



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**NAVIGATING TROUBLED WATERS: HOW LEADERS
CAN MORE EFFECTIVELY PREPARE INTELLIGENCE
ENTERPRISES FOR THE RISKS OF INTELLIGENCE
EFFORTS IN TRANSPARENT SOCIETIES**

by

Jeffrey Dambly

September 2018

Co-Advisors:

David W. Brannan (contractor)
Rodrigo Nieto-Gomez

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2018	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE NAVIGATING TROUBLED WATERS: HOW LEADERS CAN MORE EFFECTIVELY PREPARE INTELLIGENCE ENTERPRISES FOR THE RISKS OF INTELLIGENCE EFFORTS IN TRANSPARENT SOCIETIES			5. FUNDING NUMBERS	
6. AUTHOR(S) Jeffrey Dambly				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) For intelligence officials today, understanding the appropriate bounds of balancing security and liberty interests is more imperative than ever. Intelligence enterprises require the consent of their public stakeholders to be effective; running aground of public support threatens significant institutional harms. Leaders can avoid many of these harms if they develop a culture within their organizations that better balances security and liberty interests. This effort can ward off the dangers of a narrative discourse that advocates for "prevention at all costs," which leads to harmful extremes of disregarding public concerns over privacy, civil liberties, and the rule of law. This thesis uses a case study to review the social dynamics in the Bush Administration following 9/11, as a handful of policymakers secretly and unilaterally created and implemented aggressive surveillance programs. Using the social identity perspective, this thesis demonstrates the harms that may befall an organization intent on thwarting all other considerations to prevent a terrorist attack. Ultimately, this thesis provides a model for creating a culture that better balances security and liberty interests, and that ensures a better understanding of how stakeholders view an intelligence enterprise's authorities.				
14. SUBJECT TERMS prevention narrative, social identity theory, intergroup relational identity theory, Stellarwind, surveillance, rule of law, security vs. liberty, leadership, organizational culture, privacy			15. NUMBER OF PAGES 169	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**NAVIGATING TROUBLED WATERS: HOW LEADERS CAN MORE
EFFECTIVELY PREPARE INTELLIGENCE ENTERPRISES FOR THE RISKS
OF INTELLIGENCE EFFORTS IN TRANSPARENT SOCIETIES**

Jeffrey Dambly
Assistant General Counsel, