (2013). Lessons from the Summer of Snowden: The Hard Road Back to Trust. Washington D.C.: The Wilson Center Open Technology Institute. Retrieved from <http://www.wilsoncenter.org/sites/default/files/NAF-OTI-WC-SummerOfSnowdenPaper.pdf>
- Mason, M. (2010). Sample Size and Saturation in PhD Studies Using Qualitative Interviews. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 11(3). Retrieved from <http://www.qualitative-research.net/index.php/fqs/article/view/1428/3027>
- Mason, R. (2013, October 24). MI5, MI6 and GCHQ chiefs to give evidence in public for first time. *The Guardian*. Retrieved from Lexis/Nexis.
- McCadden, H. (1961). Cover in Unconventional Operations. *Studies in Intelligence* 5(3). U.S. Central Intelligence Agency. Retrieved from www.cia.gov
- McCarthy, T. (2013, October 22). Richard Cohen's reverse on Snowden: not a 'traitor', but a whistleblower. *The Guardian*. Retrieved from Lexis/Nexis.
- McCraw, D. & Gikow, S. (2013). The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World. *Harvard Civil Rights – Civil Liberties Law Review*, 48(2), 473-509. Retrieved from <http://harvardcrcl.org/archive/>
- McGruddy, J. (2013). Talking truth to power for the intelligence professional - feeling the fear and doing it anyway! *Journal of Strategic Security*, 6(5), 221-226. doi:10.5038/1944-0472.6.3S.23
- McQueen, A. (2007). Security Blanket: The State Secrets Privilege Threat to Public Employment Rights. *The Labor Lawyer* 22, 329-353. Retrieved from http://www.americanbar.org/content/dam/aba/publishing/lel_flash/LL_mcqueen.authcheckdam.pdf
- Meyer, J. (2014). *Sources and Secrets – Background Brief*. Retrieved from <http://nationalsecurityzone.org/site/background-brief-on-sources-and-secrets/>
- Miller, G. & Kirchner, S. (2014, July 11). Berlin expels top CIA officer. *The Washington Post*. Retrieved from Lexis/Nexis.

- Morrison, J. (1966). *Protecting classified intelligence information – An historical review and some recommendations*. Retrieved from www.foia.cia.gov
- Moss, S. (2013, November 25). G2: 'How does a war like this ever end?': In the four years it took to make the documentary *Dirty Wars*, about America's secret hit squads, Jeremy Scahill met many of their victims in Pakistan, Afghanistan, Yemen and Somalia. He tells Stephen Moss why he promised to tell their stories. *The Guardian*. Retrieved from Lexis/Nexis.
- Nakashima, E. (2013a, June 16). Information behind phone calls, Web interactions reveals a lot. *The Washington Post*. Retrieved from Lexis/Nexis.
- Nakashima, E. (2013b, October 25). NSA documents could expose joint operations. *The Washington Post*. Retrieved from Lexis/Nexis.
- Nakashima, E. (2013c, September 27). Officials dodge questions about surveillance. *The Washington Post*. Retrieved from Lexis/Nexis.
- Nakashima, E. (2013d, July 12). Review of Snowden said to focus on foreign espionage. *The Washington Post*. Retrieved from Lexis/Nexis.
- Nakashima, E. & Miller, G. (2013, June 25). U.S. is worried about security of documents Snowden has. *The Washington Post*. Retrieved from Lexis/Nexis.
- Nelson, J. (2002). U.S. Government Secrecy and the Current Crackdown on Leaks. *Working Paper #2003-1*. Cambridge, MA: Harvard University. Retrieved from <http://www.hks.harvard.edu/presspol/publications/papers.html>
- Nilsson, J., & Sjölin, M. (2005). *Pack-hunt journalism: Ruthless journalism as the norm in the media society*. Lund, Sweden: Lund University.
- Norton-Taylor, R. (2013a, October 9). MI5 chief hits wrong target. *The Guardian*. Retrieved from Lexis/Nexis.
- Norton-Taylor, R. (2013b, October 11). The spooks strike back over GCHQ leaks - but they have a history of exaggerating threats. *The Guardian*. Retrieved from Lexis/Nexis.
- Norton-Taylor, R. & Cobain, I. (2013, October 17). Surveillance: 'Our national security is at risk' ... the empty threat to justify suppression: For as long as security services have kept secrets they have deployed the dire consequences of disclosure to silence and convict whistleblowers, but as Richard Norton-Taylor and Ian Cobain report, these claims seldom stand up to scrutiny. *The Guardian*. Retrieved from Lexis/Nexis.

- Norton-Taylor, R. & Rushe, D. (2013, September 13). Front: Ex-MI6 chief plays down damage from NSA leaks. *The Guardian*. Retrieved from Lexis/Nexis.
- Nyst, C. (2015, August 5). Investigative journalism is vital for democracy as state surveillance increases; In Germany, as in Britain, journalists should be free to report on and hold their countries' ever-widening surveillance programmes to account. *The Guardian*. Retrieved from Lexis/Nexis.
- Odom, W.E. (2003). *Fixing Intelligence: For a More Secure America*. New Haven, CT: Yale University.
- Official Secrets Act. (1989). Retrieved from <http://www.legislation.gov.uk/ukpga/1989/6/contents>
- Oltermann, P. (2014, April 27). Merkel urged to press Obama on NSA scandal ahead of Washington talks. *The Guardian*. Retrieved from Lexis/Nexis.
- Papandrea, M-R. (2012). Balancing and the Unauthorized Disclosure of National Security Information. *Iowa Law Review Bulletin* 97, 94-114. Retrieved from http://www.uiowa.edu/~ilr/bulletin/ILRB_97_Papandrea.pdf
- Papandrea, M-R. (2014). Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment. *Boston University Law Review* 94(2), 449-544. Retrieved from ProQuest.
- Papandrea, M-R. (2011). The Publication of National Security Information in the Digital Age. *Journal of National Security Law & Policy* 5(1). Retrieved from <http://jnsllp.com/topics/read/vol-5-no-1/>
- Papandrea, M-R. (2005). Under Attack: The Public's Right to Know and the War on Terror. *Boston College Third World Law Journal* 25, 35-80. Retrieved from <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1030&context=lsfp>
- Patton, M. Q. (2002). *Qualitative research & evaluation methods*. Thousand Oaks, CA: Sage Publications.
- Pearlman, W., & Cunningham, K.G. (2012). Nonstate Actors, Fragmentation, and Conflict Processes. *Journal of Conflict Resolution* 56(1), 3-15. doi: 10.1177/0022002711429669
- Perl, R (2006). Terrorism and National Security: Issues and Trends. *CRS Issue Brief for Congress*. Washington, DC: Congressional Research Service. Retrieved from www.fas.org/sgp/crs/terror/IB10119.pdf
- Pilkington, E. (2013, October 13). New York Times says UK tried to get it to hand over Snowden documents. *The Guardian*. Retrieved from Lexis/Nexis.

- Pincus, W. (2013, December 19). Snowden still holding a 'road map' for U.S. adversaries. *The Washington Post*. Retrieved from Lexis/Nexis.
- Posner, E.A., & Vermeule, A. (2007). The Credible Executive. *University of Chicago Law Review*, 74(3), 865-913. Retrieved from <http://lawreview.uchicago.edu/page/vol-74-issue-3-summer-2007>
- Pozen, D. (2010). Deep Secrecy. *Stanford Law Review*, 62(2), 257-339. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1501803
- Pozen, D.E. (2013). The Leaky Leviathan: Why the Government Condemns and Condone Unlawful Disclosures of Information. *Harvard Law Review* 127(2). Retrieved from www.harvardlawreview.org
- Pozen, D. E. (2005). The Mosaic Theory, National Security, and the Freedom of Information Act. *Yale Law Journal*, 115(3), 628-679.
- Price, D.H. (2014). The New Surveillance Normal: NSA and Corporate Surveillance in the Age of Global Capitalism. *Monthly Review* 66(3). 43-53. Retrieved from <http://www.monthlyreview.org/2014/07/01/the-new-surveillance-normal/>
- Quinn, B. (2013, October 16). New York Times editor defends journalists over Snowden leaks. *The Guardian*. Retrieved from Lexis/Nexis.
- Radack, J. & McClellan, K. (2011). The Criminalization of Whistleblowing. *The Labor & Employment Law Forum* (2)1, 57-77.
- Rado, N. (2011). *On Wikileaks and Diplomacy: Secrecy and Transparency in the Digital Age*. Retrieved from http://www.etd.ceu.hu/2011/rado_nora.pdf
- Reuters. (2015, June 15). Britain pulls spies; Snowden leaks cited. *The Washington Post*. Retrieved from Lexis/Nexis.
- Richelson, J.T. (2012). Intelligence Secrets and Unauthorized Disclosures: Confronting Some Fundamental Issues. *International Journal of Intelligence and CounterIntelligence* 25(4), 639-677. doi: 0.1080/08850607.2012.705184
- Richelson, J.T. (1999). *The U.S. Intelligence Community*. Boulder, CO: Westview Press.
- Right Livelihood. (2014). *The Right Livelihood Award: for outstanding vision and work on behalf of our planet and its people*. Retrieved from <http://www.rightlivelihood.org/snowden.html>

- Risen, J. (2009). Media Incentives and National Security Secrets. *Harvard University Law Review* 122(8). 2228-2249. Retrieved from <http://www.harvardlawreview.org/issues/122/june09/index.php>
- Risen, J. (2013, October 18). Snowden Says He Took No Secret Files to Russia. *The New York Times*. Retrieved from Lexis/Nexis.
- Risen, J. & Lichtblau, E. (2013, June 9). How the U.S. Uses Technology to Mine More Data More Quickly. *The New York Times*. Retrieved from Lexis/Nexis.
- Risen, J. & Poitras, L. (2013, November 23). N.S.A. Report Outlined Goals for More Power. *The New York Times*. Retrieved from Lexis/Nexis.
- Roberts, D. (2013, June 10). Edward Snowden's explosive NSA leaks have US in damage control mode. *The Guardian*. Retrieved from Lexis/Nexis.
- Rogers, M. (2013, October 10). 'A very dangerous time'. *The Washington Post*. Retrieved from Lexis/Nexis.
- Ross, G. (2011). *Who watches the watchmen? The conflict between national security and freedom of the press*. Washington, D.C.: National Intelligence University.
- Sagar, R. (2009). Who holds the balance? A missing detail in the debate over balancing security and liberty. *Polity*, 41(2), 166-188. doi:10.1057/pol.2008.27
- Sales, N. A. (2012). Self-Restraint and National Security. *Journal of National Security Law & Policy*, 6(1), 227-289. Retrieved from <http://jnslp.com/topics/read/vol-6-no-1/>
- Sales, N. A. (2010). Share and Share Alike: Intelligence Agencies and Information Sharing. *The George Washington Law Review*, 78(2), 279-352. Retrieved from <http://www.gwlr.org/print/volume-78-number-2/>
- Samuelson, R. J. (2014, January 6). Snowden's dubious legacy. *The Washington Post*. Retrieved from Lexis/Nexis.
- Sangarasivam, Y. (2013). Cyber Rebellion: Bradley Manning, WikiLeaks, and the Struggle to Break the Power of Secrecy in the Global War on Terror. *Perspectives on Global Development and Technology* 12(1-2), 69-79. DOI: 10.1163/15691497-12341243
- Sanger, D. & Smale, A. (2013, December 17). U.S.-Germany Intelligence Partnership Falters Over Spying. *The New York Times*. Retrieved from Lexis/Nexis.

- Schaffert, R. W. (1992). *Media Coverage and Political Terrorists A QUANTITATIVE ANALYSIS*. Westport, CT: Praeger Publishers. Retrieved from Praeger Security International Online database.
- Schmitt, E. & Hubbard, B. (2015, July 21). ISIS Leader Takes Steps to Ensure Group's Survival. *The New York Times*. Retrieved from Lexis/Nexis.
- Schneier, B. (2015). *Schneier on Security*. Retrieved from <https://www.schneier.com>
- Schneier, B. (2014). *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2014/10/nsa_classificat.html
- Schoenfeld, G. (2013). Journalism or Espionage? *National Affairs* 17, 53-68. Retrieved from www.nationalaffairs.com
- Schoenfeld, G. (2011). *Necessary secrets: National security, the media, and the rule of law*. New York: W. W. Norton.
- Schulhofer, S. (2013). Oversight of national security secrecy in the United States. *NYU School of Law, Public Law Research Paper No. 13-21*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2258539
- Sedler, R. A. (2007). The Media and National Security. *Wayne State University Law School Legal Studies Research Paper Series*. Retrieved from <http://ssrn.com/abstract=1154069>
- Sedler, R.A., (2011) Self-Censorship and the First Amendment. *Notre Dame Journal of Law, Ethics, and Public Policy*, 25(1), 13-45. Retrieved from www.nd.edu/~ndlaw/jlepp/journals/25-Censorship.pdf
- Setty, S. (2012). The Rise of National Security Secrets. *Connecticut Law Review* 44(5), 1563-1583. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2113640
- Shane, S. (2013a, June 22). Leaker Charged With Violating Espionage Act. *The New York Times*. Retrieved from Lexis/Nexis.
- Shane, S. (2013b, August 30). New Leaked Document Outlines U.S. Spending On Intelligence Agencies. *The New York Times*. Retrieved from Lexis/Nexis.
- Silberman, L. & Robb, C. (2005). *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*. Washington, D.C.: Government Printing Office.
- Silver, D. A., (2008). National Security and the Press: The Government's Ability to Prosecute Journalists for the Possession or Publication of National Security

Information. *Communication Law and Policy* 13(4), 447-483.
doi:10.1080/10811680802388881

- Slobogin, C. (2012). Making the most of United States V. Jones in a surveillance society: A statutory implementation of Mosaic Theory. *Duke Journal of Constitutional Law & Public Policy* 8(1), 1-37. Retrieved from <http://scholarship.law.duke.edu/djclpp/vol8/iss1/1/>
- Smale, A. (2015, May 8). Germany Limits Cooperation with U.S. Over Data Gathering. *The New York Times*. Retrieved from Lexis/Nexis.
- Smolkin, R. (2006). Judgment Calls. *American Journalism Review* 28(5), 22-31. Retrieved from <http://www.ajr.org/Article.asp?id=4185>
- Somaiya, R. (2013, December 4). Editor Describes Pressure After Leaks by Snowden. *The New York Times*. Retrieved from Lexis/Nexis.
- Stake, R.E. (1995). *The Art of Case Study Research*. Thousand Oaks, CA.: SAGE Publications.
- Stan, L. (2010). Archival Records as Evidence. *Encyclopedia of Case Study Research*. Retrieved from <http://dx.doi.org/10.44135/9781412957397.n12>
- Stone, G. (2007). *Prosecuting the Press for Publishing Classified Information*. Retrieved from <https://www.law.upenn.edu/institutes/cerl/conferences/ethicsofsecrecy/reading.html>
- Stone, G. (2011). WikiLeaks, the proposed SHIELD act, and the first amendment. *Journal of National Security Law & Policy*, 5(1), 1-14. Retrieved from <http://search.proquest.com/docview/872471489?accountid=28180>
- Sutter, D. (2001). Can the Media be so Liberal? The Economics of Media Bias. *CATO Journal* 20(3), 431-451. Retrieved from <http://object.cato.org/sites/cato.org/files/serials/files/cato-journal/2001/1/cj20n3-7.pdf>
- Taylor, M. (2014, March 31). Snowden leaks prompt firms to quit 'cloud' data storage: Study reveals surveillance fears over US-run services: Shift may hurt companies like Google and Facebook. *The Guardian*. Retrieved from Lexis/Nexis.
- Travis, A. (2013, September 20). Data chief to investigate surveillance disclosures. *The Guardian*. Retrieved from Lexis/Nexis.
- Travis, A. (2014, February 19). David Miranda detention at Heathrow airport was lawful, high court rules. *The Guardian*. Retrieved from Lexis/Nexis.

