

10-29-2007

Negative Information Action: Assaulting Citizen Choice by Subverting the Democratic Process

Christopher L. Hinson
Florida State University

Follow this and additional works at: <http://diginole.lib.fsu.edu/etd>

Recommended Citation

Hinson, Christopher L., "Negative Information Action: Assaulting Citizen Choice by Subverting the Democratic Process" (2007).
Electronic Theses, Treatises and Dissertations. Paper 4032.

This Dissertation - Restricted Access is brought to you for free and open access by the The Graduate School at DigiNole Commons. It has been accepted for inclusion in Electronic Theses, Treatises and Dissertations by an authorized administrator of DigiNole Commons. For more information, please contact lib-ir@fsu.edu.

THE FLORIDA STATE UNIVERSITY

COLLEGE OF INFORMATION

NEGATIVE INFORMATION ACTION: ASSAULTING CITIZEN CHOICE BY
SUBVERTING THE DEMOCRATIC PROCESS

By

CHRISTOPHER L. HINSON

A Dissertation submitted to the
College of Information
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Degree Awarded:
Fall Semester, 2007

Copyright © 2007
Christopher L. Hinson
All Rights Reserved

The members of the Committee approve the dissertation of Christopher L. Hinson defended on October 29, 2007.

Corinne Jörgensen
Professor Directing Dissertation

Lance deHaven-Smith
Outside Committee Member

Michelle Kazmer
Committee Member

Paul Marty
Committee Member

Approved:

Larry Dennis, Dean, College of Information

The Office of Graduate Studies has verified and approved the above named committee members.

This dissertation is dedicated to my family and friends.

ACKNOWLEDGEMENTS

I want to acknowledge my committee members, Dr. Corinne Jörgensen, Dr. Michelle Kazmer, Dr. Paul Marty and especially Dr. Lance deHaven-Smith for their support and guidance. I also wish to thank Janet Capps and Delores Bryant for their editorial assistance.

TABLE OF CONTENTS

LIST OF TABLES	viii
LIST OF FIGURES	ix
ABSTRACT	x
INTRODUCTION	1
Statement of the Problem.....	2
Study Purpose	3
Significance of the Problem.....	4
Importance of the Study.....	5
Background of the Study	6
Research Goal	7
Definitions.....	7
Study Assumptions	9
Study Limitations.....	9
Summary	10
LITERATURE REVIEW	12
United States Secrecy Structure.....	12
United States Constitution	13
Legislation – Early America to World War II	13
Legislation – The Cold War.....	13
The Freedom of Information Act – Pre-September 11, 2001	15
Legislation – Post-September 11, 2001	16
The Freedom of Information Act – Post-September 11, 2001.....	17
Presidential Executive Orders – 1940 to 1970.....	18
Presidential Executive Order – 1970 to Present	19
Governmental Oversight – 1955 to 1958.....	21
Governmental Oversight – 1970 to 1997	22
Enlightened Citizen Understanding	23
Democratic Imperative.....	24
Bureaucratic Dilemma	25
Government Tactics	25
Consequences for Democracy.....	26
Secrecy Moderation	27
Open Politics	27
Whistleblowing.....	28
Unauthorized Disclosure.....	28
Recommendations	29
Conspiracies	30
Conspiracy Doctrine and Theory	31
Secrecy	33
Iran-Contra Affair	34
Nicaraguan Covert Operation	35
The Secret Iran Initiative	38

Summary	45
Research Questions	46
RESEARCH METHODOLOGY	47
Sensitive Research	47
Definitions.....	48
Sensitive Areas.....	48
Ethical and Political Issues	48
Issues Relevant to Current Study	49
Conspiracy Research.....	50
Errant Data Analysis	50
Sociological Method	51
Historical Analysis.....	51
Factor Analysis	52
Grounded Theory Research	53
Definitions.....	53
Purpose and Goals.....	53
Research Approaches.....	53
Preliminary Grounded Theory Research Inclinations.....	54
Initial Topic Selection and Sensitizing Issues	55
Summary	56
APPROACH TO CURRENT STUDY	57
Data Validity	57
Data Reliability	58
Theoretical Relevance.....	59
Literature Review.....	59
Documentary Data	60
Note Taking	60
Memoing	61
Coding.....	61
Emergence and Saturation	62
Measures, Magnitude and Predictive Value	63
DATA ANALYSIS AND FINDINGS	65
Initial Coding: Literature Review	65
Subject Qualification and Selection.....	66
Negative Information Actions Analysis.....	67
Objectives	67
Methods.....	68
Information Technology	73
Knowledge Support	74
Sample Analyses	76
Method Codes	76
Knowledge Support Codes	76
LEGAL ENVIRONMENT – IMPEDIMENTS TO INFORMATION FLOW	80
Privileged Information.....	80
Immunized Information	81
Classified Information	82

Timed Information	83
Terminated Information	84
PIGDEN, ABBATE AND DAHL REVISITED	85
Pigden: Conspiracy Theory	85
Abbate: Conspiracy Doctrine	88
Dahl: Democratic Theory	89
THEORETICAL FRAMEWORK AND MODEL	92
CONCLUSIONS AND RECOMMENDATIONS	96
FUTURE RESEARCH	98
APPENDIX A: ANALYSIS DATA	101
APPENDIX B: GLOSSARY	120
REFERENCES	123
BIOGRAPHICAL SKETCH	128

LIST OF TABLES

Table 1: Sample Negative Information Action Analysis No. 1	77
Table 2: Sample Negative Information Action Analysis No. 2	78
Table 3: Sample Negative Information Action Analysis No. 3	79
Table 4: Elliot Abrams, Assistant Secretary of State for Inter-American Affairs	101
Table 5: Duane R. Clarridge, CIA, Latin American Division Chief	102
Table 6: Joseph F. Fernandez, CIA Station Chief	103
Table 7: Allen Fiers, CIA Central American Task Force Chief	104
Table 8: Clair George, CIA Deputy Director for Operations	105
Table 9: Fawn Hall, National Security Council Staff	106
Table 10: Robert C. McFarlane, National Security Advisor	107
Table 11: Lieutenant Colonel Oliver North, USMC.....	109
Table 12: Vice-Admiral John Poindexter, USN	111
Table 13: Casper Weinberger, Secretary of Defense.....	112
Table 14: Negative Information Action Sorted by Knowledge Support	113
Table 15: Negative Information Actions Sorted by Method	115
Table 16: Negative Information Actions Using Information Technology.....	119

LIST OF FIGURES

Figure 1: Negative Information Action Model (Hinson, 2007).....	94
Figure 2: Example Using Negative Information Action Model (Hinson, 2007)	94

ABSTRACT

This dissertation explores evidence and provides insight to secrecy-related information actions that can and are sometimes used as a method to circumvent established government policy and law. These information actions may also be used to cover up such circumventions after the fact. To better understand secrecy as a negative information action and its impact on democracy, secrecy-related information actions are described according to objectives, methods, the use of information technology and knowledge support. Negative information actions are willful and deliberate acts designed to keep government information from those in government and the public entitled to it. Negative information actions are not in accordance with either the rule of law or the system of checks and balances.

Negative information actions used by government officials to violate policies and laws during the Iran-Contra Affair are identified, analyzed and categorized by type. The impact of negative information actions on enlightened citizen understanding are demonstrated using the Negative Information Action Model by assigning a location according to type on a continuum of enlightened citizen understanding. Findings are compared with democratic theory, conspiracy doctrine and conspiracy theory. Conclusions and recommendations relating the legal environment as an impediment to information flow as it relates to public accountability and the rule of law are made.

INTRODUCTION

Government secrecy is necessary and problematic for American democracy. It is necessary to prevent information about the United States military capabilities and plans from falling into the hands of enemy nations and terrorists. It is problematic because it can pose a barrier to enlightened citizen choice in elections and effective congressional and judicial oversight of the executive branch.

In the United States a complex policy framework has been developed to manage government secrecy by balancing national security interests with the public's right to know what its government is doing. This secrecy structure has proven effective in circumstances where government officials are acting in good faith and where the decisions of government employees and administrators are properly reviewed by their superiors in the chain of command. The Watergate and Iran-Contra scandals, the Gulf of Tonkin deception, the secret wars in Laos and Cambodia and similar events have revealed this policy framework is vulnerable to misuse when high-ranking policy-makers seek to evade congressional oversight, hide criminal acts, conceal embarrassing information, silence critics, or manipulate popular perceptions of international incidents.

For purposes of this study, *information* is defined as the complete and unadulterated presentation of relevant facts to those groups and individuals with oversight responsibility in government. It may be viewed as either a process or the final product. Information access is the right to use information while information availability is the opportunity to use information. Also for purposes of this study a *negative information action* is a willful and deliberate act designed to keep government information from those in government and the public entitled to it. Information actions are not in accordance with either the rule of law or the system of checks and balances.

The provision of information to those entitled is required and expected from those possessing the information. The provision of requested information to those with oversight responsibilities is considered to be the norm. Actions used to prevent or delay the provision of information is an unexpected downward departure from the given norm. Departures from the norm, negative information actions, are subject to public

accountability and the rule of law. The constitutional checks and balances and the rule of law are in place to assure that government officials work inside the expected norm. Only departures from the given norms are subject to investigation, prosecution, and this study.

This dissertation analyzes negative information actions in the Iran-Contra Affair to better understand the origins and nature of such abuses so effective policies can be devised for preventing them from occurring and detecting them when they do. Although many crimes and policy violations have been well documented, little is known about negative information actions used to subvert the secrecy structure for unlawful activities.

Statement of the Problem

The men who wrote the United States Constitution recognized problems associated with government transparency when they drafted Article 1, Section 5 of the Constitution in 1787. This section instructs houses of the legislative branch to “keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their judgment require Secrecy...” (U.S. Constitution, 1787). This information policy instrument demonstrates citizen access to government information was expected from the nation’s beginning. The secrecy provision, while included to prevent the release of information sensitive or detrimental to the nation’s interests in its formative years when covert government activity was rare and simple, may have provided the precedent for future abuses of government secrecy not envisioned by the Constitution’s authors.

During the past five decades, Americans have learned about several secrecy-related clusters of government programs. Some have been rooted in conspiracies by public officials to evade Congressional directives, conduct domestic surveillance for purposes of partisan politics and/or cover up crimes or embarrassing information. The media typically refer to political crimes not as conspiracies but as *scandals*. The two most notorious and best documented of these scandals are Watergate and the Iran-Contra Affair. Other examples of conspiracies involving the secrecy structure include the

misrepresentation of intelligence findings in the Gulf of Tonkin incident and the burglary of Daniel Ellsberg's psychiatrist's office. Recently, officials in the administration of President George W. Bush leaked classified information to smear a critic of the administration's decision to invade Iraq in 2003.

As these examples demonstrate, even though various government policy instruments consisting of constitutional provisions and legislative acts have been established to create a legitimate government secrecy structure, abuses of secrecy can and have occurred nonetheless. The United States secrecy structure attempts to balance national security interests with a citizen's right to access government information needed to make informed decisions related to political participation. The attempt to balance security and openness in government is generally seen as an ongoing dilemma. Government secrecy in the United States is problematic for enlightened citizen choice in general elections and special referendums.

The aim of this research is to identify, scrutinize and amplify information and concepts not normally addressed in the information policy research related to government information access. The intent is to better understand the nature of departures from the established secrecy structure by examining the secrecy-related negative information actions of a conspiratorial group who circumvented policy and law.

Study Purpose

The purpose of this study is to examine and discuss the general form of secrecy as negative information actions to provide a better understanding of concepts related to secrecy and to identify conditions allowing government officials to use secrecy to conceal crimes or evade accountability to Congress or the public. The Iran-Contra Affair was chosen as the subject for a case study for several reasons. Firstly, of all secrecy-related conspiracies by public officials in the past five decades, the Iran-Contra Affair has been one of the most thoroughly investigated for purposes of prosecution. The crimes associated with the Watergate break-in did not receive the same level of scrutiny, because President Gerald Ford pardoned President Richard Nixon immediately after Nixon

resigned. Secondly, recent allegations involving the present Bush administration describe activities similar in essential ways to Iran-Contra. This suggests the Iran-Contra Affair may provide insight into enduring flaws in the secrecy structure. Thirdly, the Iran-Contra Affair offers numerous examples of nefarious individuals and groups providing false and misleading statements, carrying out unauthorized covert operations, making bold attempts to cover up, and other secrecy-related abuses.

Significance of the Problem

Balancing government secrecy and national security has been particularly challenging since the invention of atomic weapons and the subsequent Cold War. The government's secrecy structure, intended to keep a citizen's right to know in balance with the need to keep information from adversaries, continues to grow. Many times individuals and groups in government keep activities unknown from others in government and from the nation's citizens. While the established secrecy structure has procedures in place for determining the need to keep information from citizens, it does so under the authoritative guidance of information policy instruments established by law or administrative regulation.

Since the United States is considered to be a democratic society, its citizens expect transparency to conduct oversight of government officials and programs. Secrecy abuses have occurred so often they are now considered to be an unfortunate yet recognized phenomenon in government. Secrecy has a detrimental impact on citizen participation and government oversight in that a citizen's ability to identify, locate, comprehend, analyze, evaluate and utilize information related to government activity is diminished. Further, those negative information actions reducing a citizen's enlightened understanding, in turn, create problems for democracy and can lead to repeated policy failures. The similarity between the misuse and abuse of secrecy to secure passage of, on the one hand, the Gulf Tonkin of Resolution, and the Iraq war resolution in 2002, suggests the secrecy structure as it stands is not meeting the needs of democratic policymaking.

Those government officials who misuse or go outside the established secrecy structure undermine the rule of law and weaken the constitutional system of democratic checks and balances. Public policy studies must recognize and investigate these kinds of sinister and concealed policy activities and activities of an apparent and positive nature to fully describe or explain the causes and consequences of government policy, intended and unintended (Dye, 1976). Excessive government secrecy in the Reagan Era bred contempt for the democratic process and encouraged several individuals to believe they were beyond the reach of the law (Doyle, 1999). During this era several high-ranking and midlevel government employees conspired with civilians to conduct secret government activities and attempted to cover up their activities once exposed—the Iran Contra Affair.

Importance of the Study

The importance of this study as it relates to information science and public administration is that it addresses the secrecy structure and the uses and misuses of secrecy in a democratic society. Much federal information policy research relating to information access has been conducted within the confines of the established secrecy structure defined by policy instruments designed to regulate citizen access to government information. This study attempts to examine federal information actions beyond those normally addressed in the information policy literature. The literature generally overlooks the possibility the very highest officials in the United States government may subvert the legitimate secrecy structure to conceal unlawful acts, yet Watergate and Iran-Contra show this has been done. These conspiracies were uncovered because of fortuitous events—the Watergate burglars were caught when they returned to the Watergate hotel to repair a secretly planted eavesdropping device, and a Central Intelligence Agency operative was captured in Nicaragua because his airplane was shot down. These suggests that many other conspiracies of a similar nature may have been carried out but never detected.

This study is designed to explore evidence and provide insight about secrecy-related information actions that can and are sometimes used as a method to circumvent established government policy and law. These information actions may also be used to cover up such circumventions after the fact. To better understand secrecy as a negative information action, secrecy-related information actions are described according to factors such as objectives, methods, the use of information technology and knowledge support. While the current study may not be predictive or generalized outside its particular historical period, it is hoped it will bring meaning to sufficiently similar historical periods of democratic rule.

Background of the Study

The Iran-Contra scandal was the result of the exposure of two secret Reagan administration policies, the Iran initiative and the Contra operation, coordinated by the National Security Agency. The Iran initiative consisted of efforts to obtain the release of American hostages held in Beirut, Lebanon, by unlawfully selling weapons to Iran. The Contra operation consisted of efforts to unlawfully support Contra resistance and other paramilitary activities in Nicaragua. The profits made from the arms sales to Iran were used to support the Contra effort. In addition to the secret programs being unlawful, they were also against United States policy. The nation's stated policies were to not trade arms for hostages and to not subvert the democratically elected government of Nicaragua. The secret programs violating these policies were exposed in 1986, when a United States cargo plane was shot down while delivering military supplies to the Contras in October and again in November when a Lebanese newspaper reported the sale of arms to Iran (Walsh, 1993). If not for this chance exposure, the entire conspiracy might have remained forever undiscovered.

Not until November 1986 did Attorney General Edwin Meese announce there existed evidence to suggest the funds from the arms sale may have been diverted to support the Contra activities. The following month Meese appointed Lawrence E. Walsh as the independent counsel to investigate the allegations contained in the announcement

(Walsh, 1993). After the investigation, Walsh concluded in addition to other policy and law violations, government officials had systematically and willfully withheld large volumes of relevant documents from investigators and had deliberately deceived Congress and the public about the government's knowledge of and support for the alleged activities (Walsh, 1993).

The final report of the independent counsel contains information not previously known to investigators during the course of the investigation. President George H. W. Bush produced a diary previously withheld from investigators during the investigation revealing his and others' complicity in the Iran-Contra Affair. Bush later pardoned several individuals who would likely have testified about his involvement. The subsequently acquired information with these questionable pardons provided additional research material for the present study.

Research Goal

The goal of this study is to identify, scrutinize and amplify information and concepts not normally addressed in the information policy research related to government information access. The methodology used in this study is known as grounded theory research. It requires the researcher examine data and explore possible theoretical conditions grounded in the data. While the grounded theory research methodology precludes specific research questions or hypotheses, it is anticipated the methodology will produce results that will help to explore why, when, how and which government officials use secrecy-related information actions to circumvent government policies or laws.

Definitions

Conspiracy – a secret plan on the part of a group to unlawfully influence events partly by covert action (Pigden, 1995).

Enlightened understanding – “the principle of political equality assumes that the members are all equally well qualified to participate in decisions provided they have adequate opportunities to learn about matters before the association by inquiry, discussion and deliberation” (Dahl, 1998, p. 39).

Fully Prosecuted – for purposes of this study, refers to criminal cases not terminating on the basis of immunity, executive privilege, failure to declassify, pardons or the statute of limitations.

Information – for purposes of this study, is the complete and unadulterated presentation of relevant facts to those groups and individuals with oversight responsibility in government. It may be view as either a process of creating knowledge or the final product of a process (Buckland, 1991).

Information technology – for purposes of this study, any mechanical, electric or electronic device used to create, communicate, manipulate or destroy information.

Indictment – the formal written document originating with the prosecutor and issued by a grand jury containing allegations and criminal charges against an individual or group of conspirators (Black, 1983).

Negative information action – willful and deliberate act designed to keep government information from those in government and the public entitled to it; information actions not in accordance with either the rule of law or the system of checks and balances.

Secrecy – withholding government information from the public.

Transparency – openness in government activities and programs.

Withholding information – to suppress or destroy [information] knowing it may be wanted in a judicial or [congressional] proceeding (Black, 1983).

Study Assumptions

The following assumptions are relevant to this study:

1. Government conspiracies having been exposed and investigated are more likely to provide data directly related to the use of secrecy than government conspiracies that are suspected but have not been prosecuted.
2. The independent counsel's investigation and final report are thorough and accurate, and due diligence was exercised in their preparation.
3. Many of the acts or omitted acts of those charged in the indictment and those of others individuals not charged, adequately represent negative information actions undertaken outside the established secrecy structure.
4. A reduction in illegitimate secrecy-related information actions will increase government accountability and enlightened citizen understanding without adversely affecting national security.

Study Limitations

Researching conspiracies is difficult in that most research subjects would have no reason to avoid detection as do those engaged in secret activities (Keeley, 1999). This lack of transparency renders scientific inquiry unfalsifiable in that there could be missing or hidden data. The same applies to secrecy because of an affirmative desire to avoid detection by those attempting to circumvent established laws and policies. Although the independent counsel's office conducted a thorough investigation and legal review, there may be additional negative information actions not known to the office, not examined, remaining unknown except to members of the conspiracy.

Secrecy is inherent in the practice of law because attorneys are sworn to zealously defend their clients during adversarial proceedings and may take measures to reduce the

negative impact of information. For example, an attorney may recommend his client not testify to prevent the client from providing information against the client's interest. Another example would be when an attorney requests the court to not admit a particular document in evidence because it would incriminate the client. In this specific example, the existence of the document and its contents may be well known to the court and to the parties, or even to the public, and not entirely secret. While evidentiary rules are in place to prevent certain information from being considered during trial, the information to be excluded is generally known to the court and the parties in a legal proceeding. With the exception of legal procedures and processes related to privilege, immunity, the declassification of government information, the statute of limitations and presidential pardons, the inherent secrecy-related issues associated with the practice of law are not addressed.

Negative information actions are limited to state crimes against democracy (deHaven-Smith, 2006). Personal gains, financial or otherwise, are not considered state crimes against democracy. For example Oliver North's home security system and children's college funds paid by those with a financial interest in the missile and arms sales did not rise to the level of a state crime against democracy (see *Final Report*, 176, 180; Appendix A, Table 11). North's actions in this regard did not impact the democratic process although the funds may have been provided by those who sought to evade government accounting and congressional oversight to maximize profits generated by the sales.

Summary

Government secrecy is a complicated subject in that there are times when secrecy is and is not in keeping with the democratic process. This dissertation's objective is to better understand the nature of departures from the established secrecy structure by examining and discussing the general form of secrets as negative information actions, providing a better understanding of concepts related to secrecy and identifying conditions

allowing government officials to use secrecy to conceal crimes or evade accountability to Congress or the public. This research is significant because undue government secrecy has a detrimental impact on citizen participation and government oversight in that the ability to identify, locate, comprehend, analyze, evaluate, and utilize government information is diminished. Furthermore, this study is important to information science and public administration because it addresses the uses and misuses of government secrecy in a democratic society. The goal of this study is to identify, scrutinize and amplify information and concepts not normally addressed in the information policy research related to government information access by examining factors related to different types of secrecy-related information actions.

LITERATURE REVIEW

The focus of this dissertation is the interface between the government secrecy structure and the Iran-Contra criminal conspiracy. This dissertation is directly related to the secrecy-related information actions occurring during President Ronald Reagan's administration and President George H. Bush's administration, particularly the Iran-Contra Affair. The focus of this literature review is on the literature related to (a) government secrecy, its impact on enlightened citizenship, its moderation and its relationship to conspiracies, and (b) the Iran-Contra Affair and its fortuitous exposure which provided information related to negative information actions designed to keep information from those entitled to it by those in government during the affair.

United States Secrecy Structure

The United States government secrecy structure is composed of a constitutional provision, laws and presidential executive orders. The information policy instruments include Article 1, Section 5 of the United States Constitution and laws including the Espionage Act of 1917, the Atomic Energy Acts of 1946 and 1954, the National Security Act of 1947, the Central Intelligence Agency Act of 1949, the Presidential Records Acts of 1978, the Classified Information Procedures Act of 1980, the USA Patriot Act of 2001, The Intelligence Authorization Act of 2003, the Intelligence Reform and Terrorism Prevention Act of 2004, the exemptions found within the Freedom of Information Act of 1966 and several presidential executive orders relating to national security. Together these secrecy-related information policy instruments make up the policy framework referred to as the United States *secrecy structure*. The terms *framework* and *structure* may be considered misleading by many in that they imply government secrecy policy is consistent and coordinated. The literature suggests otherwise.

United States Constitution

Article 1, Section 5 of the 1787 United States Constitution includes a secrecy provision for the United States Senate and House of Representatives. This section instructs houses of the legislative branch to “keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their judgment require Secrecy...” (U.S. Constitution, 1787). This secrecy provision has been interpreted to mean either the Senate or House of Representatives may meet and deliberate in secret (Jost, 2005).

Legislation – Early America to World War II

The Alien and Sedition Acts of 1798, created in response to the impending conflict with France, dealt with aliens and sedition. Each of these acts was amended from existence, repealed, or expired. These signaled the beginning of the government’s ongoing dilemma of balancing private liberty and public order in the face of a national threat (Moynihan, 1998). These acts set the precedent for the Espionage Act of 1917.

The Espionage Act of 1917 permitted the government to use wiretaps and searches to prevent unlawful disclosure of sensitive information (Relyea, 1981). The Espionage Act was substantively amended in 1933, 1938 and 1950. The 1933 amendment prohibiting publishing foreign codes was in response to publication of a book by a former top intelligence officer. The 1938 amendment prohibited the taking or distribution of photographs of military installations, while the 1950 amendment was directed toward outside governments who possessed national defense information. Since 1950 there have been numerous technical amendments related to protected information and penalty modifications for those who violate the 1917 Espionage Act (Moynihan, 1998).

Legislation – The Cold War

A culture of secrecy grew as a cold war between the United States and the Soviet Union grew. World War II, the atomic bomb and the Cold War required the government to routinely classify information and enhance its intelligence operations. The Atomic Energy Act of 1946 created a separate restricted data system for protecting atomic energy

information outside the system of presidential executive orders (U.S. Commission, 1997). Restricted information is inherently secret by virtue of its creation within particular agencies, including the Central Intelligence Agency and National Security Administration. Also offices within the Department of Defense and the Department of Energy, and have not been subject to the same declassification procedures as classified information. This relationship caused problems during the implementation of Executive Order 12958 in that the automatic declassification of restricted data violated the legal provisions of the Atomic Energy Act of 1954 (Relyea, 1996). This executive order will be discussed further in a later section.

In 1947 the National Security Act created the National Security Council (NSC) to advise presidents about all domestic, foreign and military policies relating to national defense. It also created the Central Intelligence Agency (CIA) to provide intelligence on national matters to the president and agency heads (Moynihan, 1998; Huzar, 1950). Under the direction of the NSC, the CIA was authorized to protect intelligence sources and methods, and review national security intelligence from other agencies. This relationship between the NSC and the CIA was restated in the Central Intelligence Agency Act of 1949 (Relyea, 1981).

The Presidential Records Acts of 1978 defined *presidential record* and provided the handling and preservation all presidential documents created after January 20, 1981. Presidential papers became the property of the government and were placed under the control and custody of the United States Archivist (Hernon, Relyea, Dugan, & Cheverie, 2002). Prior to the enactment of this legislation, presidents were permitted to take their records and papers with them when they left office. As a result, presidential papers were often lost, worn with time and sometimes destroyed by design (Hernon, et al., 2002). Presidents were permitted a 12 year restricted access period to prevent the immediate release of records related to certain areas including national defense, foreign policy and others. Newly elected George W. Bush issued an executive order permitting either the White House or former presidents to block the release of presidential papers. His November 2001 order prevented the release of Reagan's records and documents which were soon to be released to the public under the Presidential Records Acts (Jost, 2005).

The Classified Information Procedures Act of 1980 established evidentiary procedures for protection against the unauthorized disclosure of classified information in the custody of the United States district courts, courts of appeal, or the Supreme Court. The procedures apply to proceedings in criminal cases involving classified information and include requirements for security clearances, security officers, physical security, custody and storage of evidence and disposal of classified information (U.S. Congress, 1980). The attorney general has unrestricted discretion to determine whether to declassify information necessary for trial (Walsh, 1993).

The Freedom of Information Act – Pre-September 11, 2001

The Freedom of Information Act (FOIA), signed into law by President Lyndon Johnson in 1966, provided any person the right to request, receive, or inspect records held by the government (Feinberg, 2004). The FOIA was amended in 1974 to make it easier to access government information in the wake of the Watergate scandal of the Nixon administration (Feinberg, 2004). In 1981 the Reagan administration modified the FOIA to restrict information access if there was a substantial legal basis (Gordon-Murnane, 2002). In 1996, under President Bill Clinton, the FOIA was amended to include electronic access to government information, thereby making access to government information convenient and accessible to citizens through websites and electronic reading rooms (Smith, Fraser, & McClure, 2000). This is commonly referred to as *E-FOIA*.

FOIA provides nine exemptions under which government agencies may withhold certain government information from the public. These include:

1. Documents properly classified as secret in the interest of national defense or foreign policy.
2. Documents related solely to internal personnel rules and practices.
3. Documents exempted by other statutes.
4. Trade secret or privileged or confidential commercial or financial information obtained from a person.
5. Privileged inter-agency or intra-agency memorandum or letters.

6. Personnel, medical, or similar file the release of which would constitute a clearly unwarranted invasion of personal privacy.
7. Documents compiled for specific law enforcement purposes.
8. Documents contained in or related to examination, operation or condition reports about financial institutions.
9. Documents containing exempt information about gas or oil wells.

(U.S. Commission, 2006)

Each administration has significant latitude in how it interprets and implements the FOIA.

Legislation – Post-September 11, 2001

Immediately after the September 11, 2001, terrorist attacks on New York and Washington, D.C., the federal government enacted legislation in an attempt to prevent further attacks on the United States including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Pub. L. 107-56), commonly known as the *USA Patriot Act* signed into law by President George W. Bush (ALA, 2001). The anti-terrorist legislation addressed several secrecy-related areas, including the government's ability to conduct searches in secret. One provision expanded the Justice Department's ability to conduct secret wiretaps. Another permitted the Department to secretly enter a person's home and to conduct searches without notice to the individual. A third permitted the Department to obtain secret orders to obtain "books, records, papers, documents and other items" (U.S. Committee, 2004, p. vi). Under penalty of law no person is permitted to disclose or discuss the agency's use of the secret orders known as *national security letters* (Yost, 2005).

The Intelligence Authorization Act for fiscal year 2003 prohibited the release of certain records to specific types of requestors, including non-governmental entities (Feinberg, 2004). The agencies to which the Intelligence Authorization Act applies include the CIA, the NSC, the Defense Intelligence Agency (DIA), the National Imagery and Mapping Agency and the National Reconnaissance Office (Feinberg, 2004). The act also applies to intelligence units within the Army, Navy and Marines, the FBI; and the

Treasury, Energy, and Homeland Security departments (Feinberg, 2004). It appears the president and concerned department heads can apply this exemption by designating offices within any department as an element of the intelligence community (Feinberg, 2004).

Based upon the 9/11 Commission's recommendations in response to the September 11, 2001 attacks, the United States Congress passed the Intelligence Reform Act to create the National Intelligence Council and the post of Director of National Intelligence which serves as head of the intelligence community and oversee the National Intelligence Program (White House, 2004).

The Freedom of Information Act – Post-September 11, 2001

In addition to the USA Patriot Act, administrative agencies within the executive branch increased restrictions on the release of government information to the public. On October 12, 2001, Attorney General John Ashcroft issued a memorandum related to the release of documents under the Freedom of Information Act to all agencies across the executive branch of the federal government (U.S. Dept. of Justice, 2001). According to Martin Halstuk (2002), Ashcroft's memorandum, issued shortly after the September 11 attacks, encouraged government officials to withhold as much information as possible from FOIA requesters. Included in Ashcroft's memorandum was an offer to support and defend government officials who attempted to withhold information requested under the FOIA. This memorandum disturbed individuals who recognize administrations have a natural tendency to conceal information that may prove embarrassing or may lead to official investigations and prosecution (Halstuk, 2002). Ashcroft's position was a departure from the policy of openness established in 1993 under the Clinton administration by Attorney General Janet Reno.

A second memorandum the Bush administration issued to the department heads of the executive branch came from White House Chief of Staff Andrew Card on March 19, 2002 (Gordon-Murnane, 2002). The Card memorandum instructed any document related to weapons of mass destruction or included other information that could be misused to harm the nation's security should not be disclosed or posted on federal government

websites (Gordon-Murnane, 2002). Card's memorandum usurped the tradition of the Justice Department—not the White House—guided federal agency decision-making related to the access of government information (Feinberg, 2004).

Changes in the FOIA since the September 2001 terrorist attacks include guidance from the executive branch to restrict access under the FOIA, expansion of categories of government information exempt from the FOIA and new and expanded authority for private-sector government contractors to withhold sensitive information (Feinberg, 2004). Civilian consultants and industry contractors are authorized to assign classifications to their government-related work (Demac, 1984; Feinberg, 2004). Civilian contractors are now given broad discretion to classify government information, and these employees are not subject to congressional oversight, nor is there an automatic declassification process or an internal or judicial appeals process for civilian contractors (Feinberg, 2004). Other governmental efforts to resist the FOIA have included understaffing and under-funding government information offices, failing to provide filing systems necessary for information retrieval, using delaying tactics and misusing statutory exemptions, particularly those for national security and law enforcement (Doyle, 1999).

Presidential Executive Orders – 1940 to 1970

Prior to 1940 the armed forces administered the classification system of national security information through military regulations (Relyea, 1981). Subsequently the administration of the classification system became the responsibility of the president (Moynihan, 1998). Presidential executive orders have created, eliminated and defined classification categories; determined declassification deadlines; and defined responsibilities of intelligence directors. As a result, the application of executive orders related to classified information emphasized either public access to government information or secrecy in the name of national security, depending upon which party controlled the executive branch (U.S. Commission, 1997). Beginning with the first executive order on classification, the scope of classification initially related to military information has widened to include information related to economic and technology matters (Demac, 1984).

In 1940 President Franklin Roosevelt used a 1938 law placing the security of armed forces installations and related information under the control of the president as the basis for Executive Order 8381, the first presidential executive order related to classification of government information (Demac, 1984). In 1942 Roosevelt issued Executive Order 9066 giving the Secretary of War the power to protect against espionage and sabotage of military material by excluding individuals from designated areas. In 1947 President Harry Truman issued Executive Order 9835 which provided uniform investigative procedures for employees and authorized government employment review boards (Demac, 1984).

Truman later signed Executive Order 10104 aligning the United States information security with our allies by adding a fourth level of classified information (Hernon, et al., 2002). He also signed Executive Order 10290 in 1951 completely overhauling the security classification system by extending classification authority to non-military agencies. Information was classified in the interest of national security rather than national defense (Hernon, et al., 2002). This executive order and subsequent amendments including Executive Orders 10501 signed by President Dwight Eisenhower in 1953 further restricted the basis for assigning official secrecy to government information (Hernon, et al.). Eisenhower's 1953 Executive Order 10450 provided each federal employee be given a background investigation and an employee's superior would be held responsible should an employee be found not to be reliable, trustworthy, of good character, or disloyal to the United States (Moynihan, 1998).

Presidential Executive Order – 1970 to Present

For the most part, until the Reagan administration, executive orders relating to classification displayed a tendency toward limiting the volume of classified materials (Demac, 1984). For example, President's Nixon's 1972 Executive Order 11652 significantly reduced the number of personnel who could review government information for classification purposes, provided timetables for automatic declassification and created right for public demand review of information not declassified as directed in a classification order (Demac, 1984). Nixon's views on openness in government appear to

be at odds with his obsession with leaks within government. President Jimmy Carter's 1978 Executive Order 12065 created specific categories limiting the type of information subject to classification to those documents reasonably be expected to cause identifiable damage to the nation and imposed a balancing test to determine whether classified information could be released to the public (Demac, 1984). After the Cold War ended, and throughout the Reagan administration, the culture of secrecy continued to grow.

Reagan's 1982 Executive Order 12356 reversed the trend toward open government and public accountability by removing the balancing test, by permitting the automatic classification of documents without review to determine if they would cause identifiable harm, classifying information at the highest level when in doubt and by discarding provisions mandating systematic review and declassification (Demac, 1984). In addition to amending the classification provisions, Reagan took steps to reduce and eliminate unauthorized disclosures of government information by imposing restrictions on all contacts between agency personnel and the media and requiring lie detector tests for White House staff. His preoccupation with leaks caused him to require government employees to sign non-disclosure agreements with provisions for prepublication review of all speeches and writings containing classified information (Demac, 1984).

President Clinton signed Executive Order 12937 in 1994 to declassify certain documents held by the National Archives including explicit national defense plans from 1950s (Relyea, 1996). In 1995 Clinton signed executive order 12958 to cut back original classifications and release previously held documents to the public, in part because of the ability of secrecy to ruin presidents and threaten the constitutional order as demonstrated in the Watergate Scandal and the Iran-Contra Affair (Moynihan, 1998). This executive order also provided for the declassification of twenty-five-year-old documents by 2000 (Hernon, et al., 2002). In 1995 he signed Executive Order 12968 to further reform the classification system by requiring overhauling the clearance process for those individuals with access to classified information, and it also provided for review proceedings for clearance denials (Relyea, 1996). In 1999 Clinton signed Executive Order 13142 extending the deadline for the automatic declassification of 25-year-old documents to take place within 18 and 36 months (Hernon, et al., 2002). George W. Bush signed Executive Order 13292 extending until 2006 the scheduled declassification of documents

established by Clinton. This executive order also removed the provision to classify documents at the lowest level and required any information provided by a foreign government be kept confidential (Josh, 2005).

Governmental Oversight – 1955 to 1958

Between 1955 and 1997 the United States secrecy and classification system was scrutinized by several groups assigned by the government to review and assess various aspects of the system and to provide recommendations and corrective measures. Over the years several studies related to classification, declassification and personnel security were conducted by different commissions and committees. The 1955 Commission on Government Security was the first government review of the secrecy structure since the beginning of World War I and the passage of the Espionage Act of 1917. The Government Security Commission, formed after World War II, immediately following the communist-in-government investigations made famous by Senator Joseph McCarthy, added nothing to the body of knowledge surrounding the secrecy structure (Moynihan, 1998).

In 1956 Secretary of Defense Charles Wilson created the Coolidge Committee to investigate how to prevent future leaks of secret information by reviewing the Department of Defense classification practices and policies. The Defense Department Committee on Classified Information found the classification system sound in concept, but found classification standards to be nonspecific, causing the overclassification problem. The committee's recommendations included the creation of a director of Declassification within the Office of the Secretary of Defense (U.S. Commission, 1997).

In 1957 Lloyd Wright chaired the bipartisan Commission on Government Security also known as the Wright Commission. It held no public hearings and produced no public information. In its final report it made recommendations including restricting original classification authority to agencies possessing such authority, creating a central security office to review the management of the security system and creation of legislation criminalizing the unauthorized disclosure of classified information (U.S. Commission, 1997).

Created in 1958, the Special Government Information Subcommittee of the House Governmental Operations Committee was chaired by Representative John Moss. This subcommittee's report attributed overclassification to a lack of punishment for overclassification, but not for underclassification, of documents. It recommended an independent review of complaints related to overclassification, established automatic declassification date and provided for disciplinary action against those individuals who over classify government documents (U.S. Commission, 1997).

Governmental Oversight – 1970 to 1997

The Department of Defense Science Board's Task Force on Secrecy chaired by Dr. Frederick Seitz was created in 1970 to study the effectiveness of the Department's security measures. The Task Force found as much as 90 percent of all technical and scientific information did not require classification, so it recommended a five-year maximum classification period for all technical and scientific information to consider the benefits of public access to information resulting in technological development (U.S. Commission, 1997).

In 1985, Secretary of Defense Casper Weinberger appointed General Richard Stilwell (Ret.) to chair the Commission to Review Department of Defense Security Policies and Practices. This commission found the primary shortcoming was the inadequate implementation of existing security policy was not a deficient policy. Its recommendations included reducing the number of classifiers, the establishment of minimum security standards for all department special access programs and placing security responsibilities in a central office (U.S. Commission, 1997).

In 1994 Secretary of Defense William Perry and CIA Director James Woolsey tasked the Joint Security Commission to develop a new approach to security. Because the commission found the system was inefficient and costly, it commission recommended the creation of a Joint Security Executive Committee to develop a new, single, consolidated security policy for special access programs and sensitive compartmentalized information (U.S. Commission, 1997).

The Foreign Relations Authorization Act for Fiscal Years 1994 and 1995 created the Commission on Protecting and Reducing Government Secrecy to investigate “all matters in any way related to any legislation, executive order, regulation, practice, or procedure relating to classified information or granting security clearances” (U.S. Commission, 1997). The Commission on Protecting and Reducing Government Secrecy chaired by Senator Patrick Moynihan concluded the government was classifying too much information at too great a cost and the volume of needlessly classified information compromised the security of vital secrets. The commission identified intangible costs including an erosion of public confidence in government because without legitimate justification many documents have been classified to protect the careers of government officials (Moynihan, 1998). The commission recommended the government classification and declassification programs to be statutorily based, not based on executive order. Control by the legislature rather than the president would have provided a statutory framework including uniform classification procedures for government weighing public access to information against national security needs (Moynihan, 1998). Government classification and declassification remain based on presidential executive order.

Enlightened Citizen Understanding

“The idea of an informed citizenry began in Tudor and Stuart England, where in the sixteenth and seventeenth centuries gentlemen first defined and asserted quasi-republican principles of citizenship” (Brown, 1996, p. xiv). “Americans have believed in the idea that citizens should be informed to exercise their civic responsibilities wisely. At the birth of the republic, the necessity of an informed citizenry was proclaimed loudly and often by such notables as Samuel Adams, George Washington, Thomas Jefferson, and James Madison, in addition to a host of less well known leaders” (Brown, 1996, p. xiii). Any democratic government ought to be evaluated according to the opportunities it affords for the acquisition of information by its citizens (Dahl, 1977).

Democratic Imperative

There is no single universally accepted model of democracy. Various forms of democracy are found throughout the world today (Dahl, 2000). There exist several types of democratic governments, each with its unique political structure. For example, the United States and England are democracies, but each has a different political structure. For more than a generation, Robert Dahl has been considered the most important democratic theorist in the United States. Dahl (1998) identified five criteria a government must have to meet to be considered fully democratic:

1. Effective participation—equal and effective opportunities for citizens to make their views on policy known to others.
2. Voting equality—equal and effective opportunities for citizens to vote and have their vote counted equally.
3. Enlightened understanding—equal and effective opportunities for citizens to learn about relevant alternative policies and possible consequences.
4. Exercising final control of the agenda—policies are always open to change by citizens if they so choose.
5. Inclusion of adults—adult citizens who are permanent residents should have all of the rights implied in the first four criteria. Each of Dahl's criteria is necessary for each adult citizen to be a political equal.

Government secrecy impacts several of these democratic criteria. The one most affected may be the requirement that “citizens must have equal and effective opportunities for learning about the relevant alternative policies and their likely consequence” (Dahl, 1998, p.39). Political equality assumes all citizens are equally qualified to participate in decisions if provided sufficient opportunities to learn about matters before the government and through “inquiry, discussion and deliberation” to make decisions best serving their interests (Dahl, 1998, p. 39). There are times when a citizen's ability to obtain government information is hampered by the government's need to keep information from its enemies. There are also times when the public's ability to obtain government information is hampered by the government's desire to keep embarrassing or criminal information from the public.

Bureaucratic Dilemma

Max Weber, in his discussion on social organizations, held bureaucratic institutions have an inherent preoccupation with secrecy (Rourke, 1957). Steven Katz (1987) believed excessive government secrecy is a national problem because it promotes fugitive policy making, defeats the checks and balances system and also destroys accountability. While government secrecy is necessary for national defense and foreign affairs, not all government secrets are related to national security or authorized by law. Many times information control is used to withhold information from a foreign adversary and the public (Edwards & Wayne, 1990). Justice Hugo Black, in the Pentagon Papers case, wrote, “The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic” (Moynihan, 1998, p. 205). Secrets unrelated to national security or unauthorized by law run counter to the democratic process. As government secrecy increases, government accountability to the public decreases (Demac, 1984). Undue government secrecy prevents citizens from making informed choices in matters important to individual citizens and to society.

Government Tactics

A range of tactics and maneuvers are used by government employees at several levels to withhold documents from the public. Mid-level officials care less about whether a document is destroyed than whether the information remains inaccessible. Top-level bureaucrats use three main prerogatives of secrecy: (a) control over preservation, (b) control over custody and (c) control over access (Armstrong, 1998). Other tactics used by government employees to protect secret activities include withholding information, deemphasizing information, refusing information, timing the release of information, obfuscating information and falsifying information (Edwards & Wayne, 1990). The prevalence of misinformation weakens an individual’s ability to reason effectively and to participate politically (Demac, 1984). Government employees have altered, hidden and destroyed documents to prevent their public exposure (Walsh, 1997).

Purging and removing records from the executive branch at the end of a president’s term has proven to be an effective and efficient way to maintain a president’s secrets at the end of his administration (Armstrong, 1998). In January 1989, prior to

George H. Bush's inauguration, it was discovered the Reagan White House, with the assistance of the United States Archivist, purged its entire electronic mail system on the eve of the inauguration. A federal judge ruled the archivist of the United States had failed to fulfill his statutory duties under the Federal Records Act in that he took no action to prevent the deletion of the emails (Armstrong, 1998). On the eve of Clinton's inauguration, the United States Archivist, despite the previous judicial ruling, signed an agreement granting George H. Bush exclusive control over the email of his administration.

In addition to the measures and tactics previously discussed, government employees have been given wide latitude by their superiors to classify and preserve records and have been known to abuse this discretion to withhold government information. Prohibitions and criminal penalties against over-classification and destruction of records are lax and ineffective (Armstrong, 1998; Doyle, 1999).

Consequences for Democracy

"Secrecy has significant consequences for the national interest when, as a result, policy-makers are not fully informed, government is not held accountable for its actions, and the public cannot engage in informed debate" (Moynihan, 1998, p. 14). There is a growing concern the right to access government information is diminishing, citizens are less informed about government activities and government abuses of power increase as secrecy increases (Demac, 1984; Feinberg, 2004). Individuals and groups owning and controlling information have great advantages over those who do not (Demac, 1984). Control of the argument is the most compelling benefit of secrecy since restricting the direct access to government information ensures one side of any policy debate is heard (Armstrong, 1998). "What secrecy grants in the short run--public support for government policies--in the long run it takes away, as official secrecy gives rise to fantasies that corrode belief in the possibilities of democratic government" (Moynihan, 1998, p. 58).

Secrecy Moderation

“The politics of secrecy began long ago. It is an intricate mosaic of tangibles and intangibles carried out directly through laws, lies, and misinformation and indirectly through insider habits that shield those in office from public scrutiny. It is a practice that serves special interests inside and outside government. Yet, despite its complexity, secrecy sanctioned by the upper reaches of government and extending beyond can have but one possible result: an increasingly arrogant government and an uninformed citizenry” (Demac, 1984, p. 141). Given the government’s propensity to conquer, control and manipulate information, concerned individuals and groups must wage an ongoing low-intensity, guerrilla war for government information (Armstrong, 1998). Strategies used to reduce secrecy include open politics, whistle blowing and leaks (Ku, 1998).

Open Politics

Open politics is defined by a minimum amount of secrecy in governmental affairs so citizen access to government information is maximized (Thompson, 1999). Open politics would include open meetings of government officials or committees and provision of free copies of government reports, studies and other government documents. Sunshine laws and open-government legislation are indicative of open politics where decisions are not made in secret and citizens are encouraged to participate politically. Secrecy can be moderated by specifying how long secrets will be kept by the government. In this approach, a secret is disclosed after a certain period of time or a secret is partially revealed to the public (Thompson, 1999). Second-order publicity can also help to manage secrecy since, at this level, it is the government’s decision whether or not to keep a policy secret, and to have procedures in place to determine when secrecy is appropriate, and if and when the secret should be disclosed (Thompson, 1999).

Whistleblowing

Roberta Johnson and Michael Kraft (1990) divided whistleblowing activity into four key components:

1. An individual intentionally engages in action designed to make information public.
2. The information is actually made public.
3. The information is directly related to possible or actual wrongdoings in an organization.
4. The individual making the information public is not an ordinary citizen or a journalist, but a employee or former employee of the organization.

Whistleblowers may disclose information using several methods. The individual to whom the information is provided is expected to publicize it. The organization's wrongdoing exposed by the whistleblower may be unlawful, dangerous, or unethical. Significant wrongdoings are different from insignificant ones in that significant wrongdoings affect large numbers of individuals, result in serious harm or injury, or involve large amounts of money (Johnson & Kraft, 1990).

Unauthorized Disclosure

Leaks are the intentional unauthorized disclosure of government information by insiders who make public information that has been kept secret (Ku, 1998). Although Congress passed laws to protect federal employees who disclose intelligence to its members, those who challenge the secrecy structure risk censure, sanctions, or worse (Doyle, 1999). The unlawful release of certain government secrets is seen as reasonable when exposing government wrongdoing (Colby, 1976). Governmental wrongdoings have included official and unofficial diplomatic secrets, cover-ups of wrongdoings, under-the-table dealings, betrayals of public trust and confidential exchanges (Ku, 1998).

An example of a leak exposing the deceptive practices of the Nixon administration regarding the United States involvement in the Vietnam conflict is commonly referred to as the Pentagon Papers. In June 1971 the New York Times began a series of stories providing information concerning the government's involvement in Vietnam based on a leaked project report. Daniel Ellsberg, a member of an in-house task

force working on the top secret project report including a detailed history of the Vietnam effort, leaked the report to the newspaper after making an unauthorized copy for himself. The project report demonstrated differences in the government's rationale for entering the conflict. Based upon the report's revelations, including government documents detailing decisions leading to the Vietnam conflict, the newspaper determined the entry into the war was criminal and published the entire report (Moynihan, 1998).

President Nixon, in an attempt to prevent the publication of the Pentagon Papers by the New York Times, obtained a temporary restraining order. Upon review, the Supreme Court permitted the newspaper to publish the report (Moynihan, 1998). Like many other documents classified during the Vietnam conflict, the Pentagon Papers were kept secret more to prevent government embarrassment than to protect national security. A review of the report indicated, with the exception of early military planning and weapons specifications, little information contained in it could have placed the nation's security at risk (Moynihan, 1998).

Government methods designed to prevent the unauthorized disclosure of government information include oaths of allegiance, official acts, statutes, and executive orders (Galnoor, 1975). Former CIA Director William Colby (1976) suggested secrecy laws relating to the leaking or unauthorized disclosure of government information and any punishment authorized by law may be less effective than the application of contract law related to employee nondisclosure agreements. Daniel Elsberg (2004) suggested revising nondisclosure agreements for government employees to include a provision expressly prohibiting government employees and contractors from giving false or perjured testimony to Congress or the courts.

Recommendations

The Moynihan Commission made six formal recommendations related to government secrecy:

1. The government must demonstrate a need to protect national security before classifying information.
2. The president must establish procedures to classify and declassify information.

3. In decisions regarding whether information should be classified, the benefits of public disclosure must be weighed against the need for secrecy and must be weighed in favor of the public when in doubt.
4. Unless the need for secrecy can be recertified after 10 years, the information must be declassified; after 30 years all information must be declassified unless resulting harm can be demonstrated.
5. No authority to withhold information from Congress shall exist.
6. A federal declassification center shall be established with the responsibility of coordinating, implementing, and overseeing declassification (Moynihan, 1998).

Donna Demac (1984) suggested several ways to reverse information restrictions including:

1. To study changes of information policy.
2. To introduce a moratorium on any presidential directive imposing lie detector tests and prepublication reviews for federal employees with access to classified information.
3. Legislation to standardize the classification process.
4. To temper legislation to eliminate paperwork with procedures assuring necessary information is retained.

The government's ability to maneuver within the law and its abuse of discretionary authority raise questions about whether a balance between openness and secrecy can be achieved legislatively without changes to the constitutional system of checks and balances (Galnoor, 1975). According to Kate Doyle (1999) balancing openness and secrecy in matters of national security will require three things: the presumption of openness, a public interest balancing test and outside review.

Conspiracies

The word *conspiracy* draws different reactions from many types of individuals. Words used to describe conspiracies range from *absurd* to *legitimate*. Conspiracies can be viewed as good, bad and innocent or even laudable (Pigden, 1995). Regardless of

one's view, conspiracies, particularly government conspiracies, exist as evidenced by history. Charles Pigden (1995) is quite adamant in his view that conspiracy theories are superstitions is itself a superstition and general skepticism permits people to evade responsibility for their actions. Secrecy, according to Brian Keeley (1999), is suggestive of nefarious activities on the part of the conspirators making it necessary to keep the conspiracy perpetually secret or to make sure the conspiracy is not believed if exposed. In a democratic government conspiracies are considered *morally suspect* (Pigden, 1995).

Brian Keeley (1999) defined conspiracy as a relatively small group of persons acting in secret to cause an historical event. Charles Pigden (1995) viewed a conspiracy as a secret plan on the part of a group to influence events partly by covert action. Keeley and Pigden agree a conspiracy requires secrecy. Pigden claims a conspiracy's impact on history depends on the historical situation and the resources at the disposal of the conspirators. Pigden points out that a conspiracy does not have to be successful to cause historical events. An example of a failed conspiracy significantly impacting history is the Watergate scandal, in which a group of individuals, with the knowledge of several high-ranking members associated with President Nixon's re-election efforts, broke into the Democratic Party National headquarters with the intent of unlawfully gathering strategic information related to a presidential election. The individuals were caught and it was later proven several White House senior staff had approved their actions prior to the break-in (Pigden, 1995). Although the conspiracy was exposed, its failure significantly impacted history in that Nixon was impeached for participating in the cover-up and later resigned from office. Furthermore, the failed conspiracy seriously impacted many Americans' trust of public officials.

Conspiracy Doctrine and Theory

The negative social effects of many conspiracies rise to a level considered criminal. According to Fred Abbate (1974) a conspiracy exists when two or more persons combine to commit an unlawful act or to commit a lawful act using unlawful means. Legal scholars address these unlawful activities in what is known as the *conspiracy doctrine*. The conspiracy doctrine provides a legal framework to protect society from the anti-

social effects of conspiracies by providing criminal sanctions. Abbate contends the doctrine makes state of mind the reason for preventive action against those who threaten society, though they may not have taken a substantial step in the commission of a criminal act. The doctrine requires only a “manifestation of intent by word or conduct” to commit conspiracy (Abbate, p. 302). The enhanced punishment for those who combine and conspire to commit criminal violations is based on four factors known as the *group-danger rationale* (Abbate, 1974). Those factors are:

1. An individual is more likely to carry out group commitments than his personal commitments.
2. Group involvement decreases the likelihood a member would remove himself from the group without the approval of other members.
3. Increased probability covert action will succeed.
4. Likelihood that greater harm will occur than intended by an individual.

While conspiracy doctrine is well established in law and is defined by its legal elements, conspiracy theory is less well defined.

Charles Pigden (1995) discussed conditions that must be present for conspiracies to occur:

1. The belief by conspirators covert action is necessary to overcome the problems faced by the group.
2. The existence of like-minded individuals who will support their efforts without revealing information related to the group activities.
3. The conspirator's belief their efforts will be successful.
4. The conspirator's have access to sufficient resources.

Conspiracies, he states, are complex in that like-minded individuals must assemble, agree on a plan, gather resources and maintain secrecy to insure its covert action. Although Pigden does not address weaknesses associated with conspiracies, it appears the failure of any single condition would logically result in its failure. This was the case in the Watergate scandal and the Iran-Contra Affair.

Secrecy

Some researchers suggest the size of a conspiratorial group can reach a point of diminishing returns in that its size has a direct impact on its ability to maintain secrecy. Goldstein (1959) believes a large number of conspirators increases the likelihood of the plan being leaked to outsiders or the members' uncertainties will dissuade other members. Donna Demac (1984) suggested the smaller the number of individuals participating in secret activities, the greater the likelihood of undetected embarrassing or criminal activities. Keeley (1999) also believed modern bureaucracies, including the military and intelligence agencies, are too large to keep secrets, as evidenced by information leaks from within these vast organizations.

There is also evidence to suggest large groups can maintain secrecy. Punitive measures have been used to maintain secrecy in large organizations. In 1963, when Joseph Valachi testified about the inner workings of the Mafia, his testimony provided information related to oaths of secrecy and allegiance including the penalty of death for violating the oath of secrecy (Sanderson, 1964; Smith, 1976). Freemasons are also required to take oaths of secrecy under the threat of *horrifying sanctions* for disclosing the order's secrets (Cohen, 1971). Compartmentation is used to maintain secrecy in large organizations. Amos Hofman (1993) suggested during the French Revolution the Bavarian Illuminati used the Freemasons' pre-existing secrecy structure to compartmentalize information according to hierarchy while providing a method to communicate secretly over great distances. Today compartmentation is based on a *need to know* basis and is used to prevent unauthorized disclosures between sectors or divisions within an organization. It is used extensively in the NSC and CIA to keep activities secret (Draper, 1991).

Iran-Contra Affair

The sources providing an in-depth account of the Iran-Contra events include Theodore Draper's *A Very Thin Line*, published in 1991; Peter Kornbluh and Malcome Byrne's 1993 book, *The Iran-Contra Scandal: The Declassification History*; Lawrence Walsh's two works, the first in his role as the Independent Counsel for Iran-Contra Matters, *Final Report of the Independent Counsel for Iran-Contra Matters*, published in 1993, and second as a private author, *Firewall* (1997). Taken together these sources provide a detailed account of the affair from historical and legal perspectives. In addition, Scott Armstrong's 1998 book chapter titled, "The War over Secrecy: Democracy's Most Important Low-Intensity Conflict," presented information about secrecy-related events occurring after the prosecution ended. As a group, these works describe numerous secrecy-related information actions impeding the democratic process or obstructing government information.

In July 1979 Antonio Somoza's regime in Nicaragua fell to the Marxist-led Sandinista National Liberation Front. The Contras were opposed to the Sandinistas because the newly formed government was viewed as an expansion of communism in Central America. The United States began supplying the Contras with paramilitary support, including military arms, to fight the Sandinistas.

Later the same year, in November, 52 American hostages were kidnapped by Islamic extremists when they seized the United States embassy in Tehran, Iran, (Moynihan, 1998). After 444 days of captivity, the hostages were released on the very day of President Reagan's inauguration, after which the United States broke diplomatic relations with Iran and declared an arms embargo against Iran. Several years later, beginning in December 1983, a Hezbollah group loyal to Ayatollah Khomeini kidnapped seven Americans in Beirut, Lebanon. Reagan was opposed to dealing with hostage takers and made his stance clear in 1985 when he stated, "America will never make concessions to terrorists--to do so would invite more terrorism" (Walsh, 1997, p. 4; Kornbluh & Byrne, 1993, p.391). These two events marked the beginning of secret operations by the Reagan administration to free the hostages and support the Contra rebels who opposed the Sandinistas (Moynihan, 1998).

The Iran-Contra scandal was the end result of the exposure of two secret Reagan administration policies, the Iran Initiative and the Nicaragua Operation, coordinated by the NSA. The Iran initiative consisted of efforts to obtain the release of American hostages held in Iran by unlawfully selling weapons to Iran. The Contra operation consisted of efforts to unlawfully support paramilitary activities in Nicaragua in violation of the Boland II Amendment. They were intertwined because the profits made from the arms sales to Iran were used to support the Contra effort. The secret programs were also against United States foreign policy. These unlawful programs were exposed in 1986 when a United States cargo plane was shot down while delivering military supplies to the Contras in October, and again in November when a Lebanese newspaper reported the sale of arms to Iran (Walsh, 1993). If not for the fortuitous exposure of the secret operations, the Nicaragua operation and the Iran initiative may not have been exposed at all. The events and the attempted cover-up by high ranking Reagan administration officials would be known as the *Iran-Contra Affair*.

Nicaraguan Covert Operation

In January 1984 Reagan approved a CIA plan to covertly mine Managua harbor in support of the Contra's fight against the Sandinistas. This secret operation should have reported to the Senate Select Committee on Intelligence and the House Committee on Intelligence. Central Intelligence Director William Casey failed to inform Congress of CIA activities in Nicaragua (Moynihan, 1998).

Failure to Inform Congress

Director Casey's March 1984 briefings were not *full*, *current*, or *prior* as required by the 1980 Intelligence Oversight Act when, in a two-hour committee briefing Casey provided a single obscure sentence referencing the Nicaragua action approved by Reagan (Draper, 1991). The CIA and NSC attempted to keep their activities secret, not from Nicaraguans who knew the harbor was mined, but the American public and from elected officials (Moynihan, 1998). After Congress discovered Casey failed to notify the committee of the administration's covert activities in Nicaragua, it passed the Boland II

Amendment to ban further aid to the Contras (Moynihan, 1998). The Boland II Amendment, signed by Reagan in October 1984 clearly prohibited any military or paramilitary support for the Contras. Reagan's administration continued secretly raising funds for the Contras. Because the Boland II Amendment was a provision in an appropriations bill, it failed to provide criminal sanctions (Walsh, 1993).

False Statements to Congress

After Congress terminated the CIA's efforts to support the Contras, the CIA realized the situation in Nicaragua would not be a winning issue in the upcoming presidential election, so it relied on deceit to continue Contra support while high-level Reagan administration officials concealed their support for these activities by lying to congressional oversight committees (Walsh, 1997). In September 1995, National Security Advisor Robert McFarlane, responding to a congressional inquiry into the United States' involvement in Nicaragua, including Lieutenant Colonel Oliver North's alleged violations of the Boland Amendment, stated in a letter, "...None of us has solicited funds, facilitated contacts for prospective potential donors, or otherwise organized or coordinated the military or paramilitary efforts of the [Contra] resistance" (Kornbluh & Byrne, 1993, p. 393). McFarlane and North participated in fundraising activities to support the Contras. These men facilitated arms deals with the Iranians where profits were combined with donations from wealthy Americans and foreign contributors, including Saudi Arabia, to purchase arms for the Contras through a secret financial operation known as the *Enterprise* (Walsh, 1993). McFarlane's false official statements contained in the letter were later used as evidence against him and others who conspired to withhold information from Congress.

The Enterprise

The Enterprise was a covert, off-the-books operation to manage the flow of funds to the Iran Initiative and the Nicaragua Operation. It circumvented government accountability and congressional oversight normally associated with covert operations (Walsh, 1993). The funding sources for the Enterprise came from foreign countries, wealthy Americans and profits from the missile sales to Iran. Foreign countries contributed more than \$34-million (Draper, 1997). The funds were funneled through a network of corporations and secret Swiss bank accounts where financial transactions were concealed and laundered. Eventually the money was used to purchase military supplies for the Contras in their efforts to overthrow the Sadinista government of Nicaragua (Walsh, 1993). Nearly a year after the creation of the Enterprise, the financial operation acquired assets valued at more than \$4-million, including eight aircraft of different sizes, a freighter, an airstrip and adjacent land, and military supplies (Draper, 1997).

October Shoot Down

On October 5, 1986, an Enterprise plane carrying arms to the Contras was shot down by Sandinista soldiers in Nicaragua. The two pilots were killed but Eugene Hasenfus, an Enterprise employee, parachuted from the plane before it crashed and was captured by the Sandinistas. Hasenfus confessed to the Sandinistas the flight was authorized by CIA to provide arms to the Contras from air bases in El Salvador. In addition, he provided the name of the CIA contact and the locations of safe houses in El Salvador (Kornbluh & Byrne, 1993). Hasenfus' capture triggered damage-control efforts by Reagan administration officials who denied United States involvement. Three days later Reagan and other administration officials began to deny United States involvement. In addition to the denials, the administration created a cover story the plane was carrying humanitarian aid from private donors to the United Nicaraguan Opposition (Kornbluh & Byrne, 1993).

The Secret Iran Initiative

Shortly after the first wave of American kidnappings during December 1983, McFarlane was encouraged by high-level Israelis to arm Iran against Iraq. The plan was for the Israelis to provide missiles to Iran while the U.S. government provided Israel with replacement missiles. The arms sales were to prevent Soviet intervention in Iran and to gain the release of American hostages held in Beirut by Hezbollah extremists (Kornbluh & Byrne, 1993).

The Missile Sales and Shipments

Encouraged by CIA Director Casey, and against the advice of Secretary of State George Shultz and Secretary of Defense Casper Weinberger, McFarlane approached Reagan to discuss the possibility of an arms-for-hostage deal. After the discussion Reagan authorized the weapon sales (Walsh, 1997). In August 1985 Israel through an Iranian intermediary, shipped 96 antitank (TOW) missiles to Iran. In September a second shipment of 408 antitank missiles was sent to Iran resulting in the release of one hostage. In mid-November McFarlane and Vice Admiral John Poindexter, McFarlane's successor as National Security Advisor, were informed by counterterrorism expert, Lieutenant Colonel Oliver North, Israel was to sell 500 anti-aircraft (HAWK) missiles to Iran to be replaced by the United States in exchange for the release of four hostages (Walsh, 1997). McFarlane resigned as National Security Advisor to Reagan at the end of November 1985, and Poindexter assumed the position in early December 1985 (Draper, 1991).

Although Weinberger opposed the sale of the HAWK missiles, North shipped the missiles based on McFarlane's assertion Reagan had approved the shipment. Since the Israelis were not allowed to fly weapons to Iran, the plan was to privately charter aircraft to fly the weapons out of Israel to other countries where they would be transferred to aircraft belonging to other nations to fly the weapons to Iran. This proved to be disastrous when the European countries unexpectedly denied landing permission to the privately chartered planes. North turned to the CIA for use of its propriety aircraft to ship the first installment of HAWK missiles from Israel to Iran (Walsh, 1997). The first installment of the November 1985 HAWK missile shipment was a failure for several reasons. Eighty of the 500 missiles were available for delivery, and worse, the first 18

delivered were outdated and were stenciled with the Star of David. The Iranians were outraged.

Presidential Findings

The acting CIA Director John McMahon became concerned when he learned of the CIA's involvement in the shipment (Walsh, 1997). Concerned the CIA had violated the law by providing proprietary aircraft to ship missiles to Israel, its General Counsel insisted on a retroactive Finding including a presidential authorization for the CIA's involvement in the November 1985 arms shipments. A Finding is a presidential document authorizing covert operations by the CIA. McMahon and Casey convinced Reagan to issue a retroactive Finding approving the CIA's actions. It was signed by Reagan on December 5, 1985, and authorized the use of proprietary aircraft to ship HAWK missiles to Iran via the Israelis and directed the CIA Director from informing Congress. This first Finding remained in effect until the second Finding was signed. Neither Secretary of State Shultz nor Weinberger was told of the first Finding (Draper, 1991). Poindexter later destroyed the Finding, indicating it was not important because it was not fully discussed with the members of the NSC (Draper, 1991).

In January 1986 Reagan decided not to use the Israelis as middle men for the missile shipments and signed a second presidential Finding authorizing direct weapons shipment to Iran. This, too, was kept secret from Congress (Walsh, 1997). Reagan signed this second presidential Finding on January 6, 1986, to find a new legal basis for the arms shipments. The second Finding, not addressed to the CIA, provided a different rationale for working with *third parties* (Iranian citizens) rather than *third countries* (Israel) as addressed in the first Finding (Draper, 1991). Poindexter decided the second Finding was also flawed using the same excuse to get a third Finding--it had not been fully discussed with members of the NSC, including Shultz (Draper).

On January 17, 1986, Reagan signed the third Finding, but Poindexter insisted it was not a third Finding at all, but rather all three were a single Finding. The third Finding was, for the most part, identical to the second Finding; the difference was found in the accompanying memorandum submitted with the third Finding. The memorandum included a newly devised scheme for the CIA to purchase the weapons from the

Department of Defense under the Economy Act, and the CIA would use an *authorized agent* to deliver them to Iran. This proved to be nothing more than a scheme to avoid direct weapon sales by the United States to Iran (Draper, 1991). In addition to signing Findings to sell weapons to Iran, Reagan had divided the administration's leadership into two groups--those permitted to take part in the Iran affair and those who were not. The group not permitted to take part in the affair included Shultz and Weinberger who were opposed to the arms sales from the beginning. The White House issued instructions Weinberger was not to receive any related reports of the arms shipments even from Weinberger's own defense intelligence unit (Draper, 1991).

Operational Exposure

Less than a month after Hasenfus was shot down in Nicaragua the Iranian initiative was also exposed. In November 1986 the Lebanese newspaper *Al Shiraa* revealed the United States sold arms to Iran. Other newspapers, including those in the United States, reported the story (Walsh, 1997). After the arms sales to Iran were unexpectedly exposed in the Lebanese publication on November 3, 1986, a second round of deception was undertaken by high-ranking members of the Reagan administration who lied to Congress in a concerted effort to protect the president from possible impeachment (Walsh, 1997). Not until November 25, 1986, did Attorney General Meese announce there existed evidence to suggest the funds from the arms sale may have been diverted to support the Contra activities. The following month the attorney general appointed Lawrence E. Walsh as independent counsel to investigate the allegations contained in the announcement (Walsh, 1993). Walsh's team was hindered by Congress' rush to a superficial conclusion and the NSC's attempts to delay progress through the overclassification of crucial documents (Walsh, 1997). In addition, Congress and the independent counsel had two different objectives during the investigation. Congress's job was to provide a complete and public accounting of the Iran-Contra, while Walsh's job was to uncover violations of the law and to punish those who committed the crimes (Walsh, 1997).

Attempted Cover-Up

Reagan told congressional leaders the covert operations had nothing to do with negotiating with terrorists while Poindexter told congressional members no transfers of weapons were made until after the president's Finding signed in 1986 (Walsh, 1997). The CIA stated no one in the *agency* was aware the 1985 shipment contained anything but oil-drilling equipment, while North indicated no one in the *government* knew the cargo was actually weapons (Walsh, 1997). Later, Poindexter admitted he deliberately withheld information from Congress while North boasted he had lied to Congress and the CIA (Draper, 1991). On November 13, 1986, Reagan, in a national broadcast told the public the charges of *trafficking with terrorists* was false and the dealings were conducted to restore normal relations with Iran (Kornbluh & Byrne, 1993). The president held a second press conference six days later and repeated the false statement the U.S. had not traded missiles for hostages and denied any missile shipments to Israel had occurred (Walsh, 1997).

On November 21, 1986, after Reagan tasked Meese with developing a position for the administration to use when dealing with Congress and the media, North and North's secretary Fawn Hall shredded documents including telephone records and copies of North's memoranda to McFarlane and Poindexter related to the 1985 HAWK shipments. Poindexter destroyed the presidential Finding authorizing the CIA to ship HAWK missiles to Iran in exchange for hostages (Walsh, 1997). North altered documents indicating his superiors were aware and encouraged the highly secret support of the Contras by removing them from the official record system, retyping them, and returning the altered documents to the record system (Armstrong, 1998).

Meese, after consulting with several cabinet members, came to the dubious conclusion the president was not aware the 1985 arms shipments were in exchange for hostages. It should be noted Meese, during his telephone calls and interviews with cabinet members regarding the president's involvement, failed to take notes of the conversations as normal (Walsh, 1997). During the interviews Weinberger failed to provide Meese with his notes indicating he warned McFarlane before the shipments began they would be illegal regardless of Israel's involvement. Shultz also failed to provide his notes related to the arms sales to Iran (Walsh, 1997). At the conclusion of the

preliminary investigation, Meese told members of Congress the Israelis handled the shipments and placed the funds in a Swiss bank account indicating North was aware of this fact and Poindexter suspected it.

Investigation and Prosecution

The FBI was delayed from investigating the arms sales while Meese conducted his personal fact-finding investigation. This delay permitted the subjects of the investigation to concoct and coordinate cover stories and to hide or destroy documents (Walsh, 1997). Realizing members of the NSC were potential targets of Walsh, Reagan and many in Congress encouraged Congress to grant immunity to Poindexter and North to block their criminal prosecutions and allow them to deny the president's involvement. The immunization of witnesses is a standard procedure used to convict senior members of conspiracies by promising immunized members will not be prosecuted in exchange for their testimony against senior members (Walsh, 1997).

On November 23, 1986, FBI agents discovered a memorandum drafted by North in April 1986. The memorandum included a plan to divert \$12-million from the missile sales to Iran to support the Contra effort in Nicaragua. The memorandum became known as the *diversion memo* (Kornbluh & Byrne, 1993). Two days later a meeting was held in the situation room in the White House basement by Reagan, Bush, Weinberger, Casey, NSA Advisor Poindexter, Shultz, Meese, and Chief of Staff Donald Regan to discuss ways to protect the president from impeachment for the secret sale of U.S. weapons to Iran in exchange for American hostages in violation of the Arms Export Control Act. Unlike most presidential meetings between administration officials, the tape recording equipment was turned off and staff members were not present to take notes (Walsh, 1997).

After the meeting, on McFarlane's instructions, Colonel North continued to shred and alter documents from his office in an effort to purge NSA files of any information related to the arm sales in an effort to hide the information from Congress. Poindexter created the cover story the Israelis had shipped the missiles to the Iranians directly and the U.S. had accidentally discovered evidence of the shipments. The cover story also

contained a false statement President Reagan approved the shipments after January 1986 without mentioning the 1985 shipments (Walsh, 1997).

After the investigation, Walsh concluded in addition to other policy and law violations, government officials had systematically and willfully withheld large volumes of relevant documents from investigators and had deliberately deceived Congress and the public about the government's knowledge of and support for the alleged activities (Walsh, 1993). As a result of the Independent Counsel investigation, nine government officials were indicted by a grand jury with criminal offenses. Of the nine government officials indicted, Assistant Secretary of State Elliot Abrams, CIA Task Force Chief Allen Fiers, CIA Deputy Director Clair George, National Security Advisor Robert McFarlane, Lieutenant Colonel Oliver North, and Vice-Admiral Poindexter were convicted of crimes. CIA Station Chief Joseph Fernandez's case was dismissed during trial when the Bush administration declined to declassify information required for his defense (Walsh, 1993). The North and Poindexter convictions were overturned based on their immunized testimony before Congress. CIA Chief Clarridge and Secretary of Defense Weinberger received presidential pardons prior to a verdict. Altogether six individuals received presidential pardons including Weinberger, Clarridge, McFarlane, Fiers, Abrams and George (Walsh, 1993). Although NSC Staff Member Fawn Hall could have been indicted and convicted, she cooperated with the independent counsel and received criminal immunity from prosecution.

The outgoing president pardoned Weinberger and five other officials on December 24, 1992. The presidential pardons assured no information found in Weinberger's notes showing George H. Bush's involvement would be introduced at trial (Armstrong, 1998). Additional evidence of Bush's involvement in the Iran-Contra was discovered in his personal records provided to the Independent Counsel after the statute of limitations expired (Walsh, 1997). Although Bush's personal records were requested during the investigation, they were withheld despite repeated requests from investigators. The discovered information indicating Bush's own misconduct caused concern in that the pardons were for individuals who had lied to Congress or otherwise obstructed the investigation (Kornbluh & Byrne, 1993).

Further Attempts to Maintain Secrecy

The best evidence of the cover-up beginning in October 1986 and continuing through August 1987 was not discovered until the last part of the investigation. The discovery of previously withheld evidence was too late for prosecution because the statute of limitations had expired, but attempts to maintain secrecy surrounding the involvement of the Reagan administration continued (Walsh, 1993). In January 1989, prior to President-elect George H. Bush's inauguration, it was discovered the Reagan White House intended to purge its entire electronic mail system on the eve of the inauguration. Included in the email to be purged was an IBM proprietary communication network known as PROFS note system. The PROFS note system was used to store the NSC's secure inter-office email among NSC staff (Armstrong, 1998). The National Archives announced the emails would not be retained since printed copies of PROFS note were either paraphrase or repeated verbatim in the Tower Commission's investigation into the Iran-Contra Affair. In 1993 a judge ruled the archivist of the United States had failed to fulfill his statutory duties under the Federal Records Act in that he took no action to prevent the deletion of the emails (Armstrong, 1998).

A Tower Commission staff member discovered a backup of contemporaneous email tapes, thought to have been erased by NSC officials, actually existed. The recovered email documented the involvement of North, McFarlane, and Poindexter in the secret supply of military arms to the Iran and their management of the Contra war against the Sandinista government in Nicaragua. The email discovery also demonstrated McFarlane lied to Congress about the Reagan administration's involvement in redirecting private donations to support a secret war in Nicaragua. In addition, the email indicated Poindexter had directed North to conceal their activities and develop cover stories to hide their complicity in the affair (Armstrong, 1998).

Outgoing President Bush utilized the services of the National Archive in the same manner as his predecessor, former President Reagan. On the eve of Clinton's inauguration, the United States Archivist, despite a previous judicial ruling, signed an agreement granting then-President Bush exclusive control over the email tapes of his administration. Also, the archivist agreed to segregate the administration's electronic records from other records and to deny access to third parties including members of

Congress and the incoming president (Cook, 1996). During the night before the inauguration, a National Archive team using rented trucks removed nearly 5000 tapes and over 100 hard drives from the White House. It was later discovered the archivist had secretly agreed to become the executive director of the George Bush Center at Texas A&M University (Armstrong, 1998).

According to the Independent Counsel for Iran-Contra Matters, the Iran initiative was carried out with the knowledge of Reagan, Bush, Shultz, Weinberger, Casey, McFarlane and Poindexter (Walsh, 1993). “What set Iran-Contra apart from previous political scandals was the fact a cover-up engineered in the White House of one president and completed by his successor prevented the rule of law from being applied to the perpetrators of criminal activity of constitutional dimension” (Walsh, 1997, p.531). Quoting Theodore Draper, “If ever the constitutional democracy of the United States is overthrown, we now have a better idea of how this is likely to be done” (Moynihan, 1998, p.3).

Summary

The areas of literature reviewed include the secrecy structure, enlightened citizen understanding, moderation of secrecy, conspiracies and the Iran-Contra Affair. Although these areas may initially appear disparate in terms of subject matter, there exists a common thread running through each area--secrecy. The literature demonstrates the United States has an established system composed of a constitutional provision, legislation and presidential executive orders designed to prevent the unauthorized disclosure of government information to its adversaries. Government officials have departed from the intent of the secrecy structure by using secrecy to hide criminal or embarrassing activities. The most compelling benefit of undue government secrecy to a given group of stakeholder is it ensures one side of any policy debate dominates all others. The enlightened understanding of citizens is negatively impacted by undue government secrecy.

The government uses many tactics to keep information from the public. There exist methods to counter these tactics and to reduce or moderate secrecy to increase a

citizen's enlightened understanding as it relates to government accountability. Government conspiracies are a recurring phenomenon requiring secrecy. Certain conditions must exist for a conspiracy to occur. Finally, the Iran-Contra Affair provides a detailed account of negative information actions outside of the secrecy structure designed to reduce the enlightened understanding of citizens and others in government. Each of the literature areas provides concepts related to excess government secrecy that may be further examined using the grounded theory research method.

Research Questions

This dissertation will attempt to answer the following research questions:

1. How dangerous are government conspiracies involving the use of negative information actions?
2. What information resources are used by government conspirators to support negative information actions?
3. How does the current legal system in the United States impact information flow in regard to negative information actions?
4. What models are available to demonstrate the impact of negative information actions in democracies?

RESEARCH METHODOLOGY

Successful government conspiracies are difficult, if not impossible, to research by their inherent secrecy-related objectives. It is fortuitous when the salient issues of a failed conspiracy are brought to public attention, closely investigated and well documented. Further, the exposure of government conspiracies provides a view of the inner workings of the government and those charged with its administration not normally available to the public.

There are sensitive ethical and political issues to be considered prior to engaging in this type of research, but the public nature of the Iran-Contra Affair rendered many of these considerations moot. Several methodologies have been used in conspiracy research. For this study, grounded theory research appears to be the most promising methodology to explore the secrecy-related aspects of the affair. Although grounded theory research methodology is chosen for this particular study, several of the methodologies discussed below may serve as tools to assist in developing categories relevant to the examination of conspiratorial groups.

Sensitive Research

Sensitive research can present problems for the researcher in that such research may explore sensitive issues including those of a personal nature, deviant and criminal behavior, vested interests of powerful people, confidentiality, cultural sensitivity and inappropriate use of findings and conclusions. Unlike research where a researcher must make decisions related to each of the sensitive ethical and political issues discussed below, many of these decisions were previously addressed because of public hearings and extensive media coverage of the Iran-Contra Affair.

Definitions

Quoting Joan Sieber, *socially sensitive research* is defined as “studies in which there are potential consequences or implications, either directly for the participants in the research or for the class of individuals represented by the research” (Renzetti & Lee, 1993, pp.3-4). Clair Renzetti and Raymond Lee (1993, p. 4) defined a *sensitive topic* as “one that potentially poses for those involved a substantial threat, the emergence of which renders problematic for the researcher and/or the collection, holding, and/or dissemination of the research data.”

Sensitive Areas

Areas where research is likely to be sensitive include those in which the research delves into the private sphere or personal experiences of individuals, where the research topic is related to deviance and social control, where the research impacts the vested interests of powerful individuals or the use of coercion or domination, and where the research deals with things sacred to the study participants who may view portions of the study as irreverent (Renzetti & Lee, 1993).

Ethical and Political Issues

Ethics and politics should be considered when conducting sensitive research. Ethical issues related to sensitive social research include voluntary participation, potential harm to participants, anonymity and confidentiality, cultural differences, and analysis and reporting. Coercion should not be used to assure an individual's participation in a study. Voluntary participation requires a clear and accurate description of what is expected of the participant during the study. It permits the participant to terminate his participation at any time (Babbie, 2000). Privacy, anonymity and confidentiality issues are also related to sensitive research in that studies where participants reveal intimate or incriminating information or where their identities are compromised would be problematic for the participants (Renzetti & Lee, 1993). Cultural sensitivity includes the researcher's ability to appreciate cultural differences and to communicate in ways study participants understand, believe and find relative to their culture (Sieber, 1993).

Political issues generally focus on the findings and conclusions, and the use of the research (Babbie, 2000). Research offending or harming politicians and government officials or is conducted incompetently, without regard for validity, reliability, or potential consequences is considered unethical (Renzetti & Lee). According to Sieber and Stanley, “sensitive research addresses some of society’s most pressing issues and policy questions. Although ignoring the ethical issues in sensitive research is not a responsible approach to science, shying away from controversial topics, simply because they are controversial, is also an avoidance of responsibility” (Renzetti & Lee, p.11).

Issues Relevant to Current Study

As discussed above, sensitive areas, and ethical and political issues must be addressed before proceeding with any study. Due to the public nature of the Iran-Contra Affair many of the issues were decided in advance of this study. This study appears to involve almost all of the sensitive areas listed above. While the independent counsel’s investigation and prosecutions focused on government officials in their public service, the investigation may have delved into their personal experiences. This research topic directly relates to deviance, social control and the vested interests of powerful people in that it examines the criminal behavior of powerful government officials and groups. While the research does not deal with things sacred to participants, political considerations could be raised in this regard. The results and conclusions of this research may disturb individuals who consider themselves *Reagan Era Republicans* or *Neoconservatives* or who consider the Reagan Administration and its efforts to thwart the spread of communism as sacrosanct.

The issue of voluntary participation was rendered moot when those individuals associated with the affair engaged in conduct giving rise to a public record. Issues related to potential harm to participants and anonymity and confidentiality of participants are not relevant to this study for the same reason. While there may be political differences to consider, there are no cultural differences reflected in the independent counsel’s report. It is expected that strictly adhering to the grounded theory research procedures and processes the research will produce valid, reliable and theoretically relevant results.

Conspiracy Research

Conspiracy research has a problem unique to this study. If, as a result of secrecy or misdirection, there are missing data or unknown explanations, how can evidence be examined? Most scientists do not experience this problem in that most subjects are passive with regard to data gathering and would not attempt to avoid detection (Keeley, 1999). This situation renders scientific inquiry unfalsifiable. What methodologies are available to study conspiracies? As with any theory, conspiracy theory attempts to explain an event by providing reasons for it in terms of a significant causal relationship of a relatively small and secret group of individuals (Keeley, 1999). Conspiracies do exist and, on occasion, they fail, leaving researchers with large amounts of data to examine. It is hoped conspiracy research will reduce the negative impact of conspiratorial activities on society by providing a method to identify conspiracies before they cause undue harm to individuals and groups. The reduction of anti-social effects associated with conspiracies is in itself a justification to conduct conspiracy-related research. There are several approaches to studying conspiracies, including ground theory research.

Errant Data Analysis

Brian Keeley (1999) focused on data related to conspiracies in his attempt to understand them. According to Keeley, errant data is useful in examining whether false explanations were disseminated in a conscious effort to deceive or misdirect those who suspect a conspiracy. Errant data includes unaccounted-for data and contradictory data. Unaccounted-for data does not contradict the official government account, but goes unexplained. For example, if the majority of the September 11, 2001, airlines terrorist were from Saudi Arabia and the 9/11 Commission failed to provide complete information related to the involvement of the Saudi government or its citizens, the missing information would be considered unaccounted-for data.

Contradictory data are those which contradict the official government account. An example of contradictory data related to September 11, 2001, would be the government's official account it had no indication Al Qaeda would use airliners to attack

the United States when the President and others had been provided a presidential daily briefing indicating possibility of an attack. The evidence contradicts the official account. Keeley's approach of analyzing either unaccounted-for data or contradictory data does not address missing data that may be useful in explaining the historical event. An errant data analysis may prove beneficial for determining the differences in the official government account provided by the Reagan administration and the evidence presented in the independent counsel's final report on the Iran-Contra.

Sociological Method

Amos Hofman (1993) suggested employing the sociological method to examine social functions surrounding conspiracies including equality, consensus and hierarchy within a structured system. Such analysis might demonstrate the group of conspirators was lead by a collective force that systematically changed its leadership (Hofman, 1993). The sociological method might be used to discover information related to the conspiracy's structural system by identifying common characteristics unique to conspiracies related to the structural components of the conspiratorial group. Relationships among branches of government, offices and departments, chains of command and political institutions could be explored. The Reagan Administration's views toward open government could be examined as structural outcome.

Historical Analysis

James Russell (1955) used historical analysis to examine the possible existence of a conspiracy related to the interpretation of the Fourteenth Amendment of the United States Constitution. Russell explored the possibility a joint committee whose intent was to protect corporations against arbitrary state legislation conspired to draft the amendment to create a constitutional protection for corporations. By identifying key stakeholders and examining their roles during the period leading up to the amendment's passage, Russell determined those in a position to secretly steer its passage did not assert undue influence and could not be legitimately accused of participating in a conspiracy. By using errant data identified through the use of information technology a second

historical analysis could be used to examine events over time and later could be compared with other historical analyses to determine whether evidence exists to adjust previously held views relating to possible conspiracies.

This study is unique in that the time frame between October 1984 and April 1993, the period between the enactment of the Boland Amendment and the publishing of the *Final Report of the Independent Counsel for Iran/Contra Matters* is the focus of this study.

Factor Analysis

Charles Pigden (1995) discussed factors and conditions that must be present for conspiracies to occur, including:

1. The belief by conspirators covert action is necessary to overcome the problems faced by the group.
2. The existence of like-minded individuals who will support their effort without revealing information related to the group activities.
3. The conspirators must believe their efforts will be successful.
4. There exist sufficient and accessible resources to accomplish their objectives.

It may be possible to focus research attention on events where factors and conditions are present. It is clear the conspirators in the Iran-Contra Affair met the conditions set forth by Pigden. These and other observations may provide insight into the conditions and factors present that would encourage a group of individuals to depart from the established secrecy structure and misuse secrecy to hide criminal or policy violations.

Donald Cressey (1967) attempted to study various aspects of secret mafia activities and determined social scientists can create data by reasoning from the known to the inaccessible. Cressey suggested unlike anthropologists and geologists who assemble facts about the past based on the present, social scientists can work with contemporary data and assume in the future they will observe an event in keeping with their inferences. The research methodologies discussed above may provide tools to better understand conspiracies by creating a multi-method approach providing a broader exploratory view of this important phenomenon. Grounded theory research seems well suited as a research

methodology for the current study, and the methodologies discussed above may provide the tools required to conduct this type of research.

Grounded Theory Research

According to Anselm Strauss and Juliet Corbin (1998, p .8), the importance of grounded theory research is it “provides a sense of vision, where it is that the analyst wants to go with the research. The techniques and procedures (method), on the other hand, furnish the means for bringing that vision into reality.”

Definitions

Anselm Strauss and Juliet Corbin (1998, p.12) defined *grounded theory* as “theory that has been derived from the data, systematically gathered and analyzed through the research process.” William Trochim (2001) regarded grounded theory research as an iterative process resulting in developing a conceptually dense theory. Grounded theory research permits the researcher to be scientifically critical and analytically creative (Strauss and Corbin).

Purpose and Goals

According to Earl Babbie (2000, p. 284) grounded theory research attempts to derive theories from an analysis of the patterns, themes, and common categories discovered in observational data.” The purpose of grounded theory is to “develop theory about phenomena of interest” rooted in observation (Trochim, 2001, 160). The goal of the researcher is to develop theories from the ground up, without preconceptions (Babbie, 2000).

Research Approaches

The grounded theory research method developed by Barney Glaser and Anselm Strauss uses a four-stage constant comparative research method (Babbie, 2000). The

first step requires the researcher to specify the nature and dimensions of various concepts found in the data. In the second step concepts are examined to determine relationships among the concepts. The third step requires the researcher to assess the concepts in terms of relevance and to discard concepts not applicable to the study resulting in the reduction of categories. Finally, the fourth step requires the researcher to put his findings in writing and to communicate them to others. This step of the research process may result in the modification and improvement to the researcher's grasp of the topic (Babbie, 2000, p.284). William Trochim (2001) suggested starting the grounded theory research process by raising generative questions to guide, but not restrict, the researcher. Trochim's second step is to identify core concepts in the data. Babbie (p. 387) suggested researchers should conduct theoretical sampling "whereby groups and institutions are selected based on theoretical relevance" prior to Trochim's second step to assure core concepts are theoretically relevant. The third step is to develop tentative linkages among theoretical core concepts and to explore observable relationships until a theory emerges.

Preliminary Grounded Theory Research Inclinations

The *Final Report of the Independent Counsel for Iran/Contra Matters* provides data that may be used to study government secrecy. The independent counsel's investigation resulted in the indictment of 14 individuals including nine government officials and another government employee who was provided criminal immunity based on her cooperation with the independent counsel. The individual indictments contain criminal charges supported by underlying facts, many of which are considered negative information actions contrary to the democratic process—specifically, withholding information from Congress and government agencies entitled to it.

This researcher's education and work experience sensitized him to certain issues related to government secrecy. A review of the final report of the independent counsel in the Iran-Contra Affair was the beginning of a *ground up* approach to identifying preliminary concepts and topics to examine during a review of the literature. It is expected a close examination of the underlying facts contained in the final report, will

provide data sufficient to help better understand the issues and concepts related to the use of negative information actions. Based on the literature review several categories were predetermined by other researchers while other categories emerged from a closer examination of the independent counsel's report.

Initial Topic Selection and Sensitizing Issues

After this researcher familiarized himself with the Iran-Contra Affair he recognized government officials used various actions to withhold information from others in government and the public. He further recognized the affair was the result of government officials combining and conspiring to circumvent congressional oversight through the use of secrecy. Prior research and education lead the researcher to describe the current federal secrecy structure by examining federal information policy instruments, including constitutional provisions, laws and executive orders. Having been sensitized to issues related to federal information policy, including the issue of citizen access to government information, the topic of enlightened citizen choice was further researched. Ways to reduce the negative impact of government secrecy through secrecy moderation were identified and researched.

Finally, this researcher's military and law-related experience enabled him to recognize the value of the *Final Report of the Independent Counsel for Iran/Contra Matters*. Active duty military experience as a member of the United States Navy Ceremonial Guard required serving as an escort to President Reagan and other high-ranking government dignitaries and foreign heads of state. The need for discretion and confidentiality in the military was reinforced during his legal training.

After returning to Florida this researcher served as a litigation support member to various state agencies and departments including the Office of the Attorney General. The litigation duties included the gathering and organizing of evidence during the discovery and trial phases of several lawsuits between government agencies and departments and private groups and organizations. This researcher also represented state agencies as a non-lawyer legal representative conducting trials and depositions before the Florida

Division of Administrative Hearings. This experience and legal training provided insight to the importance of the rule of law as it relates to constitutional and other legal matters.

Summary

The Iran-Contra Affair is rich with examples of negative information actions designed to circumvent government oversight which diminishes enlightened citizen understanding. Many of the sensitive, ethical and political issues related to this study have been previously decided by those in government. Although the topic of this dissertation may be controversial, it would be socially irresponsible not to study issues related to undue government secrecy. It would also be academically irresponsible to ignore a data source providing a rare, thorough and accurate accounting of a government conspiracy relevant to the study of secrecy-related issues and their impact on the democratic process.

APPROACH TO CURRENT STUDY

The research method chosen for this study combines general aspects of Babbie's, Trochim's, and Glaser and Strauss's grounded theory research approaches. As previously discussed, the generally accepted approach to grounded theory research is to (a) collect data, (b) analyze the data through coding and theoretical sampling and (c) after saturation occurs and the process of emergence has exhausted itself the researcher should place his or her findings and conclusions in writing and communicate them to others. The iterative nature of grounded theory research and its constant comparative method requires the researcher to repeat coding and theoretical sampling until emergence and saturation occur resulting in an "extremely well-considered explanation for some phenomenon of interest" (Trochim, 2001, p. 160).

Data Validity

The *Final Report of the Independent Counsel for Iran/Contra Matters* was issued on August 4, 1993. The report contains a summary of the prosecutions, the underlying facts, the history of the investigation, a legal analysis of the operational conspiracy, a discussion on political oversight and the rule of law, and investigations and cases against various individuals from the NSC Staff, the CIA, the Department of State, the Department of Defense and the White House. Also included is a second summary of prosecutions, the indictments or pleas of 14 individuals, 5 civilians and 9 government officials, indicted as a result of the independent counsel's investigation, four interim reports to Congress about immunity-related issues, national security classification-related issues, the discovery of previously withheld information and its implications and the impact of presidential pardons.

The report describes numerous examples of negative information actions designed to withhold information from those entitled to it. These negative information actions include false testimony, destruction and removal of documents, altered documents, cover stories, misused security classifications, grants of immunity and pardons. These actions,

while relatively large in number, provide a rare opportunity to research the secrecy-related issues impacting the democratic process. The final report provides an in depth account of the government officials and their choice of negative information action used to withhold information from those entitled to it.

The final report was the end result of not one, but two, fortuitous exposures—the initial exposure of the secret Iran-Contra programs and the discovery of evidence of a cover-up. In many cases the evidence was produced too late for the independent counsel to successfully prosecute certain individuals. The *Final Report of the Independent Counsel for Iran/Contra Matters* provides data valid to the current study.

Data Reliability

The *Final Report of the Independent Counsel for Iran/Contra Matters* provides uncommon data in that rarely do successful conspiracies reveal data sufficient to conduct secrecy-related research. The independent counsel's report was thoroughly investigated by an appointed independent counsel, numerous agents of the FBI, 65 attorneys, over two dozen paralegals and several consultants. The due diligence required to be exercised by these professionals prior to the presentation of the evidence to a federal grand jury adds to the reliability of the previously gathered data contained in the official government report.

A secondary review of the evidence and testimony by the federal grand jury prior to the issuance of the indictments provides additional rigor to the data-collection efforts during the investigation and post-investigation phases. Data collection and analytical procedures give rigor to the research and provide reliability to grounded theory research (Babbie, 2000). In addition, the independent counsel's evidence-collection procedures, which were in accordance with the federal rules of evidence and federal rules of procedure, were subject to grand jury review, congressional review, and judicial review and were reliable.

Theoretical Relevance

The scope of any criminal investigation and prosecution is limited by its relevance to the underlying criminal activity. While violations of the Boland Amendment were the initial topics of a congressional investigation, they were not criminal. The attempts to circumvent congressional oversight and criminal investigations were criminal and relevant. In addition to being legally relevant, the facts contained in the report are also theoretically relevant to the investigation of negative information actions taken by government officials. The investigation and this study examine the underlying actions related to withholding information from those in government entitled to it.

Literature Review

Some grounded theorists would not concern themselves with conducting a literature review until after data analysis (Glaser, et al., 2004). This approach has merit in that it attempts to minimize the researcher from being unduly influenced by the research of others but it does not serve well those lacking a basic understanding of a known phenomenon of interest. The idea of a technical literature review to examine different methodologies related to a particular type of study requires the researcher to review the technical information while simultaneously sequestering substantive findings and conclusions to not bias the study's methodological approach.

A literature review producing little or no research, technical or substantive, directly related to a particular area of interest requires researchers to conduct a literature review of areas indirectly related to their particular research topic. This examination of related literatures may be viewed as an initial form of open coding in that concepts emerge, sometimes disparately, until the researcher has gained a basic understanding of salient areas surrounding the phenomenon of interest. A post-analysis literature review combined with a pre-analysis literature review may provide additional codes or concepts not readily realized during the first review.

Documentary Data

Data and data collection in grounded theory research is usually associated with information collected during interviews of individuals and groups. There are other sources of data including documentary data (Pandit, 1996; Glaser, 2004). Availability is an issue to consider when identifying possible data sources. Those phenomena involving sensitive and potentially embarrassing issues would make interviewing subjects problematic. Without the availability of interviews the researcher must turn to documentary data. In this case, the documentary data is based on the interviews of witnesses and documentary evidence relevant to the underlying issue of a cover up and not the initial policy violation.

Note Taking

In general, note taking consists of assigning an identifier to significant points in a transcript in such a way to permit the researcher to review the content and key points by following sequential codes (Allan, 2003). In this study, key point coding consists of identifying negative information actions and electronically highlighting those portions of the report in yellow followed by the assignment of a code starting at the first investigative report and continuing on through the remaining investigative reports and each subsequent pass. The key point code contains an upper case letter indicating a particular investigative file followed by a number representing a particular key point. A number within parentheses following the key point code identifies repeated information actions. For example, PM1(2) indicates Vice Admiral Poindexter “M1” destroyed documents a second time “(2).” The final codes are used to locate the position of negative information actions on a continuum of enlightened citizen understanding according to their relative impact. The method coding is combined with knowledge support coding and information technology indicators to provide a broader picture of relative concepts and categories.

Memoing

In addition to note cards, notebooks, tape recorders, and marginalia used to record ideas related to theoretical relevance and other considerations, electronic memoing may be used to serve the same function. Electronic memoing may be used to consolidate the other methods used to record ideas and what C. Wright Mills (1959, p. 29) referred to as “fringe thoughts: various ideas occur, which may be by-products of everyday experience, snatches of conversation...or for that matter, dreams.” For example, while driving on a trip it occurs to the researcher that whether negative information actions are charged as a misdemeanor or as a felony has more to do with whether the subject cooperated with the prosecution than whether the act was egregious, or whether aggravating factors were present. In this example, the researcher would create a mental note indicating the insignificance of misdemeanors and felonies and later would create an electronic memo reflecting the same. Memoing may, to a degree, aid in replicating emergent thought. The issue of replication in the scientific method is further addressed in an upcoming section related to emergence and saturation.

Coding

The process of coding conceptualizes underlying issues found in the data. Micro-analysis (word by word and line by line) may lead to over conceptualization and data overload. Identifying key points significant to the investigation and research questions avoids these problems associated with micro-analysis (Allan, 2003; Pandit, 1996). In this study key point coding consists of highlighting points in the text relevant to the study and assigning an identifier to the key point. Events containing previously identified negative information actions found in the documentary data are isolated for examination. Concepts emerge as codes are compared to create groupings which are subsequently categorized. As new key points are discovered they are compared with the previously identified codes and categories by using the constant comparative method (Allan, 2003).

Open coding, used to develop concepts and categories, may be followed by axial coding used to identify relationships among categories (Pandit, 1996).

Emergence and Saturation

Theoretical sampling enhances the theoretical framework by narrowing the emergent theoretical issues relevant to the study (Pandit, 1996). The linking of categories and the examination of relationships among concepts and categories permit theoretical emergence (Allan, 2003). The process of emergence ends when the benefits of constant comparison reach the point of diminishing return with regard to discovering emerging concepts and categories. This is generally known in grounded theory research as saturation.

Grounded theory research permits the researcher to be scientifically critical and analytically creative (Strauss and Corbin, 1998). The analytical creative ability of a researcher may be readily demonstrated during emergence. Researchers do not possess the same creative capacity to recognize relationships among concepts and categories since it is a subjective effort on the part of individual researchers. This ability has been brought into question by those in research fields and disciplines who believe this to be a departure from the scientific rigors normally associated with objective scientific research. The difficulty of replicating emergent moments runs counter to the scientific method requiring others using the same methodology and data to reproduce the same outcome.

Creative ability and its role in research were addressed by C. Wright Mills (1959) in his examination of the topics of sociological imagination and intellectual craftsmanship. The sociological imagination is “the capacity to shift from one perspective to another, and in the process to build up an adequate view of a total society and its several components” while intellectual craftsmanship allows the researcher’s personal involvement in intellectual production (Mills, 1959, p. 40).

Barney Glaser (2004) suggested grounded theorists must possess theoretical sensitivity to generate concepts from data and to relate them to normal models of theory and theory development in the social sciences. According to Glaser, theoretical

sensitivity requires two characteristics: (a) a temperamental bent to maintain an analytic distance, tolerate confusion and regression and the ability to trust preconscious processing and conceptual emergence, and (b) an ability to conceptualize and organize, make abstract connections and to visualize and consider issues from multiple perspectives. Imagination, craftsmanship and sensitivity used during grounded theory research serve to complement objective analytical rigor generally associated with scientific research.

Measures, Magnitude and Predictive Value

According to Donald Katzner (2001), it is easier to measure elements related to a physical phenomenon than to measure a social phenomenon because there are few, if any, scales to measure salient social science variables. There exist no cardinal or ratio measures for abstract variables such as security, honesty, freedom or trust (Katzner, 2001). Negative information actions performed by individuals can be counted. Such counts cannot convey information related to many factors including impact. Also, orders of magnitude cannot be substituted for cardinal or ratio measures. For example, the significance of shredding a routinely created document does not necessarily outweigh the significance of a presidential pardon. In this example, the shredding may have destroyed evidence of a crime and ultimately resulted in an individual not going to prison, but so would a pardon. Furthermore, a staffer's shredding of a memo concerning a routine meeting would not rise to the level of shredding a presidential Finding by a national security advisor. Based on the above, there will be no attempt to measure the impact of negative information actions based on their magnitude.

Social science is not a predictive science in that laws in social science are relevant for the past and present (Katzner, 2001). Donald Cressey (1967) suggests, unlike anthropologists and geologists who assemble facts about the past based on the present, social scientists can work with contemporary data and assume in the future they will observe an event in keeping with their inferences. It is hopeful this research will assist others to identifying conditions conducive for government conspiracies to succeed so that

preemptive measures or countermeasures may be taken to assure greater enlightened citizen understanding.

DATA ANALYSIS AND FINDINGS

Initial Coding: Literature Review

The following is a preliminary list of negative information actions derived from the literature review. This list of negative information actions serves as a form of open coding in that the focus of this study is the public's access to government information as it relates to modern democracies. The following are examples of negative information actions identified during the literature review:

1. Altering information.
2. Deemphasizing information.
3. Destroying information.
4. Misusing executive pardons.
5. Failing to provide retrieval systems.
6. Falsifying information.
7. Hiding information.
8. Obfuscating information.
9. Misusing security classifications.
10. Misusing immunity provisions.
11. Misusing statutory exemptions.
12. Refusing information.
13. Under-funding information offices.
14. Understaffing information offices.
15. Untimely release of information.

Subject Qualification and Selection

The subjects for this analysis were selected for several reasons. The individuals selected were all government employees at the time of the Iran-Contra. Each individual played a role leading to their investigation by the Office of Independent Counsel. With the exception of Fawn Hall who cooperated with the prosecution and was provided criminal immunity, all the subjects were indicted by a grand jury on the basis of their efforts to obstruct justice. The legal relevance used in the prosecution is sufficiently similar, if not unlike, the theoretical relevance sought in this study. While others in government may have committed negative information actions, the actions did not rise to the level of a prosecutable offense. The individual investigations used in this study include the following subjects:

<u>Name</u>	<u>Position</u>
1. Elliot Abrams	Assistant Secretary of State
2. Duane Clarridge	CIA Division Chief
3. Joseph Fernandez	CIA Station Chief
4. Allen Fiers	CIA Task Force Chief
5. Clair George	CIA Deputy Director
6. Fawn Hall	NSC Staff Member
7. Robert McFarlane	National Security Advisor
8. Lieutenant Colonel Oliver North	NSC Counter-Terrorism Expert
9. Vice Admiral John Poindexter	National Security Advisor
10. Casper Weinberger	Secretary of Defense

Negative Information Actions Analysis

While negative information actions may come in a variety of forms from shredding to presidential pardons, they result in the withholding of information from those groups and individuals entitled to the information. The phrase *withholding of information* is generally used to describe several types of negative information actions including, but not limited to altering information, destroying information, hiding information and the misuse of security classifications. Other examples of negative information actions include the misuse of constitutional and statutory provisions, including, but not limited to pardons, immunity, classification laws and privileged communications. Examining negative information actions provides the opportunity to explore related categories including:

1. Objectives.
2. Methods.
3. Information technology use.
4. Knowledge support.

After the information action analysis is conducted, axial coding is used to examine the relationships among objectives, methods, information technology use, and knowledge support. Selective coding is then used to narrow the theoretical issues. Finally, emergent information theory is examined with other selected theories and doctrines of Charles Pigden, Fred Abbate and Robert Dahl to determine the relationship between information flow, conspiratorial groups and democracy.

Objectives

The objectives to be achieved by the conspirator's use of negative information actions related to this analysis include:

1. Protecting superiors.
2. Avoiding detection.
3. Avoiding prosecution.
4. Case dismissal.
5. Conviction reversal.

Methods

The methods utilized by the conspirators included the following negative information actions:

1. altering information,
2. classification misuse,
3. delaying information,
4. destroying information,
5. false statements,
6. immunity misuse,
7. misleading statements,
8. pardon misuse,
9. privilege misuse.
10. misuse of statutory provisions.

Altering Information

The most prominent example of altering information is found in the North and Hall investigative files. After North was alerted to the Department of Justice investigation into the Iran arm sales, he began to make hand written revisions to the National Security Council documents. North then instructed Hall to type the revisions and to replace the original documents with the altered ones (see *Final Report*, p. 147; Appendix A, Table 11).

Classification Misuse

In addition to using restricted information and communication equipment from intelligence and military programs to conceal missile shipments to Iran and United States involvement in Nicaragua, several members of the administration used the Classified Information Protection Act (CIPA) as a means to avoid criminal prosecution. For example, Joseph Fernandez, a Central Intelligence Agency section chief requested certain classified information be admitted as evidence of his innocence during his criminal

prosecution. This tactic, known as *graymail*, was also used by North and Poindexter claiming the need for classified information that would not likely be declassified for their defense at trial. The requests to invoke the CIPA provision were used by North and Poindexter to frustrate the prosecution strategy. In the Fernandez case, the administration was concerned the classified documents could result in additional exposure of clandestine government operations in Latin America. Attorney General Richard Thornburg intervened to deny the release of the requested classified documents on the basis of national security. The unreleased information included several facts well-known to the public and others in government. This provided the administration the opportunity to continue to deny well-known facts. Not capable of mounting an adequate defense without the requested documents, the criminal charges were dropped against the section chief (see *Final Report*, 288-292, 565; Appendix A, Table 6).

Delaying Information

The most prominent examples of delaying information include the untimely production of Casper Weinberger's diary notes and George H. Bush's diary. Weinberger and Bush were requested by the prosecution to provide these documents early in the investigation into the Iran-Contra investigation. The information contained in the documents clearly indicated Bush was well-informed with regard to the missile shipments to Iran. These documents were provided to the prosecution after the statute of limitations expired. While the diaries contained information indicating their prior statements were false regarding each man's knowledge regarding the shipments, they could not be prosecuted even though they mislead investigators about their personal knowledge and involvement (see *Final Report*, 405; Appendix A, Table 13).

Destroying Information

A negative information action used by the Reagan administration to hide the missile and arm shipments was simply to destroy any documentary evidence indicating members of the administration complicity in the affair. Fawn Hall testified she shredded stacks of documents and telephone logs indicating McFarlane, Poindexter, and North violated the Boland Amendment by providing weapons and military support to the Contras. The most prominent example of destroying information is found in the North and Poindexter cases where North testified he witnessed Poindexter destroy a presidential Finding directing any information regarding the Iran missile sale should be kept from the CIA director (see *Final Report*, 147-148; Appendix A, Table 9).

False Statements

Perhaps the most used negative information action by those in the Reagan administration was to simply lie. The false statements put forth by the administration ranged from cover stories provided during press conferences to false statements and perjured testimony before various members and committees in Congress. Also, there was a group effort to create a false chronology of related events to provide consistency to the administration's position that the president was unaware of the missiles for hostages deal (see Appendix A, Table 15).

Immunity Misuse

When Congress provided immunity to Poindexter and North to testify before the Tower commission regarding their knowledge of the secret programs, it was to provide a full public accounting into the government's role in the missile and arms sales. Several members of Congress saw this as an opportunity to insulate and protect the president from further scrutiny. Hoping the immunity would allow Poindexter and North to deny the presidential involvement; several members urged fellow members to grant congressional immunity; which they did (see *Final Report*, 558-559).

Realizing they could not be prosecuted because of their immunized testimony, Poindexter and North readily denied the president's knowledge and their own involvement. Not until Poindexter and North's criminal trials did their recollections

change to include the involvement of individuals higher than themselves. Each then indicated that events originally disavowed during the congressional hearing had actually occurred, but they were simply operating on orders from above, including the president. The use of immunity permitted the creation of not one, but two official versions of the administration's involvement in the Iran-Contra (see *Final Report*, 32-34, 564; Appendix A, Tables 11, 12).

Misleading Statements

Joseph Fernandez gave misleading answers on matters at the heart of the congressional investigations of his activities in Latin America to congressional investigators. While his statements were accurate, they were incomplete and designed to mislead government investigators. It should be noted that the charge of providing misleading information was separate from the charge of making false statements related to the same topics. While one set of charges stemmed from providing incomplete answers the other charges resulted from providing false information (see *Final Report*, 284; Appendix A, Table 6).

Pardon Misuse

An example of presidential pardon misuse was when President George H. Bush pardoned several Reagan administration officials prior to his leaving office. Several cases against administration members were dismissed because of issues involving immunity while others were dismissed because of issues involving the protection of classified information. The remaining government officials who participated in the secret programs and attempted to obstruct Congress received a presidential pardon. Bush indicated the charges against those administration officials were not criminal, but rather political. Bush said the pardons were justified because the individual motivations were patriotic and it was time for the nation to heal. The pardons required the independent counsel to discontinue any further efforts to gather additional information since evidence cannot be collected absent pending charges which no longer existed (see *Final Report*, xxiii-xxiv; Appendix A, Tables 4-5, 7-8, 10, 13).

Privilege Misuse

Probably the most recognized form of privilege associated with government is executive privilege. It should be noted President Reagan did not invoke executive privilege during the Iran-Contra investigation. When asked he voluntarily answered interrogatories regarding his knowledge of the events and provided testimony at trial. President George H. Bush later invoked executive privilege to prevent the release of Reagan's diary. Other types of privilege invoked during the criminal investigation into the Iran-Contra matters included attorney-client privilege. Several individuals used the privilege against self-incrimination which is generally invoked by defendants at the advice of legal counsel.

Privileged communication between a defendant and his or her attorney simply means neither the client nor attorney is compelled to disclose their discussions including case strategy. In North's case the attorney-client privilege was used to further obstruct justice and violate the law. North's attorney, in addition to the normal activities conducted by an attorney on behalf of a defendant, was complicit in removing documents from a secured site and was responsible for coaching the testimony of others participating in the unlawful removal of government documents (see *Final Report*, 148-149; Appendix A, Table 9).

Statutory Misuse

President Reagan cooperated with government investigators by answering interrogatories and providing testimony. After leaving the White House, Reagan retained custody of his diary and personal records that were exempt from disclosure under the Presidential Records Act without a lawfully issued subpoena. The National Archivist and the Bush administration sought to quash the independent counsel's subpoena of Reagan's diary on the basis of executive privilege in an attempt to circumvent the Presidential Records Act. The court upheld the Bush administration's motion to quash and held that any information contained in the diary could have been gathered during Reagan's prior testimony (see *Final Report*, 126-128; Appendix A, Table 12).

Information Technology

The secret nature of conspiracies requires members to communicate undetected to avoid exposure. Military and intelligence agencies throughout the world have relied upon advances in information technology for this. The United States government procures and provides to its military and intelligence units advanced communications equipment and technologies to keep secret operations from being exposed to the nation's adversaries. These technologies are generally restricted to those with access and used are only used for official government purposes.

In the Iran-Contra Affair members of the administration misused communication technologies to avoid detection. For example Poindexter and North misused a PROFS note system and also made it available to civilians, including retired Former National Security Advisor McFarlane, without proper access. A PROFS note system is an IBM proprietary communication network. The PROFS note system was used to store the NSC's secure inter-office email among NSC staff. The use of this technology prevented those not participating in the secret operations from detecting their policy departures. Subsequently North altered the email contained in the PROFS note system and replaced the original electronic notes with the altered ones (see *Final Report*, 94; Appendix A, Table 10).

Another misuse of information technologies was brought to light in Duane Clarridge's trial. Clarridge was a career CIA officer who as chief of the Latin American Division from 1981 to 1984, directed CIA efforts to support the Contras and assisted North in transferring missiles to Iran. Clarridge misused a secured cable system to alert other foreign intelligence units to assist North in his attempt to deliver missiles to Iran. He used a *flash* priority, the second highest priority for CIA cables requiring immediate attention. The precedence higher than *flash*, rarely used is *critic*, which is for events such as an attack on an embassy or a coup. Clarridge misused the cable system to avoid detection. He also maintained exclusive control over the messages. During the course of the investigation the only cables missing from his files were those relating to North's activities. Early in the conspiracy members of the National Security Council, particularly National Security Advisor Robert McFarlane and Secretary of State George Shultz used a

back-channel cable to secret communicate information regarding the missile shipments (see *Final Report*, 90, 249; Appendix A, Tables 5, 10).

While those participating in the secret programs misused advanced electronic information technology to avoid detection and prosecution, a less advanced information technology was also used to destroy information regarding the policy departures. Poindexter, North and Hall used a shredder to destroy hundreds of documents, ledgers and phone logs. While the shredder is not an advanced technology, it was used to achieve the same objective to destroy information of an embarrassing or criminal nature relative to the policy departures. Another example of less advanced information technology used to communicate secret information was the telephone, a pay telephone phone. The pay telephone was used by McFarlane to secretly convey a cover story to be used by North when asked about presidential authorizations. North was to indicate the president made a mental Finding authorizing the missiles shipment to Iran. Using the pay telephone was an attempt to avoid information technology used to record outgoing telephone conversations of government employee working in sensitive programs and offices (see *Final Report*, 116-117, 148; Appendix A, Table, 9, 11, 12).

Knowledge Support

In addition to misusing various information technologies those participating in the secret operation recruited others with specific knowledge and skill sets.

Business and Finance

Those members of the administration participating in the Iran-Contra used knowledge and expertise of those not in government including Secord, Channell and Miller. Richard Secord was a retired Air Force Major General who prior experience included arms sales to middle-eastern countries. Professional fund-raisers Carl R. Channell and Richard R. Miller were recruited to secretly open Swiss bank accounts and to raise large sums of money from foreign heads of state. Even North's attorney Tom Green had a financial interest in the arm sales (see *Final Report*, 84, 105, 187; Appendix A, Tables 10, 11).

Governmental

Members of the conspiracy utilized individuals in the United States government with knowledge and expertise. Many of the individuals possessed operational knowledge while others used their knowledge to aid in the cover up. Individuals within the Central Intelligence Agency provided their knowledge and expertise and included station chiefs and other career officers with experience in covert operations. Non-military personnel in the Department of Defense with procurement experience used their knowledge to assist members of the conspiratorial group to circumvent the Arms Export Act to sell weapons to a recognized terrorist nation. Others in government used their knowledge and expertise to help cover up activities once they were exposed, including the national archivist who together with Bush failed to produce Bush's diary and assisted not once, but twice in the removal and destruction of electronic records from the White House in violation of the Federal Records Act. Several members of Congress pushed to give those participating in the secret programs congressional immunity in order protect the president and to later frustrate the prosecution (see *Final Report*, 32-34, 126-128, 564; Appendix A, Tables 11, 12).

Legal

Individuals with legal knowledge and expertise were used for cover up purposes. Edwin Meese as United State Attorney General failed in his fact finding duties after the exposure of arm sales profits used to provide arms for the Contras. He failed to take notes, held secret White House meetings, and falsely stated Reagan had no knowledge regarding the sale of missiles in exchange for American hostages. Individuals with the Central Intelligence Agency's Office of General Counsel first proposed a retroactive presidential Finding in order keep secret the sale and transport of missiles to Iran via Israel. North's attorney, in addition to investing in the arm sales and crafting Fawn Hall's misleading testimony, instructed North to exercise his privilege against self-incrimination, thereby keeping much of North and his attorney's personal involvement secret (see *Final Report*, 24, 148-149, 319; Appendix A, Table 9, 12).

Military

Several members of the National Security Council participating in the two covert operations had military experience including three Naval Academy graduates, McFarlane, Poindexter and North. As previously mentioned former Air Force Major General Richard Secord used the knowledge and expertise gained on active military duty to carry out the group's objectives. Former Army Major General John K. Singlaub solicited South Korea and Taiwan for military aid for Contras. The transport of missiles and arms to Iran and Nicaragua were initially carried out using CIA, but were later transferred to foreign military aircraft for final delivery (see *Final Report*, 84, 123; Appendix A, Tables 10, 11, 12).

Sample Analyses

Method Codes

M1- Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

- K1 - Business and Finance
- K2 - Governmental
- K3 - Legal
- K4 - Military
- K5 - Political

Table 1: Sample Negative Information Action Analysis No. 1

Subject: Duane R. Clarridge, CIA, Latin American Division Chief

LOC	O	M	NIA	I	K	ID
C1(1)	Avoid Prosecution	M5	Lied re: Weapons Cargo (c)			CM5(1)
C1(2)	Avoid Prosecution	M5	Lied re: North's Info. (c)			CM5(2)
C2(1)	Avoid Prosecution	M5	Lied re: Weapons Cargo (s)			CM5(3)
C2(2)	Avoid Prosecution	M5	Lied re: North's Info. (s)			CM5(4)
C4(1)	Avoid Detection	M7	Created Secord's Secret ID	Y		CM7(1)
C9(1)	Avoid Detection	M7	Coordinated Air Plane Use			CM7(2)
C11(1)	Avoid Detection	M5	Lied re: Cargo Spare Parts			CM5(5)
C12(1)	Avoid Detection	M5	Lied re: CIA Role (i)			CM5(6)
C13(1)	Avoid Prosecution	M5	Lied re: Commercial Deal			CM5(7)
C17(1)	Avoid Detection	M4	Destroyed Cable	Y		CM4(1)
C29(1)	Avoid Prosecution	M5	Lied re: Funds Solicitation			CM5(8)
C2(3)	Avoid Prosecution	M8	Benefited from Pardon		K5	CM8(1)

Table Key

LOC	Location in Investigative File
O	Objective
M	Method Code
NIA	Negative Information Action
I	Information Technology
K	Knowledge Support Code
ID	Identification Code
(c)	Senate Select Committee on Intelligence
(s)	Committee Staff
(i)	Inspector General

Method Codes

M1 - Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 - Political

Table 2: Sample Negative Information Action Analysis No. 2

Subject: Fawn Hall, National Security Council Staff

LOC	O	M	NIA	I	K	ID
H2(1)	Protect Lt. Col. North	M1	Alter E-Documents	Y	K4	HM1(1)
H2(2)	Protect Lt. Col. North	M4	Shred Docs & Logs	Y	K4	HM4(1)
H2(3)	Protect Lt. Col. North	M4	Shred Prof Notes	Y	K4	HM4(2)
H3(1)	Protect Lt. Col. North	M4	Removed Docs		K4	HM4(3)
H4(1)	Protect Lt. Col. North	M5	Craft Testimony (s)		K3	HM5(1)
H4(2)	Protect Lt. Col. North	M5	Craft Testimony (r)		K3	HM5(2)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

(s) - Document Shredding

(r) - Document Removal

Method Codes

M1 - Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

Table 3: Sample Negative Information Action Analysis No. 3

Subject: Vice-Admiral John Poindexter, USN

LOC	OBJECTIVE	M	NIA	I	K	ID
P2(1)	Protect President	M5	Created cover story		K2	PM5(1)
P2(2)	Avoid Detection	M4	Destroyed - Finding	Y	K2	PM4(1)
P2(3)	Avoid Detection	M2	Secret Channel	Y	K2	PM2(1)
P2(4)	Avoid Detection	M4	Delete Messages	Y	K2	PM4(2)
P3(1)	Avoid Prosecution	M5	Reagan Knowledge			PM5(2)
P4(1)	Avoid Prosecution	M6	Congressional Immunity		K3	PM6(1)
P8(1)	Avoid Prosecution	M10	Reagan Diary (p)			PM10(1)
P11(1)	Avoid Prosecution	M5	Directed North to Lie		K4	PM5(3)
P12(1)	Avoid Prosecution	M5	Directed False Chronology		K4	PM5(4)
P13(1)	Avoid Prosecution	M1	Directed Altering Docs		K4	PM1(1)
P21(1)	Conviction Reversal	M6	Congressional Immunity		K3	PM6(2)

Table Key

LOC - Location in Investigative File
O - Objective
M - Method Code
NIA - Negative Information Action
I - Information Technology
K - Knowledge Support Code
ID - Identification Code
(p) - Presidential Records Act

Method Codes

M1 - Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 - Political

LEGAL ENVIRONMENT – IMPEDIMENTS TO INFORMATION FLOW

The theoretical issues relevant to this study have been, for the most part, narrowed to issues surrounding impediment to information flow. Constitutional checks and balances and the rule of law may serve as impediments to information flow. While the rule of law is expected to provide the legal means to settle disagreements and to provide justice, the very elements assuring fairness in the United States legal system may be misused to frustrate public accountability and in turn used to diminish enlightened citizen choice. Legal issues surrounding privileged communication, immunity, classified information, time limitations and pardons can be either beneficial or detrimental depending on the use or misuse of the legal system and the rule of law.

Privileged Information

There are several types of privileged communications including executive, attorney-client communication, privilege against self-incrimination and others not relevant to this study. While many of these rights are constitutional, many are legislated and others evolve out of tradition. Executive privilege evolved out of tradition because of the need for advisors to speak frankly to the president without fear of reprisal from others with competing agendas. While Reagan did not invoke executive privilege during the Iran-Contra, Bush in his succession as president did so during the investigation into the cover-up when he and the national archivist sought to prevent the release of his diary located in the presidential records held at the National Archives.

Attorney-client privilege is a statutory creation providing inaccessibility to anyone other than the client and his attorney. Even if the attorney is complicit in an underlying crime he is not required to disclose any conversations with his or her client. North's attorney, Thomas Green's, was complicit in the affair in that he was a chief investor in the arms deal. Also, Fawn Hall testified regarding North's attorney's attempt to coach and craft testimony favorable to his client.

In addition to privileged communications between an attorney and his client, an attorney may recommend a client invoke his or her right against self incrimination. The right against self incrimination is a constitutional right found in the Fifth Amendment. Although a defendant may possess information relative to an ongoing investigation he or she may simply remain silent. The information issues related to enlightened citizen understanding with regard to privileged information is unlike classified information that will be declassified at a later date, privileged information remains inaccessible.

Immunized Information

Immunity provisions, whether congressional or criminal, provide an opportunity for individuals to freely provide information without fear of prosecution from those seeking the information. Congressional immunity can be used to frustrate future criminal investigations and prosecutions. In the Iran-Contra Affair congressional immunity was used as a prosecutorial impediment. From the beginning of the inquiries into the United States involvement in Central America, the aims of Congress and the independent counsel were at odds. Congress was interested in a full and accurate public accounting of the alleged activities and was not concerned with prosecuting individuals. By providing immunity to those being investigated by Congress, the independent counsel was prohibited from using any information provided to Congress against the individuals testifying to Congress. Several in Congress viewed this as an opportunity to protect the president through suspect testimony indicating Reagan was not aware of the covert activities undertaken by the National Security Council.

In the instant case immunity help create conflicting information in that Poindexter and North testified to Congress certain activities did not take place and the president could not be aware. North testified other activities occurred without the president's direct knowledge, as well. Later, during the criminal prosecution North and Poindexter indicated they previously denied activities occurred, but they were following orders from above. Determining which version of events to believe created problems for the White House and the prosecution. The information issues related to enlightened citizen

understanding with regard to immunity is conflicting information. Reliability of government information is diminished when there exists more than one official version of the same event.

Classified Information

Restricted information is inherently secret by virtue of its creation within particular agencies, including military and intelligence units, and it has not been subject to the same declassification procedures as classified information. Whether information is restricted or classified, its availability is limited to those with access and a need to know the information. Issues of access and availability limit the public's and those in government's knowledge of secret government programs. Those with clearance and a need to know have the right to access, others do not. Even if an individual has met the access requirements, he or she may be prevented from handling the information because it is no longer or is temporarily unavailable. For example, the Federal Bureau of Investigation agents investigating the Iran-Contra had legal access to North's documents and phone logs. The removal, alteration, or destruction of these documents made them unavailable to investigating agents.

Unlike privileged information that may never be available to anyone other than an attorney and his client, classified information may be declassified at a later date. Whether an administration adheres to the classification schedule established by their predecessors is discretionary. For example, an executive order in place from the Clinton administration to release presidential documents from former presidents after an established period was amended by George W. Bush to prevent the release of those documents at the request of either the former president or the White House. Prior to an expected release of Reagan's documents, the President issued the executive order staying the release. Recently academic researchers successfully litigated to gain the release of Reagan's diary, but its release was too late for immediate research purposes.

Certain government information must be kept secret from our nation's enemies to protect national defense. Not all of the classified information is kept secret to prevent

attacks from foreign adversaries. At times information is made secret for political reasons and not defense reasons. For example, Richard Thornburg prevented release of certain classified information not because it would be a threat to national defense, but because the United States could maintain plausible deniability of its involvement in global affairs. This includes information readily available outside the government and known to many including our enemies. For example, the Nicaraguans knew their harbor in Managua had been mined by the Central Intelligence Agency. Several individuals in government, including the CIA, did not want Americans to learn of its activities in Central America. Foreign and domestic newspapers have frustrated attempts to keep government information secret in the United States. On numerous occasions, newspapers have identified and reported the death of CIA station chiefs in obituaries printed in foreign newspapers. Many times the government insists on the need to preserve *deniability* of well-known facts. The information issue related to enlightened citizen understanding with regard to classified information is availability. Much of classified information is expected to be released to the public according to established declassification schedules. As previously stated, these declassification schedules may be modified depending on an administration's need to keep information from the public and others in government.

Timed Information

The statute of limitations provides that after a prescribed period of time an individual may not be prosecuted for a crime. There are exceptions to the statute of limitations, including murder. Although George H. Bush, as vice president was asked to produce his diary, he failed to produce the diary until after the statute of limitations had expired. This was also the case with Casper Weinberger's notes concerning missile shipments to Iran. While the negative information actions contained in the documents were later known to the public neither Bush nor Weinberger could be held legally accountable since prosecution was no longer an available option. While citizens may

examine dated documents to better understand the underlying facts surrounding a policy departure, they cannot be used to exact justice or to hold public officials accountable for their actions. The timeliness of information is the central information-related issue.

Terminated Information

Presidential pardons are constitutional provisions permitting the president to exempt an individual from the punishment demanded by law for a criminal offense by restoring the rights and privileges forfeited because of the offense. Pardons may be given after a conviction or during an investigation prior to a conviction. It appears pardons may be given to terminate investigations which in turn frustrate public accountability.

In the Iran-Contra case, pardons were given before and after convictions to individuals charged with obstructing Congress and circumventing the rule of law. Once the pardons were given any information related to Bush's role in the affair discovered by examining Weinberger's note or his testimony were rendered mute. The information issue related to enlightened citizen understanding with regard to presidential pardons is information gathering. Evidence of a crime may only be collected when there is a chance of a successful prosecution. Any information previously collected becomes unusable after a pardon.

PIGDEN, ABBATE AND DAHL REVISITED

A secondary literature review provided additional insight into theories and doctrines related to conspiracies and democracy. By comparing the findings of the current study with the condition set forth by Pigden, Abbate's group-danger rationale, and Dahl's criteria for democracy, it is clear negative information action used to circumvent the system of constitutional checks and balances and the rule of law can be carried out secretly with dangerous consequences for democracy.

Pigden: Conspiracy Theory

Charles Pigden (1995) discussed conditions that must be present for conspiracies to occur, including:

1. The belief by conspirators that covert action is necessary to overcome the problems faced by the group.
2. The existence of like-minded individuals who will support their effort without revealing information related to the group activities.
3. The conspirators must believe their efforts will be successful.
4. The existence of sufficient and accessible resources to accomplish their objectives.

The conditions and factors necessary for conspiracies to occur were present during Iran-Contra Affair. Although the initial conspiracy charges against North, Poindexter, Secord and Hakim were dismissed, the ruling was based on legal issues directly related to prior congressional grants of immunity and not the underlying facts. The Reagan administration was at odds with the Congress because of an untimely revelation of covert support to the Contras by Central Intelligence Director William Casey. The information should have been provided in a timely manner to members of the Intelligence Oversight Committee. The mining of Managua Harbor in Nicaragua by the Central Intelligence Agency should have been disclosed to Congress. As a result the Boland Amendment cutting off congressional funding for militarily arms and military

support to the Contras passed in Congress and was signed into law. This frustrated the administration's long range goal of preventing the expansion of communism in Central America. The administration secretly took steps to continue providing covert military support outside the oversight of Congress in violation of the Boland Amendment.

In addition to the issue of communist expansion in Central America, the administration also participated in an aggressive campaign to discourage countries from providing arms to sponsors of terrorism including Iran. Iran was placed on the terrorist list because of prior kidnappings of Americans in Tehran during the Carter administration. The Reagan administration now faced a second round of American kidnappings by Iranians in Beirut, Lebanon. Having publicly proclaimed the United States government would not deal with terrorists, the administration sought ways to gain the release of hostages, including secretly trading arms to Iran for hostages in violation of the Arms Export Act, once again outside the oversight of Congress. The shadow of communism also hung over the secret Iran Initiative. Iran was at war with Iraq and needed weapons in the effort. If the United States did not secretly provide weapons to Iran the Soviet Union could have while creating a political foothold in the Middle East by supporting Iran. Based on the above, certain members of the United States government participating in the secret programs felt covert action was necessary to overcome the problems faced by the Reagan administration. The first condition offered by Pigden was met by this covert action.

Certain members of United States government participating in the secret programs also met the second condition provided by Pigden in that like-minded individuals in and outside the group attempted to support their efforts without revealing information related to group activities. With a few exceptions of those who remained silent, members in the Reagan administration, including several cabinet members, agency heads and National Security Council staff took measures including negative information actions to support the secret programs. Outside secret supporters included several foreign heads of state and wealthy Americans including Ross Perot and the Colorado beer magnate, Joseph Coors. Coors even shook North's hand in full view of the jury. Former United States military generals could also be counted as outside secret supporters. This included Army Major

General John Singlaub who saluted North from the witness stand during his testimony against North.

Pigden's third condition was met when the Reagan administration transferred the Nicaraguan Operation responsibilities from the Central Intelligence Agency to the National Security Council and staff to secretly avoid congressional oversight. The use of secret emissaries to Iran and secret meetings between United States government officials and foreign leaders on different continents were designed to keep hostage negotiations secret. Swiss bank accounts were used to prevent congressional oversight and evade financial oversight by the Government Accounting Office. Another finding related to the group's ability to maintain secret support was the use of secret programs and information technologies not readily available outside the national security and intelligence community. Together, the use of secret negotiations, off-the-books accounting, inherently secret means of communication and record keeping allowed the conspirators to believe their actions would be undetected by those charged with oversight responsibilities resulting in their success.

Pigden's fourth and final condition was met with the availability of secret funding, secret transport, off-the-books accounting, inherently secret means of communication and record keeping that provided certain members of the Reagan administration the means and resources to successfully conduct secret program outside the oversight of congress and others in government. The Enterprise amassed millions of dollars in assets including aircraft, a freighter, land and munitions. These examples demonstrate that government officials participating in the Iran-Contra met the conditions of a conspiratorial group.

Abbate: Conspiracy Doctrine

According to Fred Abbate (1974), a conspiracy exists when two or more persons combine to commit an unlawful act or to commit a lawful act using unlawful means. Legal scholars address these unlawful activities in what is known as the *conspiracy doctrine*. The conspiracy doctrine provides a legal framework to protect society from the anti-social effects of conspiracies by awarding criminal sanctions usually higher than a penalty for the underlying criminal violation itself. The enhanced punishment for those who combine and conspire to commit criminal violations is based on four factors known as the *group-danger rationale* (Abbate, 1974). Those factors are:

1. An individual is more likely to carry out group commitments than his personal commitments.
2. Group involvement decreases the likelihood a member would remove himself from the group without the approval of other members.
3. Increased probability covert action will succeed.
4. Likelihood that greater harm will occur than intended by an individual.

Abbate's first factor was evidenced during the independent counsel investigation identifying a national commitment to prevent the expansion of communism and to gain the release of American hostages. Issues involving loyalty, patriotism and commitment outweighed the vested interests of any one individual, including the possibility of fines, imprisonment and damage to reputation.

Although a few members of the conspiracy were less than enthusiastic with the group's direction and were removed from the information loop, their tacit silence, their failure to produce requested notes and to cooperate with Congress and investigators demonstrated their reluctance to leave the group or expose the secret programs. These actions demonstrate the existence of Abbate's second factor.

The third factor is identified by the group's ability to successfully keep undetected two secret government programs and to gather resources sufficient to maintain and continue the programs. If not for the exposure resulting from the Nicaraguan airplane shooting and a crewman's capture combined with an article printed in a Lebanese

newspaper about the government's attempts to trade arms for hostages, the secret programs may have continued unnoticed to those outside the group.

Abbate's fourth factor was demonstrated when the group managed to temporarily circumvent congressional oversight through a concerted effort by several members on multiple occasions to deceive through the use of negative information actions including false and misleading testimony, destruction of documents and misuses of constitutional and statutory provisions. The government officials participating in the secret government programs and their use of negative information actions demonstrates all of the factors identified in the group-danger rationale.

Dahl: Democratic Theory

Robert Dahl (1998) identified five criteria a government must meet to be considered fully democratic:

1. Effective participation—equal and effective opportunities for citizens to make their views on policy known to others.
2. Voting equality—equal and effective opportunities for citizens to vote and have their vote counted equally.
3. Enlightened understanding—equal and effective opportunities for citizens to learn about relevant alternative policies and possible consequences.
4. Exercising final control of the agenda—policies are always open to change by citizens if they so choose.
5. Inclusion of adults—adult citizens who are permanent residents should have all of the rights implied in the first four criteria.

United States citizens were deprived of the opportunity to make their policy views known to other citizens and their government representatives regarding the Reagan administration secret programs. For example, a lack of knowledge of missile shipments to Iran or arms supplies to the Contras prevented citizens and groups who would have publicly opposed such programs from making their views known. In a representational democracy, it is important for representatives in Congress to make their constituents

views known to the administration through legislation and policy formation. These congressional mandates were known and ignored by the Reagan administration. The end result is not unlike many forms of censorship: a citizen's ignorant silence is interpreted as tacit approval by those in the administration. The Reagan administration failed to provide United States citizens and groups the opportunity to voice opposition to the secret programs either directly or indirectly through legislative representatives. Dahl's first criterion of democracy was not met during the Iran-Contra Affair when the administration prevented effective political participation by its citizens.

Dahl's second criterion requires citizens to have equal and effective opportunities to vote and to have the votes counted equally. By ignoring the legislation passed by a duly elected Congress, the Reagan administration's end result was the same as if no vote was cast or any legislation passed. For practical purposes, when administration officials ignored the congressional vote count and violated the Boland Amendment, they substituted their own vote for the votes of citizens and legislative representative. Dahl's second criterion was not met in this regard to voting equality.

The third criterion requires equal and effective opportunities for citizens to learn about relevant alternative policies and the possible consequences. This condition was not met since there were secret programs not known to citizens and Congress. Undue secrecy surrounding the missile sales to Iran or the provision of military arms to the Contras prevented the public from learning about relevant alternatives and consequences, thereby denying citizens an opportunity to gain an enlightened understanding of the administration's secret programs.

The fourth criterion was not met in that citizens, through their elected representatives, could not determine the government's agenda to effect change. Decisions regarding whether to vote for incumbent political candidates, including those participating in the secret programs, or to vote for other candidates to effect change in the agenda was frustrated by undue secrecy.

The fifth criterion requires adult citizens who are permanent residents to have all of the rights implied in the first four criteria. Having failed to meet the first four criteria, the Reagan administration's secret government programs effectively excluded many adult citizens who were entitled to the withheld information. The citizens were denied the

information and thereby prevented from participating and were excluded from the political processes.

THEORETICAL FRAMEWORK AND MODEL

Based on the above conditions, factors, and criteria related to conspiracy and democracy, the negative information actions used by the Reagan administration to carry out the Nicaragua operation and the Iran initiative had a direct impact on a citizen's political participation with regard to their enlightened understanding of government activities. Constitutional checks and balances and the rule of law have been traditionally used to keep government accountable to itself and its citizens. Constitutional provisions may be readily used to circumvent the delicate balance among the three branches of government. Constitutional provisions including pardons and immunity should not be used to encourage or facilitate unconstitutional and criminal behavior by those in government. It has been long recognized government secrecy is acceptable in a democracy to protect citizens and preserve national security. The United States secrecy structure attempts to balance national security interests with a citizen's right to access government information needed to make informed decisions related to political participation. While it is difficult, if not impossible to measure negative information actions, it is possible to identify the type of negative information actions and locate these actions on a continuum of enlightened citizen understanding. The author's Negative Information Action Model is designed to demonstrate the relative impact of different types of information actions on enlightened citizen understanding and choice (see Table 1).

This model is used to locate deliberate and willful information actions either in accordance with or not in accordance with the rule of law or the system of checks and balances. The continuum runs from enlightened citizen understanding to unenlightened citizen understanding. Information actions identified and located on the extreme left are in keeping with the established secrecy structure, and enlightened citizen understanding while information actions found on the extreme right provide no information serving to enlightened citizen choice. The closer an information action is located to the right, the less enlightened citizen choice.

The five types of information actions affecting enlightened citizen choice are:

IA1. Information actions in accordance with the rule of law and the system of checks and balances and are conducted in accordance with the established secrecy structure,

IA2. Information actions not in accordance with either the rule of law or the system of checks and balances that are fully revealed and fully prosecuted. For example, a defendant agrees to provide requested information to the prosecutor and serves a lesser sentence.

IA3. Information actions not in accordance with either the rule of law or the system of checks and balances where the revelation is partially revealed and fully prosecuted. For example, one or more counts in a defendant's case are dismissed because he or she cannot prepare an adequate defense, but other counts are fully prosecuted.

IA4. Information actions not in accordance with either the rule of law or the system of checks and balances where the revelation is either partial or untimely and not fully prosecuted. For example, withheld information or untimely information rendered useless to the prosecution because of the statute of limitations.

IA5. Information actions not in accordance with either the rule of law or the system of checks and balances that remain unknown and are not prosecuted. For example, the identities and actions of undiscovered conspirators not revealed to the public.

It should be noted information actions in keeping with the secrecy structure (IA1.) generally have declassification dates at which time things not previously known to the public will be revealed according to established declassification schedules.

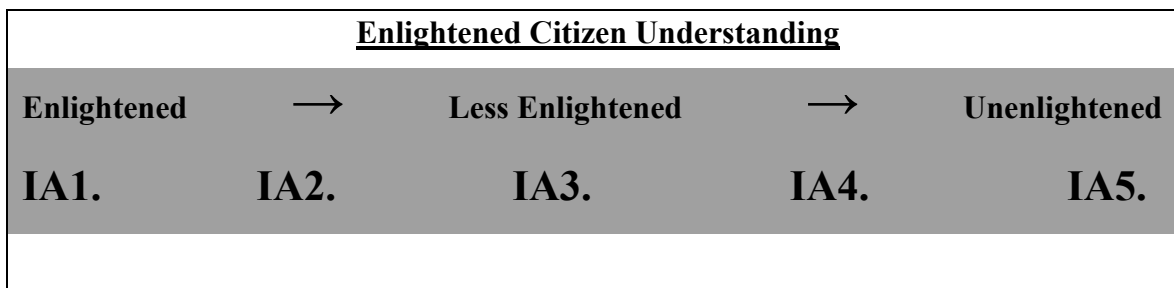


Figure 1: Negative Information Action Model (Hinson, 2007)

An example of the impact of negative information actions on enlightened citizen understanding may be demonstrated by assigning a location on a continuum of enlightened citizen understanding according to their type (see Table 2).

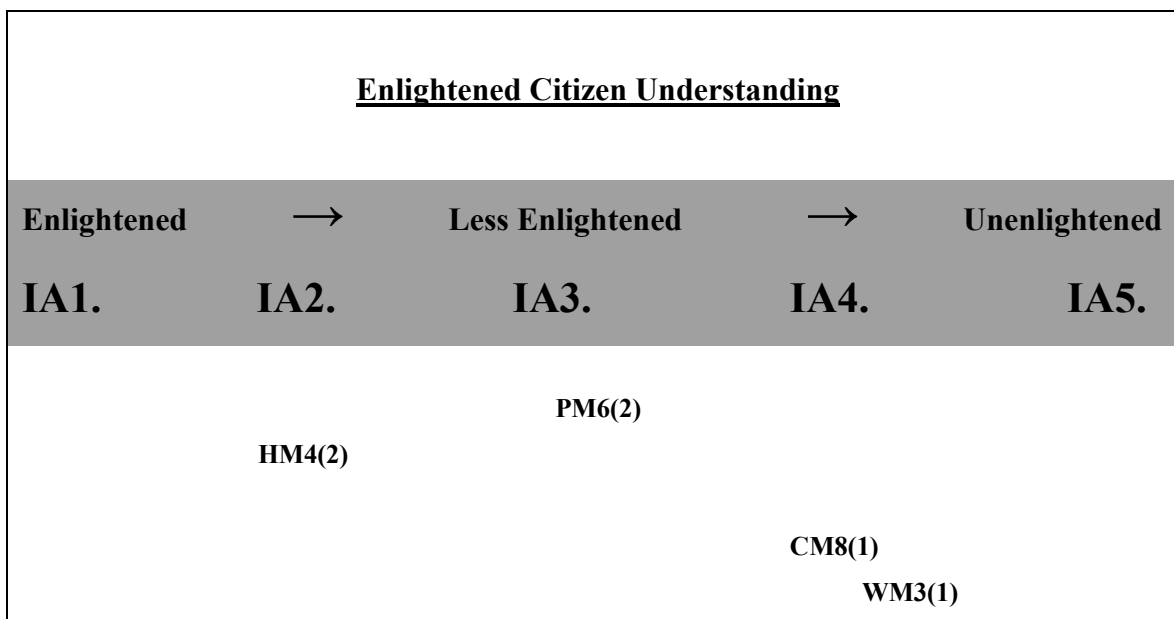


Figure 2: Example Using Negative Information Action Model (Hinson, 2007)

HM4(2) Fawn Hall shredded documents sought by the Federal Bureau of Investigation, but by cooperating with the Independent Counsel was not charged with a crime. Hall's information actions were not in accordance with either the rule of law or the system of checks and balances, but were fully revealed and fully prosecuted. Hall's position is located on or near IA2. on the continuum of enlightened citizen understanding.

PM6(2) John Poindexter invoked congressional immunity during his trial and his conviction was reversed on the same basis and not fully prosecuted. Poindexter's conflicting testimony during congressional and criminal hearings were different and his actions could not be fully known. Poindexter's position is located somewhere on or to the right of IA3. on the continuum of enlightened citizen understanding.

CM8(1) Duane Clarridge obstructed Congress, but was pardoned after his indictment and as a result was not fully prosecuted. Because he failed to cooperate with the CIA Inspector General or the FBI investigators many of his actions were partially revealed. Clarridge's position is located on or near IA4. on the continuum of enlightened citizen understanding.

WM3(1) Casper Weinberger denied having notes of meetings indicating several members were aware of the missile shipments that were in exchange for hostages. His notes on the underlying facts were discovered too late to use as evidence in a criminal trial. Since the statute of limitations expired with regard to the evidence contained within the notes, he received a pardon before trial he and others could not be fully prosecuted. His actions draw questions to whether he was ever completely forthright with congressional and criminal investigators. His actions remain partially known and not prosecuted. Weinberger's position is also located on or to the right of IA4. on the continuum of enlightened citizen understanding.

CONCLUSIONS AND RECOMMENDATIONS

A democracy's legal environment generally used to promote public accountability and justice, when misused produces negative information actions that subvert citizen choice. The legal environment as it exists may be misused to frustrate public accountability and justice. Changes of constitutional and statutory provisions may be made to diminish the impact of negative information actions. The constitutional authority of the president to pardon and the constitutional rights of privilege must be revised to allow for a complete and documented investigation. Restricting a president's use of pardons until after a completed investigation or limiting government officials use privilege may be required. Restricting the use of congressional immunity in a criminal trial would be needed to overcome current shortcomings. A longer statute of limitations may be required when dealing with newly discovered, but previously withheld information related to negative information actions committed by those in government. Legislation should mandate the declassification of information well known to the public where the released information does not cause national harm or was used to hide embarrassing or criminal information. Constitutional and statutory adjustments are required to reduce negative information actions related to the legal environment.

Government conspiracies by their secret nature impact enlightened citizen choice and the constitutional system of checks and balances. The group-danger rationale found in the conspiracy doctrine provides a basis that when applied to the system of checks and balances demonstrates how a relatively small group of individuals working together can subvert the popular control of government through the use of negative information actions. Governments possess and have access to resources required by those participating in government conspiracies. Those individuals must have access to resources created for the purpose of communicating secretly. The resources are made available from those agencies and groups within government with measures in place to prevent outside knowledge of their existence or use. The information related resources used by the government conspirators include restricted information technologies and specialized knowledge bases. Until adequate measures are in place to guarantee restricted

information technologies will not be misused by individuals in government, other conditions required for successful conspiracies to occur must be the focus of preventive measures.

Any member of a government conspiracy previously found guilty of the underlying facts relating to obstructing Congress or criminal investigations, or other negative information actions, should not be permitted to serve in any future government capacity. Case dismissals, reversal of convictions, grants of immunity and pardons do not erase the impact of the underlying negative information action and may serve to increase the danger created by the conspirators and its impact on the popular control of government. Certain individuals have been permitted to continue government employment because of a pardon or conviction reversal. This practice should be prohibited. This is further discussed in the section related to future research.

Based on the democratic criteria set forth by Dahl and Abbate's group-danger rationale, negative information actions can dangerously impact democracy. Negative information actions impact each of the five criteria of democratic theory, particularly enlightened citizen choice. The Negative Information Action Model may be used to locate the relative impact of negative information actions on enlightened citizen choice in any type of democratic setting. The model may be used to locate the impact of negative information in all types of democratic government, including putative democracies, procedural democracies, representative democracies, and full democracies.

FUTURE RESEARCH

Richard Secord's hand written notes discovered during the Iran-Contra Affair included a list of objectives to be achieved during the secret Iran initiative (Draper, 1991). An objective found in the list was to depose the president of Iraq, Saddam Hussein. Hussein was not captured and hung until the George W. Bush administration. Given the intelligence failures relating to terrorist attacks on the United States and the mishandling of information relied upon to enter the war, one must question the manifest reasoning, a direct relationship among Hussein and middle-eastern terrorists. Evidence examined by the 9/11 Commission found no direct relationship between Hussein and the terrorists. Given the United States predisposition to depose Saddam Hussein and the false and misleading statements circulated by the Bush administration during the debate to invade Iraq, future research into information actions related to disinformation, misinformation, propaganda, and other negative information actions and their impact on the decision to go to war in Iraq is recommended.

While this dissertation examined negative information actions designed to circumvent laws and policies with regard to the established secrecy structure, there exists other violations of the secrecy structure not addressed. The leaking of secret information and the misuse of declassification provisions within the established secrecy structure as negative information actions is recommended for future research. For example, the negative information actions to be examined are directly related to intentional leaks and premature declassification of secret information for political purposes. Recently, issues of this nature came to light in regard to the disclosed identity of CIA operative Valerie Plame. Her husband, a former ambassador, was at odds with George W. Bush's reasons to enter the war with Iraq. Recently Richard Armitage, who was also investigated in the Iran-Contra Affair, was identified by the investigating prosecutor as the individual who leaked the identity of Plame.

As Pigden prescribed, certain conditions must be met in order for a conspiracy to occur. The first two conditions require there exist a belief by conspirators covert action is necessary to overcome the problems faced by the group and the existence of like-minded

individuals who will support their efforts without revealing information related to the group activities. An issue that may be further researched is the existence of like-minded individuals working covertly to achieve a common objective. There are a number of individuals participating in the Iran-Contra Affair during the Ronald Reagan and George H. Bush administrations. Individuals who served or are serving in the George W. Bush administration who were investigated to their role in the Iran-Contra include Elliot Abrams, Robert Gates, Colin Powell, John Poindexter, and Richard Armitage. It should be noted Abrams and Poindexter were previously convicted in federal court for obstructing justice. As previously mentioned, Richard Armitage was identified by a federal prosecutor as the individual who leaked the identity of Valerie Plame. Although not part of the George W. Bush administration, George Shultz and Edwin Meese, who were investigated during the Iran-Contra Affair, served on the 9/11 Commission investigating shortcomings leading to the invasion and the United States occupation in Iraq. Would individuals whose information actions were previously brought into question be more likely to carry out negative information actions for an administration than those without prior experience? The predisposition of individuals to use negative information actions to circumvent constitutional checks and balances or the rule of law should be researched.

Upon the death of former President Gerald Ford, several public officials and dignitaries praised him for allowing the nation to heal in the wake of Watergate when he pardoned President Richard Nixon. President George H. Bush indicated he pardoned those individuals participating in the Iran-Contra Affair to allow the country to move on. The facts indicate Ford did not have to pardon Nixon before a full and public accounting had taken place. Rather than examining issues not revealed at the time of the pardon to fully understand the underlying problem, Bush like Ford failed to allow for an exhaustive investigation of the facts related to the policy departures in the Iran-Contra Affair. After pardoning those participating in the Iran-Contra Affair, Bush explained their conduct was patriotically motivated and not criminal. Regardless of the explanation their actions were criminal and committed outside the constitutional system of check and balances.

Themes of national healing and patriotism were raised again after the terrorist attacks in New York and Washington, D. C. In what appeared to be an attempt to heal

the nation, President George W. Bush signed several executive orders to protect the nation from further harm. In actuality, under the theme of national healing, the administration undertook activities of questionable nature including domestic spying. The legislation following the terrorist attacks was popularly known as the USA PATRIOT Act. Those who opposed its questionable provisions were characterized as unpatriotic by those seeking to expand presidential authority not found in the constitution. Citizens not aware the legislation's actual title was Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act may have inferred from the use of the acronym by administration members their patriotism would be questioned by others if they found provisions within the legislation troubling. Do themes of national healing and patriotism diminish the public's perception of negative information actions and their impact on democracy? This question and others should be addressed in future research concerning a possible correlation among an increased use of thematic references and later discovered negative information actions.

It is suggested future research include the study of leaks and the misuse of the secrecy structure for political purpose, information actions related to disinformation, misinformation and propaganda, and the like-mindedness and predisposition of individuals previously associated with negative information action events. The use of thematic information designed to suppress dissent of government programs is also recommended for additional research.

APPENDIX A: ANALYSIS DATA

Table 4: Elliot Abrams, Assistant Secretary of State for Inter-American Affairs

LOC	O	M	NIA	I	K	ID
A1(1)	Avoid Detection	M3	Contra Assistance Activities (s)			AM3(1)
A1(2)	Avoid Detection	M3	Contra Assistance Activities (h)			AM3(2)
A1(3)	Avoid Detection	M3	Sultan of Brunei Contributions (s)			AM3(3)
A1(4)	Avoid Detection	M3	Sultan of Brunei Contribution (h)			AM3(4)
A14(1)	Avoid Detection	M7	Coordinated Misstatements		K2	AM7(1)
A18(1)	Avoid Detection	M5	Denied Government Knowledge (sc)			AM5(1)
A25(1)	Avoid Detection	M5	Denied Gomez Connection to VP (s)			AM5(2)
Chrono	Case Dismissal	M8	Benefited from Presidential Pardon		K5	AM8(1)

Table Key

LOC - Location in Investigative File
 O - Objective
 M - Method Code
 NIA - Negative Information Action
 I - Information Technology
 K - Knowledge Support Code
 ID - Identification Code
 (h) - House Permanent Select Committee on Intelligence
 (s) - Senate Foreign Relations Committee
 (sc) - Senate Committee on Foreign Relations

Method Codes

M1 - Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
 K2 - Governmental
 K3 - Legal
 K4 - Military
 K5 - Political

Table 5: Duane R. Clarridge, CIA, Latin American Division Chief

LOC	O	M	NIA	I	K	ID
C1(1)	Avoid Prosecution	M5	Lied re: Weapons Cargo (c)			CM5(1)
C1(2)	Avoid Prosecution	M5	Lied re: North's Info. (c)			CM5(2)
C2(1)	Avoid Prosecution	M5	Lied re: Weapons Cargo (s)			CM5(3)
C2(2)	Avoid Prosecution	M5	Lied re: North's Info. (s)			CM5(4)
C4(1)	Avoid Detection	M7	Created Secord's Secret ID	Y		CM7(1)
C9(1)	Avoid Detection	M7	Coordinated Air Plane Use			CM7(2)
C11(1)	Avoid Detection	M5	Lied re: Cargo Spare Parts			CM5(5)
C12(1)	Avoid Detection	M5	Lied re: CIA Role (i)			CM5(6)
C13(1)	Avoid Prosecution	M5	Lied re: Commercial Deal			CM5(7)
C17(1)	Avoid Detection	M4	Destroyed Cable	Y		CM4(1)
C29(1)	Avoid Prosecution	M5	Lied re: Funds Solicitation			CM5(8)
C2(3)	Avoid Prosecution	M8	Benefited from Pardon		K5	CM8(1)

Table Key

LOC - Location in Investigative File
 O - Objective
 M - Method Code
 NIA - Negative Information Action
 I - Information Technology
 K - Knowledge Support Code
 ID - Identification Code
 (c) - Senate Select Committee on Intelligence
 (s) - Committee Staff
 (i) - Inspector General

Method Codes

M1 - Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
 K2 - Governmental
 K3 - Legal
 K4 - Military
 K5 - Political

Table 6: Joseph F. Fernandez, CIA Station Chief

LOC	OBJECTIVE	M	NIA	I	K	ID
F2 (1)	Avoid Detection	M5	Costa Rican Air Strip			FM5(1)
F2 (2)	Avoid Detection	M5	Costa Rican Defense			FM5(2)
F2 (3)	Avoid Detection	M5	Involvement (q)			FM5(3)
F2 (4)	Avoid Detection	M5	Involvement (n)			FM5(4)
F2 (5)	Avoid Detection	M5	Weapons Supply			FM5(5)
F3(1)	Avoid Detection	M7	Airstrip Operations			FM7(1)
F3(2)	Avoid Detection	M7	Re-supply Operation			FM7(2)
F3(3)	Avoid Detection	M7	Relationship (n)			FM7(3)
F3(4)	Avoid Detection	M7	Relationship (r)			FM7(4)
F10(1)	Avoid Prosecution	M6	Invoked Congress. Immunity		K3	FM6(1)
F10(2)	Avoid Prosecution	M2	Invoked CIPA (f)		K3	FM2(1)
F16(1)	Case Dismissal	M2	Invoked CIPA (a)		K2	FM2(1)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

(a) - Attorney General

(d) - Fernandez

(n) - North

(q) - Quintero

(r) - Rodriguez

Method Codes

M1- Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

Table 7: Allen Fiers, CIA Central American Task Force Chief

LOC	O	M	NIA	I	K	ID
FR1(1)	Avoid Detection	M5	Lied: Identity Max Gomez			FRM5(1)
FR1(2)	Avoid Detection	M5	Lied: CIA-Contra Contact			FRM5(2)
FR1(3)	Avoid Detection	M5	Lied: Identity Benefactors		K1	FRM5(3)
FR1(4)	Avoid Detection	M5	Lied: North's Activities			FRM5(4)
FR2(1)	Avoid Detection	M5	Lied: U.S. Citizen Aid			FRM5(5)
FR2(2)	Avoid Detection	M5	Lied: Account RIG Meeting			FRM5(6)
FR1(5)	Avoid Prosecution	M8	Benefited from Pardon		K5	FRM8(1)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

Method Codes

M1 - Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

Table 8: Clair George, CIA Deputy Director for Operations

LOC	O	M	NIA	I	K	ID
G1(1)	Avoid Prosecution	M2	Invoke CIPA		K3	GM2(1)
G2(1)	Avoid Detection	M5	Lied: Hasenfus (s)			GM5(2)
G2(2)	Avoid Detection	M5	Lied: Identity Max Gomez (s)			GM5(3)
G2(3)	Avoid Detection	M5	Lied: Secord Contact (s)			GM5(4)
G2(4)	Avoid Prosecution	M5	Lied: Hasenfus (g)			GM5(5)
G2(5)	Avoid Prosecution	M5	Lied: Identity Max Gomez (g)			GM5(6)
G2(6)	Avoid Prosecution	M5	Lied: Secord Contact (g)			GM5(7)
G3(1)	Avoid Detection	M3	Compartment Foreign Funds		K2	GM3(1)
G4(1)	Avoid Detection	M7	CIA Authority			GM7(1)
G5(1)	Avoid Detection	M1	Altered Soft Files		K2	GM1(1)
G6(1)	Avoid Detection	M3	Compartment. Nicaraguan Air Def.		K2	GM3(2)
G8(1)	Avoid Detection	M1	Altered Prepared Statement		K2	GM1(2)
G22(1)	Avoid Prosecution	M8	Presidential Pardon		K5	GM8(1)

Table Key

LOC - Location in Investigative File
O - Objective
M - Method Code
NIA - Negative Information Action
I - Information Technology
K - Knowledge Support Code
ID - Identification Code
(s) - Senate Foreign Relations Committee
(g) - Grand Jury

Method Codes

M1- Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 - Political

Table 9: Fawn Hall, National Security Council Staff

LOC	O	M	NIA	I	K	ID
H2(1)	Protect Lt. Col. North	M1	Alter E-Documents	Y	K4	HM1(1)
H2(2)	Protect Lt. Col. North	M4	Shred Docs & Logs	Y	K4	HM4(1)
H2(3)	Protect Lt. Col. North	M4	Shred Prof Notes	Y	K4	HM4(2)
H3(1)	Protect Lt. Col. North	M4	Removed Docs		K4	HM4(3)
H4(1)	Protect Lt. Col. North	M5	Craft Testimony (s)		K3	HM5(1)
H4(2)	Protect Lt. Col. North	M5	Craft Testimony (r)		K3	HM5(2)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

(s) - Document Shredding

(r) - Document Removal

Method Codes

M1 - Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

Table 10: Robert C. McFarlane, National Security Advisor

LOC	O	M	NIA	I	K	ID
M1(1)	Avoid Detection	M3	Compartmentized North's Activities		K2	MM3(1)
M3(1)	Avoid Detection	M3	Secret Trip to Israel		K2	MM3(2)
M4(1)	Avoid Detection	M3	Secret Trip to Raise Funds		K2	MM3(3)
M5(1)	Protect President	M3	Compartmentized Fund Raising		K2	MM3(4)
M9(1)	Avoid Detection	M5	North's Nicaraguan. Involvement (b)			MM5(1)
M9(2)	Avoid Detection	M5	North's Nicaraguan. Involvement (h)			MM5(2)
M9(3)	Avoid Detection	M5	Created Fake ID for North's Travels			MM5(3)
M10(1)	Avoid Detection	M5	Created Fake End-User Certificates			MM5(4)
M13(1)	Avoid Detection	M1	Directed North to Alter Documents			MM1(1)
M13(2)	Avoid Detection	M4	Directed North Destroy Documents			MM4(1)
M15(1)	Avoid Detection	M5	Denied NSC Involvement (s)			MM5(5)
M18(1)	Avoid Detection	M3	Used Private Intermediaries		K2	MM3(4)
M19(1)	Avoid Detection	M5	Lied to Shultz re: Intermediaries			MM5(6)
M34(1)	Avoid Detection	M4	Directed PROF File Purge	Y		MM4(2)
M36(1)	Avoid Detection	M1	Revised Missile Chronology		K2	MM1(2)
M40(1)	Avoid Detection	M3	Used Pay Phone re: Mental Finding	Y	K4	MM3(5)
M43(1)	Avoid Detection	M5	Lied about Saudi Solicitations (hc)			MM5(7)
M43()	Avoid Detection	M7	Lied about Prince Bandar Solicitation			MM7(1)
Chrono	Avoid Prosecution	M8	Benefited from Presidential Pardon		K5	MM8(1)

Table Key

LOC - Location in Investigative File
 O - Objective
 M - Method Code
 NIA - Negative Information Action
 I - Information Technology
 K - Knowledge Support Code
 ID - Identification Code
 (b) - Rep. Michael Barnes
 (h) - Rep. Lee Hamilton
 (hc) - House Committee on Foreign Affairs
 (s) - Senate Select Committee on Intelligence

Method Codes

M1 - Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Table 10 (Continued)

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 – Political

Table 11: Lieutenant Colonel Oliver North, USMC

LOC	O	M	NIA	I	K	ID
N12(1)	Avoid Detection	M5	Lied: Fund Raising (h)			NM5(1)
N12(2)	Avoid Detection	M5	Lied: Fund Raising (hp)			NM5(2)
N12(3)	Avoid Detection	M5	Lied: Fund Raising (hp)			NM5(3)
N12(4)	Avoid Detection	M5	Lied: Military Advice (h)			NM5(4)
N12(5)	Avoid Detection	M5	Lied: Military Advice (hp)			NM5(5)
N12(6)	Avoid Detection	M5	Lied: Military Advice (hp)			NM5(6)
N12(7)	Avoid Detection	M5	Lied: Supply Movement (h)			NM5(7)
N12(8)	Avoid Detection	M5	Lied: Supply Movement (hp)			NM5(8)
N12(9)	Avoid Detection	M5	Lied: Supply Movement (hp)			NM5(9)
N12(10)	Avoid Detection	M5	Lied: Military Advice (hp)			NM5(10)
N12(11)	Avoid Detection	M5	Lied: Military Action (hp)			NM5(11)
N12(12)	Avoid Detection	M5	Lied: Singlaub Contact(hp)			NM5(12)
N12(13)	Avoid Detection	M5	Lied: Fund Raising (hp)			NM5(13)
N12(14)	Avoid Detection	M5	Lied: Owen Contact(hp)			NM5(14)
N12(15)	Avoid Detection	M5	Lied: Advising Owen (hp)			NM5(15)
N12(16)	Avoid Detection	M5	Created False Chronology (hp)		K2	NM5(16)
N12(17)	Avoid Detection	M4	Destroyed Documents (hp)		K2	NM5(17)
N12(18)	Avoid Detection	M5	Lied: NSC Iran Involvement (m)			NM5(18)
N12(19)	Avoid Detection	M5	Israeli Involvement in Iran (m)			NM5(19)
N12(20)	Avoid Detection	M5	Lied: Swiss Banks Account (m)		K1	NM5(20)
N12(21)	Avoid Prosecution	M4	Destroyed Iran-Contra Documents		K2	NM4(1)
N22(1)	Avoid Prosecution	M3	Failed to Provide Letters (i)		K2	NM3(1)
N22(2)	Avoid Prosecution	M3	Failed to Provide Letters (hs)		K2	NM3(2)
N22(3)	Avoid Prosecution	M9	Invoked Self-Incrimination (n)		K3	NM9(1)
N27(1)	Case Dismissal	M2	Invoked CIPA		K3	NM2(1)
N27(26)	Case Dismissal	M6	Invoked Congressional Immunity		K3	NM6(1)

Table Key

LOC - Location in Investigative File
 O - Objective
 M - Method Code
 NIA - Negative Information Action
 I - Information Technology
 K - Knowledge Support Code
 ID - Identification Code
 (h) - House Foreign Affairs Subcommittee
 (hp) - House Permanent Select Committee on Intelligence
 (hs) - House and Senate Intelligence Committees
 (i) - Independent Counsel
 (m) - Edwin Meese
 (n) - Notebook

Table 11 (Continued)

Method Codes

M1 - Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 - Political

Table 12: Vice-Admiral John Poindexter, USN

LOC	OBJECTIVE	M	NIA	I	K	ID
P2(1)	Protect President	M5	Created cover story		K2	PM5(1)
P2(2)	Avoid Detection	M4	Destroyed - Finding	Y	K2	PM4(1)
P2(3)	Avoid Detection	M2	Secret Channel	Y	K2	PM2(1)
P2(4)	Avoid Detection	M4	Delete Messages	Y	K2	PM4(2)
P3(1)	Avoid Prosecution	M5	Reagan Knowledge			PM5(2)
P4(1)	Avoid Prosecution	M6	Congressional Immunity		K3	PM6(1)
P8(1)	Avoid Prosecution	M10	Reagan Diary (p)			PM10(1)
P11(1)	Avoid Prosecution	M5	Directed North to Lie		K4	PM5(3)
P12(1)	Avoid Prosecution	M5	Directed False Chronology		K4	PM5(4)
P13(1)	Avoid Prosecution	M1	Directed Altering Docs		K4	PM1(1)
P21(1)	Conviction Reversal	M6	Congressional Immunity		K3	PM6(2)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

(p) - Presidential Records Act

Method Codes

M1 - Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

Table 13: Casper Weinberger, Secretary of Defense

LOC	O	M	NIA	I	K	ID
W22(1)	Avoid Prosecution	M5	Existence of Notes			WM5(1)
W31(1)	Avoid Detection	M10	Diary (p)		K2	WM2(1)
W33(1)	Avoid Detection	M5	Saudi Arabia Support			WM5(2)
W43(1)	Avoid Detection	M5	Planned Missile Shipment			WM5(3)
W47(1)	Avoid Detection	M5	Replenishment			WM5(4)
W20(1)	Avoid Prosecution	M8	Presidential Pardon		K5	WM8(1)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

(p) - Presidential Records Act

Method Codes

M1- Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

Table 14: Negative Information Action Sorted by Knowledge Support

LOC	O	M	NIA	I	K	ID
FR1(3)	Avoid Detection	M5	Lied: Identity Benefactors		K1	FRM5(3)
N12(20)	Avoid Detection	M5	Swiss Banks Account (m)		K1	NM5(20)
G5(1)	Avoid Detection	M1	Altered Soft Files		K2	GM1(1)
G8(1)	Avoid Detection	M1	Altered Prepared Statement		K2	GM1(2)
M36(1)	Avoid Detection	M1	Revised Missile Chronology		K2	MM1(2)
F16(1)	Case Dismissal	M2	Invoked CIPA (a)		K2	FM2(1)
P2(3)	Avoid Detection	M2	Secret Channel	Y	K2	PM2(1)
G3(1)	Avoid Detection	M3	Compartment Foreign Funds		K2	GM3(1)
G6(1)	Avoid Detection	M3	Compart. Nicaraguan Air Def.		K2	GM3(2)
M1(1)	Avoid Detection	M3	Compartmentized North's Activities		K2	MM3(1)
M3(1)	Avoid Detection	M3	Secret Trip to Israel		K2	MM3(2)
M4(1)	Avoid Detection	M3	Secret Trip to Raise Funds		K2	MM3(3)
M5(1)	Protect President	M3	Compartmentized Fund Raising		K2	MM3(4)
M18(1)	Avoid Detection	M3	Used Private Intermediaries		K2	MM3(4)
N22(1)	Avoid Prosecution	M3	Failed to Provide Letters (i)		K2	NM3(1)
N22(2)	Avoid Prosecution	M3	Failed to Provide Letters (hs)		K2	NM3(2)
N12(17)	Avoid Detection	M4	Destroyed Documents (hp)		K2	NM5(17)
N12(21)	Avoid Prosecution	M4	Destroyed Iran-Contra Documents		K2	NM4(1)
P2(2)	Avoid Detection	M4	Destroyed - Finding	Y	K2	PM4(1)
P2(4)	Avoid Detection	M4	Delete Messages		K2	PM4(2)
N12(16)	Avoid Detection	M5	Created False Chronology (hp)		K2	NM5(16)
P2(1)	Protect President	M5	Created cover story		K2	PM5(1)
A14(1)	Avoid Detection	M7	Coordinated Misstatements		K2	AM7(1)
W31(1)	Avoid Detection	M10	Diary (p)		K2	WM2(1)
F10(2)	Avoid Prosecution	M2	Invoked CIPA (f)		K3	FM2(1)
G1(1)	Avoid Prosecution	M2	Invoke CIPA		K3	GM2(1)
N27(1)	Case Dismissal	M2	Invoked CIPA		K3	NM2(1)
H4(1)	Protect. North	M5	Craft Testimony (s)		K3	HM5(1)
H4(2)	Protect. North	M5	Craft Testimony (r)		K3	HM5(2)
F10(1)	Avoid Prosecution	M6	Invoked Congress. Immunity		K3	FM6(1)
N27(26)	Case Dismissal	M6	Invoked Congress. Immunity		K3	NM6(1)
P4(1)	Avoid Prosecution	M6	Congressional Immunity		K3	PM6(1)
P21(1)	Conviction Reversal	M6	Congressional Immunity		K3	PM6(2)
N22(3)	Avoid Prosecution	M9	Invoked Self-Incrimination (n)		K3	NM9(1)
H2(1)	Protect. North	M1	Alter E-Documents	Y	K4	HM1(1)
P13(1)	Avoid Prosecution	M1	Directed Altering Docs		K4	PM1(1)
M40(1)	Avoid Detection	M3	Used Pay Phone re: Mental Finding	Y	K4	MM3(5)
H2(2)	Protect. North	M4	Shred Docs & Logs	Y	K4	HM4(1)
H2(3)	Protect. North	M4	Shred Prof Notes	Y	K4	HM4(2)
H3(1)	Protect. North	M4	Removed Docs		K4	HM4(3)
P11(1)	Avoid Prosecution	M5	Directed North to Lie		K4	PM5(3)
P12(1)	Avoid Prosecution	M5	Directed False Chronology		K4	PM5(4)
Chronology	Case Dismissal	M8	Benefited from Presidential Pardon		K5	AM8(1)
C2(3)	Avoid Prosecution	M8	Benefited from Pardon		K5	CM8(1)
FR1(5)	Avoid Prosecution	M8	Benefited from Pardon		K5	FRM8(1)
G22(1)	Avoid Prosecution	M8	Presidential Pardon		K5	GM8(1)
Chronology	Avoid Prosecution	M8	Benefited from Presidential Pardon		K5	MM8(1)
W20(1)	Avoid Prosecution	M8	Presidential Pardon		K5	WM8(1)

Table 14 (Continued)

Table Key

LOC - Location in Investigative File
O - Objective
M - Method Code
NIA - Negative Information Action
I - Information Technology
K - Knowledge Support Code
ID - Identification Code
(p) - Presidential Records Act

Method Codes

M1- Altering Information	M6 - Immunity Misuse
M2 - Classification Misuse	M7 - Misleading Statements
M3 - Delaying Information	M8 - Pardon Misuse
M4 - Destroying Information	M9 - Privilege Misuse
M5 - False Statements	M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 - Political

Table 15: Negative Information Actions Sorted by Method

LOC	O	M	NIA	I	K	ID
G5(1)	Avoid Detection	M1	Altered Soft Files		K2	GM1(1)
G8(1)	Avoid Detection	M1	Altered Prepared Statement		K2	GM1(2)
H2(1)	Protect. North	M1	Alter E-Documents	Y	K4	HM1(1)
M13(1)	Avoid Detection	M1	Directed North to Alter Documents			MM1(1)
M36(1)	Avoid Detection	M1	Revised Missile Chronology		K2	MM1(2)
P13(1)	Avoid Prosecution	M1	Directed Altering Docs		K4	PM1(1)
F10(2)	Avoid Prosecution	M2	Invoked CIPA (f)		K3	FM2(1)
F16(1)	Case Dismissal	M2	Invoked CIPA (a)		K2	FM2(1)
G1(1)	Avoid Prosecution	M2	Invoke CIPA		K3	GM2(1)
N27(1)	Case Dismissal	M2	Invoked CIPA		K3	NM2(1)
P2(3)	Avoid Detection	M2	Secret Channel	Y	K2	PM2(1)
A1(1)	Avoid Detection	M3	Contra Assistance Activities (s)			AM3(1)
A1(2)	Avoid Detection	M3	Contra Assistance Activities (h)			AM3(2)
A1(3)	Avoid Detection	M3	Sultan of Brunei Contributions (s)			AM3(3)
A1(4)	Avoid Detection	M3	Sultan of Brunei Contribution (h)			AM3(4)
G3(1)	Avoid Detection	M3	Compartment Foreign Funds		K2	GM3(1)
G6(1)	Avoid Detection	M3	Compart. Nicaraguan Air Def.		K2	GM3(2)
M1(1)	Avoid Detection	M3	Compartmentized North's Activities		K2	MM3(1)
M3(1)	Avoid Detection	M3	Secret Trip to Israel		K2	MM3(2)
M4(1)	Avoid Detection	M3	Secret Trip to Raise Funds		K2	MM3(3)
M5(1)	Protect President	M3	Compartmentized Fund Raising		K2	MM3(4)
M18(1)	Avoid Detection	M3	Used Private Intermediaries		K2	MM3(4)
M40(1)	Avoid Detection	M3	Used Pay Phone re: Mental Finding	Y	K4	MM3(5)
N22(1)	Avoid Prosecution	M3	Failed to Provide Letters (i)		K2	NM3(1)
N22(2)	Avoid Prosecution	M3	Failed to Provide Letters (hs)		K2	NM3(2)
C17(1)	Avoid Detection	M4	Destroyed Cable	Y		CM4(1)
H2(2)	Protect. North	M4	Shred Docs & Logs	Y	K4	HM4(1)
H2(3)	Protect. North	M4	Shred Prof Notes	Y	K4	HM4(2)
H3(1)	Protect. North	M4	Removed Docs		K4	HM4(3)
M13(2)	Avoid Detection	M4	Directed North Destroy Documents			MM4(1)
M34(1)	Avoid Detection	M4	Directed PROF File Purge	Y		MM4(2)
N12(17)	Avoid Detection	M4	Destroyed Documents (hp)		K2	NM5(17)
N12(21)	Avoid Prosecution	M4	Destroyed Iran-Contra Documents		K2	NM4(1)
P2(2)	Avoid Detection	M4	Destroyed - Finding	Y	K2	PM4(1)
P2(4)	Avoid Detection	M4	Delete Messages		K2	PM4(2)
A18(1)	Avoid Detection	M5	Denied Government Knowledge (sc)			AM5(1)
A25(1)	Avoid Detection	M5	Denied Gomez Connection to VP (s)			AM5(2)
C1(1)	Avoid Prosecution	M5	Lied re: Weapons Cargo (c)			CM5(1)
C1(2)	Avoid Prosecution	M5	Lied re: North's Info. (c)			CM5(2)
C2(1)	Avoid Prosecution	M5	Lied re: Weapons Cargo (s)			CM5(3)
C2(2)	Avoid Prosecution	M5	Lied re: North's Info. (s)			CM5(4)
C11(1)	Avoid Detection	M5	Lied re: Cargo Spare Parts			CM5(5)
C12(1)	Avoid Detection	M5	Lied re: CIA Role (i)			CM5(6)
C13(1)	Avoid Prosecution	M5	Lied re: Commercial Deal			CM5(7)
C29(1)	Avoid Prosecution	M5	Lied re: Funds Solicitation			CM5(8)

Table 15 (Continued)

F2 (1)	Avoid Detection	M5	Costa Rican Air Strip			FM5(1)
F2 (2)	Avoid Detection	M5	Costa Rican Defense			FM5(2)
F2 (3)	Avoid Detection	M5	Involvement (q)			FM5(3)
F2 (4)	Avoid Detection	M5	Involvement (n)			FM5(4)
F2 (5)	Avoid Detection	M5	Weapons Supply			FM5(5)
FR1(1)	Avoid Detection	M5	Lied: Identity Max Gomez			FRM5(1)
FR1(2)	Avoid Detection	M5	Lied: CIA-Contra Contact			FRM5(2)
FR1(3)	Avoid Detection	M5	Lied: Identity Benefactors		K1	FRM5(3)
FR1(4)	Avoid Detection	M5	Lied: North's Activities			FRM5(4)
FR2(1)	Avoid Detection	M5	Lied: U.S. Citizen Aid			FRM5(5)
FR2(2)	Avoid Detection	M5	Lied: Account RIG Meeting			FRM5(6)
G2(1)	Avoid Detection	M5	Lied: Hasenfus (s)			GM5(2)
G2(2)	Avoid Detection	M5	Lied: Identity Max Gomez (s)			GM5(3)
G2(3)	Avoid Detection	M5	Lied: Secord Contact (s)			GM5(4)
G2(4)	Avoid Prosecution	M5	Lied: Hasenfus (g)			GM5(5)
G2(5)	Avoid Prosecution	M5	Lied: Identity Max Gomez (g)			GM5(6)
G2(6)	Avoid Prosecution	M5	Lied: Secord Contact (g)			GM5(7)
H4(1)	Protect. North	M5	Craft Testimony (s)		K3	HM5(1)
H4(2)	Protect. North	M5	Craft Testimony (r)		K3	HM5(2)
M9(1)	Avoid Detection	M5	North's Nicaraguan. Involvement (b)			MM5(1)
M9(2)	Avoid Detection	M5	North's Nicaraguan. Involvement (h)			MM5(2)
M9(3)	Avoid Detection	M5	Created Fake ID for North's Travels			MM5(3)
M10(1)	Avoid Detection	M5	Created Fake End-User Certificates			MM5(4)
M15(1)	Avoid Detection	M5	Denied NSC Involvement (s)			MM5(5)
M19(1)	Avoid Detection	M5	Lied to Shultz re: Intermediaries			MM5(6)
M43(1)	Avoid Detection	M5	Lied about Saudi Solicitations (hc)			MM5(7)
N12(1)	Avoid Detection	M5	Lied about Fund Raising (h)			NM5(1)
N12(2)	Avoid Detection	M5	Lied about Fund Raising (hp)			NM5(2)
N12(3)	Avoid Detection	M5	Lied about Fund Raising (hp)			NM5(3)
N12(4)	Avoid Detection	M5	Lied about Military Advice (h)			NM5(4)
N12(5)	Avoid Detection	M5	Lied about Military Advice (hp)			NM5(5)
N12(6)	Avoid Detection	M5	Lied about Military Advice (hp)			NM5(6)
N12(7)	Avoid Detection	M5	Lied about Supply Movement (h)			NM5(7)
N12(8)	Avoid Detection	M5	Lied about Supply Movement (hp)			NM5(8)
N12(9)	Avoid Detection	M5	Lied about Supply Movement (hp)			NM5(9)
N12(10)	Avoid Detection	M5	Lied about Military Advice (hp)			NM5(10)
N12(11)	Avoid Detection	M5	Lied about Military Action (hp)			NM5(11)
N12(12)	Avoid Detection	M5	Lied about Singlaub Contact(hp)			NM5(12)
N12(13)	Avoid Detection	M5	Lied about Fund Raising (hp)			NM5(13)
N12(14)	Avoid Detection	M5	Lied about Owen Contact(hp)			NM5(14)
N12(15)	Avoid Detection	M5	Lied about Advising Owen (hp)			NM5(15)
N12(16)	Avoid Detection	M5	Created False Chronology (hp)		K2	NM5(16)
N12(18)	Avoid Detection	M5	NSC Involvement in Iran (m)			NM5(18)
N12(19)	Avoid Detection	M5	Israeli Involvement in Iran (m)			NM5(19)
N12(20)	Avoid Detection	M5	Swiss Banks Account (m)		K1	NM5(20)
P2(1)	Protect President	M5	Created cover story		K2	PM5(1)
P3(1)	Avoid Prosecution	M5	Reagan Knowledge			PM5(2)
P11(1)	Avoid Prosecution	M5	Directed North to Lie		K4	PM5(3)
P12(1)	Avoid Prosecution	M5	Directed False Chronology		K4	PM5(4)
W22(1)	Avoid Prosecution	M5	Existence of Notes			WM5(1)
W33(1)	Avoid Detection	M5	Saudi Arabia Support			WM5(2)

Table 15 (Continued)

W43(1)	Avoid Detection	M5	Planned Missile Shipment			WM5(3)
W47(1)	Avoid Detection	M5	Replenishment			WM5(4)
F10(1)	Avoid Prosecution	M6	Invoked Congress. Immunity		K3	FM6(1)
N27(26)	Case Dismissal	M6	Invoked Congress. Immunity		K3	NM6(1)
P4(1)	Avoid Prosecution	M6	Congressional Immunity		K3	PM6(1)
P21(1)	Conviction Reversal	M6	Congressional Immunity		K3	PM6(2)
A14(1)	Avoid Detection	M7	Coordinated Misstatements		K2	AM7(1)
C4(1)	Avoid Detection	M7	Created Secord's Secret ID	Y		CM7(1)
C9(1)	Avoid Detection	M7	Coordinated Air Plane Use			CM7(2)
F3(1)	Avoid Detection	M7	Airstrip Operations			FM7(1)
F3(2)	Avoid Detection	M7	Re-supply Operation			FM7(2)
F3(3)	Avoid Detection	M7	Relationship (n)			FM7(3)
F3(4)	Avoid Detection	M7	Relationship (r)			FM7(4)
G4(1)	Avoid Detection	M7	CIA Authority			GM7(1)
M43()	Avoid Detection	M7	Lied about Prince Bandar Solicitation			MM7(1)
Chronology	Case Dismissal	M8	Benefited from Presidential Pardon		K5	AM8(1)
C2(3)	Avoid Prosecution	M8	Benefited from Pardon		K5	CM8(1)
FR1(5)	Avoid Prosecution	M8	Benefited from Pardon		K5	FRM8(1)
G22(1)	Avoid Prosecution	M8	Presidential Pardon		K5	GM8(1)
Chronology	Avoid Prosecution	M8	Benefited from Presidential Pardon		K5	MM8(1)
W20(1)	Avoid Prosecution	M8	Presidential Pardon		K5	WM8(1)
N22(3)	Avoid Prosecution	M9	Invoked Self-Incrimination (n)		K3	NM9(1)
P8(1)	Avoid Prosecution	M10	Reagan Diary (p)			PM10(1)
W31(1)	Avoid Detection	M10	Diary (p)		K2	WM2(1)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

Method Codes

M1 - Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Table 15 (Continued)

Knowledge Support Codes

K1 - Business and Finance
K2 - Governmental
K3 - Legal
K4 - Military
K5 – Political

Table 16: Negative Information Actions Using Information Technology

LOC	O	M	NIA	I	K	ID
C17(1)	Avoid Detection	M4	Destroyed Cable	Y		CM4(1)
C4(1)	Avoid Detection	M7	Created Secord's Secret ID	Y		CM7(1)
H2(1)	Protect. North	M1	Alter E-Documents	Y	K4	HM1(1)
H2(2)	Protect. North	M4	Shred Docs & Logs	Y	K4	HM4(1)
H2(3)	Protect. North	M4	Shred Prof Notes	Y	K4	HM4(2)
M34(1)	Avoid Detection	M4	Directed PROF File Purge	Y		MM4(2)
M40(1)	Avoid Detection	M3	Used Pay Phone re: Mental Finding	Y	K4	MM3(5)
P2(2)	Avoid Detection	M4	Destroyed - Finding	Y	K2	PM4(1)
P2(3)	Avoid Detection	M2	Secret Channel	Y	K2	PM2(1)
P2(4)	Avoid Detection	M4	Delete Messages	Y	K2	PM4(2)

Table Key

LOC - Location in Investigative File

O - Objective

M - Method Code

NIA - Negative Information Action

I - Information Technology

K - Knowledge Support Code

ID - Identification Code

(p) - Presidential Records Act

Method Codes

M1 - Altering Information

M2 - Classification Misuse

M3 - Delaying Information

M4 - Destroying Information

M5 - False Statements

M6 - Immunity Misuse

M7 - Misleading Statements

M8 - Pardon Misuse

M9 - Privilege Misuse

M10 - Statutory Misuse

Knowledge Support Codes

K1 - Business and Finance

K2 - Governmental

K3 - Legal

K4 - Military

K5 - Political

APPENDIX B: GLOSSARY

Arms Export Control Act – legislation requiring congressional notification on arms sales abroad (McCormack & Smith, 1987).

Boland Amendment – legislation prohibiting the use of funds for the purpose of overthrowing governments (McCormack & Smith, 1987).

Central Intelligence Agency – a federal agency responsible for coordinating national security-related information (Black, 1983).

Democratic accountability – popular control of government through periodic elections presenting real choices to an informed electorate.

Democratic criteria – standards required of a democratic government: effective participation by the citizenry, equality in voting, enlightened understanding by the electorate, exercise of final control of the agenda and inclusion of all adults (Dahl, 1998).

Department of Defense – the federal department responsible for national defense.

Department of State – the federal department responsible for foreign affairs.

Export Administration Act – legislation restricting exports to nations supporting terrorism (McCormack & Smith, 1987).

False statements – statements known to be false, or made recklessly without an honest belief in their truth, and with the purpose of misleading others (Black, 1983).

Finding – a presidential document authorizing covert operations by the Central Intelligence Agency unless another agency is designated by the president and subject to Congressional reporting procedures (Draper, 1991, p. 208).

Immunity – a grant prohibiting criminal prosecution in exchange for testimony (Black, 1983).

Information access – is the right to use information.

Information action – a willful and deliberate act designed to provide information to those entitled to it.

Information availability – is the opportunity to use information.

Information policy instruments – a set of interrelated laws, administrative rules and regulations and guidelines related to information and its uses (McClure, 1999).

Intelligence Oversight Act – legislation requiring prior congressional notification of covert operations (McCormack & Smith, 1987).

Misleading statements – statements calculated to misdirect or confuse others (Black, 1983).

National Security Council – according to Huzar (1950, p. 149), the NSC was established to advise the President on integrated information about “domestic, foreign, and military policies relating to the national security.”

Obstruction – an attempt to impede the administration of justice (Black, 1983).

Pardon – An act of grace exempting an individual from the punishment demanded by law for an offense and restores the rights and privileges forfeited on account of the offense (Black, 1983).

State Crime Against Democracy – “concerted actions or inactions by public officials that are intended to weaken or subvert popular control of their government” (deHaven-Smith, 2006, p. 333).

REFERENCES

- Abbate, F. (1974). The conspiracy doctrine: A critique. *Philosophy and Public Affairs*, 3(3), 295-311.
- Allan, G. (2003). *A critique of using grounded theory as a research method*. Retrieved July 1, 2007 from <http://www.ejbrm>
- American Library Association, (2001). *USA Patriot Act: Chronology*. Retrieved February 25, 2003 from <http://www.ala.org/washoff/patriotchron.html>
- Armstrong, S. (1998). The war over secrecy: Democracy's most important low-conflict. In Athan G. Theoharis (Ed.), *A culture of secrecy: The government versus the people's right to know* (pp. 140-185). Lawrence, KS: University Press of Kansas.
- Babbie, E. (2000). *The practice of social research* (9th ed.). Belmont, CA: Wadsworth/Thomson Learning.
- Black, H. C. (1983). *Black's Law Dictionary* (5th ed.). St. Paul: West Publishing Co.
- Brown, R. D. (1996). *The strength of a people: The idea of an informed citizenry in America, 1650-1870*. Chapel Hill, NC: The University of North Carolina Press.
- Buckland, M. K. (1991). Information as a thing. *Journal of the American Society for Information Science*, 42(5), 351-360.
- Cohen, A. (1971). The politic of ritual secrecy. *Man*, 6(3), 427-448.
- Colby, W. E. (1976). Intelligence secrecy and security in a free society. *International Security*, 1(2), 3-14.
- Cook, B. W. (1996). Presidential papers in crisis: some thoughts on lies, secrets, and silence. *Presidential Studies Quarterly*, 26, 285-292.
- Cressey, D. (1967). Methodological problems in the study of organized crime as a social problem. *Annals of the American Academy of Political and Social Science*, 374(Nov.), 101-112.
- Dahl, R. A. (1977). On removing certain impediments to democracy in the United States. *Political Science Quarterly*, 92(1), 1-20.
- Dahl, R. A. (1998). *On democracy*. New Haven, CT: Yale University Press.

- Dahl, R. A. (2000). A democratic paradox. *Political Science Quarterly*, 115(1), 35-40.
- deHaven-Smith, L. (2006). When political crimes are inside jobs: Detecting state crimes against democracy. *Administrative Theory and Praxis*, 28(3), 330-355.
- Demac, D. A. (1984). *Keeping America uninformed: Government secrecy in the 1980's*. New York: The Pilgrim Press.
- Doyle, K. (1999). The end of secrecy: U.S. national security and the imperative for openness. *World Policy Journal*, 16(1), 34-51.
- Draper, T. (1991). *A very thin line: The Iran-Contra affairs*. New York: Hill and Wang.
- Dye, T. R. (1976). *Policy analysis: What governments do, why they do it, and what Difference it makes*. University, AL: The University of Alabama Press.
- Edwards, G. C., & Wayne, S. J. (1990). *Presidential leadership: Politics and policy making* (2nd ed.). New York: St. Martin's Press.
- Elsberg, D. (2004). Secrecy oaths: A license to lie? *Harvard International Review*, 26(2), 16-20.
- Feinberg, L. E. (2004). FOIA, federal information policy, and information policy, and information availability in a post-9/11 world. *Government Information Quarterly*, 21(4), 439-460.
- Galnoor, I. (1975). Government secrecy: Exchanges, intermediaries, and middlemen. *Public Administration Review*, 35(1), 32-52.
- Glaser, B. G. (2004). Remodeling grounded theory. *Forum: Qualitative Social Research* 5(2). Retrieved June 25, 2007 from <http://www.qualitative-research.net/fqs/>.
- Goldstein, A. S. (1959). Conspiracy to defraud the United States. *Yale Law Journal* 68(2), 405-463.
- Gordon-Murnane, L. (2002). Access to government information in a post 9/11 world. *Searcher*, 10(6), 50-62.
- Halstuk, M. (2002). In review: The threat to freedom of information. *Columbia Journalism Review*, 40(5), p. 8.
- Hernon, P., Relyea, H., Dugan, R. E., & Cheverie, J. F. (2002). *United States government information: Policies and sources*. Westport, Ct: Libraries Unlimited.

- Hofman, A. (1993). Opinion, illusion, and the illusion of opinion: Barruel's theory of conspiracy. *Eighteenth Century Studies*, 27(1), 27-60.
- Huzar, E. (1950). Reorganization for national security. *Journal of Politics*, 12(1), 128-152.
- Johnson, R. A., & Kraft, M. E. (1990). Bureaucratic whistleblowing and policy change. *The Western Political Quarterly*, 43(4), 849-874.
- Jost, K. (2005). Government secrecy: Is too much being kept from the public? *CQ Researcher*, 15(42), 1007-1024.
- Katz, S. L. (1987). *Government secrecy: Decisions without government*. Washington, DC: People for the American Way.
- Katzner, D. W. (2001). *Unmeasured information and the methodology of social science*. Norwell, MA: Kluwer Academic Publisher.
- Keeley, B. (1999). Of conspiracy theories. *The Journal of Philosophy*, 96(3), 109-126.
- Kornbluh, P., & Byrne, M. (1993). *The Iran-Contra scandal: The declassified history*. New York: The New Press.
- Ku, Agnes S. (1998). Boundary politics in the public sphere: Openness, secrecy, and leak. *Sociological Theory*, 16(2), 172-192.
- Layder, D. (1993). *New strategies in social research: An introduction and guide*. Cambridge, MA: Polity Press.
- Pandit, N. R. (1996). The creation of grounded theory: A recent application of the grounded theory method. *The Qualitative Report* 2(4). Retrieved July 1, 2007 from <http://www.nova.edu/ssss/QR/QR2-4/pandit.html>.
- Pandit, N. R. (1996). The creation of grounded theory: A recent application of the grounded theory method. *The Qualitative Report* 2(4). Retrieved July 1, 2007 from <http://www.nova.edu/ssss/QR/QR2-4/pandit.html>.
- Pigden, C. (1995). Popper revisited, or what is wrong with conspiracy theories? *Philosophy of the Social Science*, 25(1), 3-34.
- McClure, C. R. (1999). Information policy. In *Encyclopedia of Library and Information Science* (Supp. 65, pp. 306-314).
- McCormick, J. M., & Smith, S. S. (1987). The Iran arm sale and the Intelligence Oversight Act of 1980. *PS*, 20(1), 29-37.

- Mills, C. W. (1959). In L. Gross (ed.). *Symposium on sociological theory*. Evanston, IL: Row, Peterson, & Company, 1959.
- Moynihhan, D. P. (1998). *Secrecy: The American experience*. New Haven, CT: Yale University Press.
- Relyea, H. C. (1981). *The presidency and information policy*. New York: Center for the Study of the Presidency.
- Relyea, H. C. (1996). National security information policy after the end of the cold world. In P. Hernon, C. R. McClure, & H. C. Relyea, (Eds.), *Federal information policies in the 1990s: Views and perspectives* (pp. 165-182). Norwood, NJ: Ablex Publishing Company.
- Renzetti, C. M., & Lee R. M. (1993). *Researching sensitive topics*. Newberry Park, CA: Sage Publications, Inc.
- Rourke, F. E. (1957). Secrecy in American bureaucracy. *Political Science Quarterly*, 72(4), 540-564.
- Russell, J. (1955). The railroads in the “conspiracy theory” of the fourteenth amendment. *The Mississippi Valley Historical Review*, 41(4), 601-622.
- Sanderson, J. (1967). Ingua Cosa Nostra. *American Speech*, 39(4), 304-306.
- Sieber J. E. (1993). The ethics and politics of sensitive research. In C. M. Renzetti, & R. M. Lee (Eds.). *Researching sensitive topics*. Newberry Park, CA: Sage Publications, Inc.
- Smith, B., Fraser, B. T., & McClure, C. R. (2000). Federal information policy and access to web-based federal information. In Bertot, J.C. (Ed.), *Information Policy*, *Journal of Academic Librarianship*, 26(4), 274-281.
- Smith, D. (1976). Mafia: The prototypical alien conspiracy. *Annals of the American Academy of Social Science*, 423(Jan.), 75-88.
- Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.) Thousand Oaks, CA: Sage Publications, Inc.
- Thompson, D. F. (1999). Democratic secrecy. *Political Science Quarterly*, 114(2), 181-193.
- Trochim, W. M. (2001). *The research methods knowledge base* (2nd ed.). Cincinnati: Atomic Dog Publishing.

- United States Commission Protecting and Reducing Government Secrecy. (1997). *Report of the Commission on Protecting and Reducing Government Secrecy*. Washington, DC: U.S. Government Printing Office.
- United States Committee on Government Reform (2004). Secrecy in the Bush administration. Federation of American Scientist website. Retrieved February 24, 2006, from <http://www.fas.org/sgp/library/waxman.pdf>
- United States Congress (1980). *Classified Information Procedures Act PL96-456*. Federation of American Scientist website. Retrieved June 20, 2006, from <http://www.fas.org/irp/offdocs/laws/pl096456>
- United States Constitution (1787). Article I, Section 5. *The Constitution of the United States*. Retrieved April 12, 2005 from http://www.archives.gov/national_archives_experience/charters/constitution.html
- United States Department of Justice (2001). *New attorney general FOIA memorandum issued*. FOIA Post. Office of Information and Privacy Website. Retrieved February 2, 2003 from <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>
- United States Securities and Exchange Commission (2006). *Freedom of Information Act exemptions*. United States Securities and Exchange Commission website. Retrieved April, 10, 2006 from <http://www.sec.gov/foia/nfoia.htm>
- Walsh, Lawrence E. (1997). *Firewall: The Iran-Contra conspiracy and cover-up*. New York: W. W. Norton & Company.
- Walsh, Lawrence E. (1993). *Final report of the Independent Counsel for Iran/Contra matters*. Washington, D.C.: United States District Court of Appeals for the District of Columbia.
- White House (2004). *President signs Intelligence Reform and Terrorism Prevention Act*. White House Website. Retrieved March 27, 2006, from <http://www.whitehouse.gov/news/releases/2004/12/20041217-1.html>

BIOGRAPHICAL SKETCH

Christopher Hinson received his Doctor of Philosophy Degree from the Florida State University College of Information in 2007, his Master of Science Degree from the Florida State University School of Information Studies in 2002, and is expected to complete a second Master of Science Degree from the Florida State University Department of Political Science in 2008.

Hinson was awarded a 2002 Florida State University College Teaching Fellowship. He is a member of Beta Phi Mu International Library and Information Studies Honor Society and a member of Golden Key International Honour Society. Prior to graduation Hinson published a peer-reviewed article in the *Journal of Education for Library and Information Science* in 2005.

Hinson served as a member of United States Navy Ceremonial Guard. His military duties included serving as an escort to President Ronald Reagan and other U.S. and foreign officials and dignitaries in and outside the Washington, D.C. area. His governmental duties included representing the State of Florida in proceedings before the Florida Division of Administrative Hearings.