- Travis, A. & Roberts. D. (2013, June 11). Front: Europe demands answers from Obama over surveillance by US. *The Guardian*. Retrieved from Lexis/Nexis.
- Traynor, I. (2013a, October 25). Germany and France warn NSA spying fallout jeopardises fight against terror. *The Guardian*. Retrieved from Lexis/Nexis.
- Traynor, I. (2013b, June 30). Key US-EU trade pact under threat after more NSA spying allegations. *The Guardian*. Retrieved from Lexis/Nexis.
- Traynor, I. (2013c, October 25). Spying on friends is intolerable, says Merkel amid German backlash at US: Chancellor and Hollande to co-ordinate response: UK stalls French push for new data protection rules. *The Guardian*. Retrieved from Lexis/Nexis.
- Udo-Akang, D. (2012). Theoretical Constructs, Concepts, and Applications. *American International Journal of Contemporary Research*, 2(9), 89-97.
- U.S. Const. amend. I.
- U.S. Defense Intelligence Agency. (2013). *DOD Information Review Task Force-2: Initial Assessment*. Retrieved from <http://s3.documentcloud.org/documents/1165528/tf-2-initial-assessment-copy-for-release.pdf>
- U.S. National Security Agency (2016). *Frequently Asked Questions: Terms and Acronyms*. Retrieved from https://www.nsa.gov/about/faqs/terms_acronyms.shtml
- U.S. Office of the Director of National Intelligence. (2011). *U.S. National Intelligence: An Overview 2011*. Retrieved from www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf
- U.S. Senate. (1997). Report of the Commission on Protecting and Reducing Government Secrecy. *Senate Document 105-2*. Washington, DC: United States Government Printing Office. Retrieved from <http://www.gpo.gov/congress/commissions/secrecy/>
- U.S. White House. (2009). *Executive Order 13526 – Classified National Security Information*. Retrieved from <https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>
- Vladeck, S.I. (2012). Democratic Competence, Constitutional Disorder, and the Freedom of the Press. *Washington Law Review* 8(2), 529-548. Retrieved from <https://digital.law.washington.edu/dspace-law/handle/1773.1/1141>
- Vladeck, S. I. (2008). The Espionage Act and National Security Whistleblowing after Garcetti. *American University Law Review* 57(5), 1531-1546. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1315344

- Vladeck, S. I. (2007). Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press. *Harvard Law & Policy Review*, 1(1), 219-237.
- Vogel, R. (2010). Parallel, transformer or collaboration strategy of relating theory to practice? A case study of public management debate in Germany. *Public Administration*, 88(3), 680-705. doi:10.1111/j.1467-9299.2010.01828.x
- Wacker, J.G. (1998). A definition of theory: research guidelines for different theory-building research methods in operations management. *Journal of Operations Management*, 16, 361-385.
- Washington Post. (2013a, October 23). Common Sense on Spying. Retrieved from Lexis/Nexis.
- Washington Post. (2013b, September 30). Information needs a shield. Retrieved from Lexis/Nexis.
- Washington Post. (2013c, July 2). Plug these leaks. Retrieved from Lexis/Nexis.
- Watt, N. (2013, October 11). Guardian 'naive and arrogant' to publish Snowden articles, says Straw. *The Guardian*. Retrieved from Lexis/Nexis.
- Weaver, W. G. & Pallitto, R.M. (2005). State Secrets and Executive Power. *Political Science Quarterly*, 120(1) 85-112. Retrieved from <http://www.psqonline.org/article.cfm?IDArticle=15101>
- White, H. A. (1996). The Salience and Pertinence of Ethics: When Journalists Do and Don't Think for Themselves. *Journalism and Mass Communication Quarterly*, 73(1), 17-28. Retrieved from <http://search.proquest.com.proxy1.ncu.edu/docview/1009905193?accountid=28180>
- Wilson, V. (2007). *Fair Game: How a top CIA agent was betrayed by her own government*. New York: Simon & Schuster.
- Wirtz, J. (2010). The Sources and Methods of Intelligence Studies [Abstract]. In L.K. Johnson (Ed.), *The Oxford Handbook of National Security Intelligence*. doi: 10.1093/oxfordhb/9780195375886.003.0004
- Yin, R.K. (2012). *Applications of Case Study Research*. Thousand Oaks, California: SAGE
- Yin, R.K. (2014). *Case Study Research: Design and Methods*. Thousand Oaks, California: SAGE

Appendixes

Appendix A: Study Findings References

Appendix A: Study Findings References

1. Pincus, W. (2013, December 19). Snowden still holding a 'road map' for U.S. adversaries. *The Washington Post*. Retrieved from Lexis/Nexis.
2. Pincus, W. (2014, February 11). Facts not cooling outrage over NSA. *The Washington Post*. Retrieved from Lexis/Nexis.
3. O'Carroll, L., Booth, R. & Watt, N. (2013, August 24). Snowden leaks: Guardian deal with New York Times. *The Guardian*. Retrieved from Lexis/Nexis.
4. Nakashima, E. & Miller, G. (2013, June 25). U.S. is worried about security of documents Snowden has. *The Washington Post*. Retrieved from Lexis/Nexis.
5. Hopkins, N. (2013b, October 9). MI5 chief's criticism of Snowden and the Guardian is hardly unexpected. *The Guardian*. Retrieved from Lexis/Nexis.
6. Booth, R. (2013, August 13). David Miranda: police win wider powers to investigate seized data. *The Guardian*. Retrieved from Lexis/Nexis.
7. Taylor, M. & Ball, J. (2013, December 2). The Snowden files: Inside the surveillance state: Decoded: Revelations about mass surveillance by the NSA and GCHQ have shocked some and embarrassed others. Here we outline the main stories, what they mean and why they matter. *The Guardian*. Retrieved from Lexis/Nexis.
8. Ball, J., Borger, J. & Greenwald, G. (2013, September 6). Front: Exclusive: how US and Britain unlock privacy on the internet: Elaborate safeguards broken by NSA and GCHQ: Encryption meant to protect emails, bank and medical records: New Snowden revelations certain to cause political row. *The Guardian*. Retrieved from Lexis/Nexis.
9. Traynor, I. (2013b, June 30). Key US-EU trade pact under threat after more NSA spying allegations. *The Guardian*. Retrieved from Lexis/Nexis.
10. Miller, G., Tate, J. & Gellman, B. (2013, October, 17). NSA role in drone strikes is revealed. *The Washington Post*. Retrieved from Lexis/Nexis.
11. Cole, D. (2014, May 18). NSA mantra: 'Collect it all . . . know it all'. *The Washington Post*. Retrieved from Lexis/Nexis.
12. Gellman, B., & Nakashima, E. (2013, August, 31). 'Black budget' details a war in cyberspace. *The Washington Post*. Retrieved from Lexis/Nexis.

13. Schneier, B. (2014, February 28). Comment: The naked truth behind the NSA's doublespeak: The agency has claimed it's not been collecting data on us. But the Yahoo revelations expose the violation of our privacy. *The Guardian*. Retrieved from Lexis/Nexis.
14. Scott, M., & Breeden, A. (2015, February 26). Spy Agencies May Have Sought SIM Encryption Codes. *The New York Times*. Retrieved from Lexis/Nexis.
15. Bolton, J. (2013, June 18). Edward Snowden's leaks are a grave threat to US national security. *The Guardian*. Retrieved from Lexis/Nexis.
16. Gellman, B., & Nakashima, E. (2013, August, 31). 'Black budget' details a war in cyberspace. *The Washington Post*. Retrieved from Lexis/Nexis.
17. Gellman, B. & Miller, G. (2013, August 30). 'Black budget' summary details U.S. spy network's successes, failures and objectives. *The Washington Post*. Retrieved from Lexis/Nexis.
18. Boycott, O. (2014, May 13). GCHQ's spy malware operation faces legal challenge. *The Guardian*. Retrieved from Lexis/Nexis.
19. Hopkins, N. (2013, December 2). The Snowden files: Inside the surveillance state: From: Turing to Tempora: The US-UK intelligence pact, forged in the second world war, has evolved beyond the two governments' control - and perhaps even their understanding. *The Guardian*. Retrieved from Lexis/Nexis.
20. Shane, S. (2013, November 3). No Morsel Too Minuscule for All-Consuming N.S.A. *The New York Times*. Retrieved from Lexis/Nexis.
21. Gellman, B., & Nakashima, E. (2013, August, 31). 'Black budget' details a war in cyberspace. *The Washington Post*. Retrieved from Lexis/Nexis.
22. Ball, J., Borger, J. & Greenwald, G. (2013, September 6). Front: Exclusive: how US and Britain unlock privacy on the internet: Elaborate safeguards broken by NSA and GCHQ: Encryption meant to protect emails, bank and medical records: New Snowden revelations certain to cause political row. *The Guardian*. Retrieved from Lexis/Nexis.
23. Pincus, W. (2015, June 9). Another bum rap for the NSA. *The Washington Post*. Retrieved from Lexis/Nexis.

24. Rushe, D. (2015, February 20). Sim card database hack gave US and UK spies access to billions of cellphones; International row likely after revelations of breach that could have given NSA and GCHQ the power to monitor a large portion of world's cellular communications. *The Guardian*. Retrieved from Lexis/Nexis.
25. Roberts, D. (2013, August 23). NSA analysts deliberately broke rules to spy on Americans, agency reveals. *The Guardian*. Retrieved from Lexis/Nexis.
26. Black, I. (2013, June 10). NSA spying scandal: what we have learned. *The Guardian*. Retrieved from Lexis/Nexis.
27. Miller, G., Tate, J. & Gellman, B. (2013, October, 17). NSA role in drone strikes is revealed. *The Washington Post*. Retrieved from Lexis/Nexis.
28. Nakashima, E., Gellman, B. & Miller, G. (2013, June 21). Documents reveal bounds of NSA's secret programs. *The Washington Post*. Retrieved from Lexis/Nexis.
29. Mattingly, P. (2013, June 20). FBI chief admits agency uses drones in domestic surveillance FBI chief admits agency uses drones in domestic surveillance. *The Washington Post*. Retrieved from Lexis/Nexis.
30. Rich, S. & Gellman, B. (2014, January 3). NSA aims to crack most online codes. *The Washington Post*. Retrieved from Lexis/Nexis.
31. Nakashima, E. (2013, June 16). Only a few hundred people's records were reviewed, U.S. says. *The Washington Post*. Retrieved from Lexis/Nexis.
32. Nakashima, E. (2013, August 22). NSA collected thousands of domestic e-mails. *The Washington Post*. Retrieved from Lexis/Nexis.
33. Devereaux, R., Greenwald, G. & Poitras, L. (2014, May 19). Data Pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas. *The Intercept*. Retrieved from <https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/>
34. Miller, G., Tate, J. & Gellman, B. (2013, October, 17). NSA role in drone strikes is revealed. *The Washington Post*. Retrieved from Lexis/Nexis.
35. Taylor, M. & Ball, J. (2013, December 2). The Snowden files: Inside the surveillance state: Decoded: Revelations about mass surveillance by the NSA and GCHQ have shocked some and embarrassed others. Here we outline the main

- stories, what they mean and why they matter. *The Guardian*. Retrieved from Lexis/Nexis.
36. Gellman, B., Soltani, A. & Peterson, A. (2013, November 4). What Yahoo and Google did not think the NSA could see. *The Washington Post*. Retrieved from <http://apps.washingtonpost.com/g/page/world/what-yahoo-and-google-did-not-think-the-nsa-could-see/555/#document/p6/a130015>
 37. Gellman, B., Tate, J. & Soltani, A. (2014, July 6). Caught up in the NSA net. *The Washington Post*. Retrieved from Lexis/Nexis.
 38. Miller, G. & Horwitz, S. (2013, June 14). U.S. officials fear leaker has more classified files. *The Washington Post*. Retrieved from Lexis/Nexis.
 39. Gellman, B. (2013, August 15). NSA broke privacy rules thousands of times per year, audit finds. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html
 40. Greenwald, G. & Maurizi, S. (2013, December 5). Revealed: How the NSA Targets Italy. *l'Espresso*. Retrieved from http://espresso.repubblica.it/inchieste/2013/12/05/news/revealed-how-the-nsa-targets-italy-1.144428?refresh_ce
 41. Devereaux, R., Greenwald, G. & Poitras, L. (2014, May 19). Data Pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas. *The Intercept*. Retrieved from <https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/>
 42. MacAskill, E. (2013, June 30). New NSA leaks show how US is bugging its European allies. *The Guardian*. Retrieved from Lexis/Nexis.
 43. MacAskill, E. (2013, June 21). How does GCHQ's internet surveillance work? *The Guardian*. Retrieved from Lexis/Nexis.
 44. Priest, D. (2013, July 22). At NSA, a boom fed by post-9/11 demands. *The Washington Post*. Retrieved from Lexis/Nexis.
 45. Rushe, D. (2013, October 30). Google and Yahoo furious over reports that NSA secretly intercepts data links. *The Guardian*. Retrieved from Lexis/Nexis.

46. Black, I. (2013, June 10). NSA spying scandal: what we have learned. *The Guardian*. Retrieved from Lexis/Nexis.
47. Der Spiegel. (2014, June 18). The NSA in Germany: Snowden's Documents Available for Download. *SPIEGEL Online*. Retrieved from <http://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html>
48. Nippert, M. (2015, March 11). UK Foreign Secretary Philip Hammond says it's time to 'move on' from Snowden. *The New Zealand Herald*. Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11415169
49. Laughland, O. (2013, August 19). Pine Gap's role in US drone strikes should be investigated - rights groups. *The Guardian*. Retrieved from Lexis/Nexis.
50. Gallagher, R. & Greenwald, G. (2014, March 12). How the NSA Plans to Infect 'Millions' of Computers with Malware. *The Intercept*. Retrieved from <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>
51. Devereaux, R., Greenwald, G. & Poitras, L. (2014, May 19). Data Pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas. *The Intercept*. Retrieved from <https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/>
52. Priest, D. (2013, July 22). At NSA, a boom fed by post-9/11 demands. *The Washington Post*. Retrieved from Lexis/Nexis.
53. Timberg, C. (2013, July 11). Slide shows NSA surveillance of data from undersea cables. *The Washington Post*. Retrieved from Lexis/Nexis.
54. Cole, D. (2014, May 18). NSA mantra: 'Collect it all . . . know it all'. *The Washington Post*. Retrieved from Lexis/Nexis.
55. Nakashima, E. (2013, October 25). NSA documents could expose joint operations. *The Washington Post*. Retrieved from Lexis/Nexis.
56. Risen, J. & Poitras, L. (2013, November 23). N.S.A. Report Outlined Goals for More Power. *The New York Times*. Retrieved from Lexis/Nexis.
57. Lewis, P. (2013, October 28). NSA review panel to present Obama with dossier on surveillance reforms. *The Guardian*. Retrieved from Lexis/Nexis.

58. Obermaier, F., Moltke, H., Poitras, L. & Strozyk, J. (2014, November 25). Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts. *Süddeutsche Zeitung*. Retrieved from <http://international.sueddeutsche.de/post/103543418200/snowden-leaks-how-vodafone-subsubsidiary-cable>
59. Poitras, L., Rosenbach, M., Schmid, F., Stark, H. & Stock, J. (2013, July 1), Cover Story: How the NSA Targets Germany and Europe. *Der Spiegel*. Retrieved from <http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html>
60. Dredge, S. (2014, December 5). Live from The Logan Symposium: secrecy, surveillance and censorship; From Wikileaks and Edward Snowden to investigative journalism and the future of hacking, London event gets underway. *The Guardian*. Retrieved from Lexis/Nexis.
61. Sparrow, A. (2013, November 10). Guardian faces fresh criticism over Edward Snowden revelations. *The Guardian*. Retrieved from Lexis/Nexis.
62. Schmitt, E. & Hubbard, B. (2015, July 20). ISIS Leader Takes Steps to Ensure Group's Survival. *The New York Times*. Retrieved from http://www.nytimes.com/2015/07/21/world/middleeast/isis-strategies-include-lines-of-succession-and-deadly-ring-tones.html?_r=0
63. Ball, J., Borger, J. & Greenwald, G. (2013, September 6). Front: Exclusive: how US and Britain unlock privacy on the internet: Elaborate safeguards broken by NSA and GCHQ: Encryption meant to protect emails, bank and medical records: New Snowden revelations certain to cause political row. *The Guardian*. Retrieved from Lexis/Nexis.
64. Appelbaum, J., Horchert, J. & Stocker, C. (2013, December 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. *Der Spiegel*. Retrieved from <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>
65. Maass, P. & Poitras, L. (2014, October 10). Core Secrets: NSA Saboteurs in China and Germany. *The Intercept*. Retrieved from <https://theintercept.com/2014/10/10/core-secrets/>
66. Priest, D. (2013, July 22). At NSA, a boom fed by post-9/11 demands. *The Washington Post*. Retrieved from Lexis/Nexis.

67. Hamilos, P. (2013, October 28). Spain summons US ambassador over claim NSA tracked 60m calls a month. *The Guardian*. Retrieved from Lexis/Nexis.
68. Greenwald, G. & MacAskill, E. (2013, June 11). Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian*. Retrieved from <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>
69. Gallagher, R. (2014, August 25). The Surveillance Engine: How the NSA Built Its Own Secret Google. *The Intercept*. Retrieved from <https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>
70. Gellman, B. & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
71. Ball, J., Borger, J. & Greenwald, G. (2013, September 6). Front: Exclusive: how US and Britain unlock privacy on the internet: Elaborate safeguards broken by NSA and GCHQ: Encryption meant to protect emails, bank and medical records: New Snowden revelations certain to cause political row. *The Guardian*. Retrieved from Lexis/Nexis.
72. Perloth, N., Larson, J. & Shane, S. (2013, September 5). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*. Retrieved from <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>
73. Norton-Taylor, R. & Cobain, I. (2013, October 17). Surveillance: 'Our national security is at risk' ... the empty threat to justify suppression: For as long as security services have kept secrets they have deployed the dire consequences of disclosure to silence and convict whistleblowers, but as Richard Norton-Taylor and Ian Cobain report, these claims seldom stand up to scrutiny. *The Guardian*. Retrieved from Lexis/Nexis.
74. Ignatius, D. (2014, July 23). Partners in spying, *The Washington Post*. Retrieved from Lexis/Nexis.
75. Laughland, O. (2013, November 19). Intelligence gathering: Indonesia: Ambassador recalled over Australian attempts to listen to leaders' calls. *The Guardian*. Retrieved from Lexis/Nexis.

76. Gallagher, R. (2014, August 25). The Surveillance Engine: How the NSA Built Its Own Secret Google. *The Intercept*. Retrieved from <https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>
77. Aranda, G. (2013, November 4). Claves y giros del espionaje masivo en España: Los gobiernos europeos pasan de la indignación a preguntar a sus servicios de inteligencia. *El Mundo*. Retrieved from <http://www.elmundo.es/internacional/2013/11/04/52769eb561fd3d6d0a8b4582.html>
78. Gallagher, R. (2014, August 25). The Surveillance Engine: How the NSA Built Its Own Secret Google. *The Intercept*. Retrieved from <https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>
79. Hamilos, P & Chrisafis, A. (2013, October 31). Snowden leaks: Spanish intelligence services 'helped NSA surveillance operations in Spain': Papers suggest France swapped data with US: German delegation vents anger over Merkel bugging. *The Guardian*. Retrieved from Lexis/Nexis.
80. Poitras, L., Rosenbach, M., Sontheimer, M. & Stark, H. (2014, August 31). A Two-Faced Friendship: Turkey Is 'Partner and Target' for the NSA. *Der Spiegel*. Retrieved from <http://www.spiegel.de/international/world/documents-show-nsa-and-gchq-spied-on-partner-turkey-a-989011.html>
81. Müller-Maguhn, A., Poitras, L., Rosenbach, M., Sontheimer, M. & Grothoff, C. (2014, September 14). Treasure Map: The NSA Breach of Telekom and Other German Firms. *Der Spiegel*. Retrieved from <http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html>
82. Rensfeldt, G. (2013, December 11). Uppdrag Granskning: Read the Snowden Documents from the NSA. *Sveriges Television*. Retrieved from <http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa>
83. Nippert, M. (2015, March 11). UK Foreign Secretary Philip Hammond says it's time to 'move on' from Snowden. *NZ Herald*. Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11415169
84. Greenwald, G. (2014, August 4). Cash, Weapons and Surveillance: The U.S. is a Key Party to Every Israeli Attack. *The Intercept*. Retrieved from <https://theintercept.com/2014/08/04/cash-weapons-surveillance/>

85. Ball, J. (2013, October 24). NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*. Retrieved from Lexis/Nexis.
86. Smale, A., Eddy, M. & Sanger, D. (2013, October 13). Data Suggests Push to Spy on Merkel Dates to '02. *The New York Times*. Retrieved from <http://www.nytimes.com/2013/10/28/world/europe/data-suggests-push-to-spy-on-merkel-dates-to-02.html>
87. Anonymous. (2013, September 2). Veja os documentos ultrassecretos que comprovam espionagem a Dilma. *O Globo Fantástico*. Retrieved from <http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html>
88. Cole, D. (2014, May 18). NSA mantra: 'Collect it all . . . know it all'. *The Washington Post*. Retrieved from Lexis/Nexis.
89. MacAskill, E. (2014, July 1). NSA chief plays down damage done to intelligence by Snowden leaks. *The Guardian*. Retrieved from Lexis/Nexis.
90. Bell, E. (2013, December 16). Media: A year of fireworks for the NSA and BBC: Austerity and the digital era have forced big changes on to the media, with new partnerships and bold decisions the keys to delivering quality journalism in the new world. *The Guardian*. Retrieved from Lexis/Nexis.
91. Hopkins, N. (2013, October 9). MI5 chief's criticism of Snowden and the Guardian is hardly unexpected. *The Guardian*. Retrieved from Lexis/Nexis.
92. Castle, S. (2013, June 11). Accused of Scheming with U.S., Britain Says It Follows the Law in Gathering Intelligence. *The New York Times*. Retrieved from Lexis/Nexis.
93. Boycott, O. (2015, July 2). GCHQ spied on Amnesty International, tribunal tells group in email; Human rights group denounces revelation as outrageous as after Investigatory Powers Tribunal says its communications have been illegally retained. *The Guardian*. Retrieved from Lexis/Nexis.
94. Mason, R. (2015, March 13). Intelligence and security committee report: the key findings; The landmark report calls for a total overhaul of laws governing Britain's intelligence agencies. *The Guardian*. Retrieved from Lexis/Nexis.
95. Fahrenholt, D.A. (2013, July 29). With leak, Wyden can at last name his crusade. *The Washington Post*. Retrieved from Lexis/Nexis.

96. Wintour, P. (2014, March 3). Front: Labour plans to overhaul controls over spy agencies. *The Guardian*. Retrieved from Lexis/Nexis.
97. Bolton, J. (2013, June 18). Edward Snowden's leaks are a grave threat to US national security. *The Guardian*. Retrieved from Lexis/Nexis.
98. Bell, E. (2013, December 16). Media: A year of fireworks for the NSA and BBC: Austerity and the digital era have forced big changes on to the media, with new partnerships and bold decisions the keys to delivering quality journalism in the new world. *The Guardian*. Retrieved from Lexis/Nexis.
99. Sanger, D. (2013, August 4). A Washington Riddle: What Is 'Top Secret'? *The New York Times*. Retrieved from Lexis/Nexis.
100. Nakashima, E. (2013, December 22). U.S. reasserts need to keep details of domestic surveillance secret. *The Washington Post*. Retrieved from Lexis/Nexis.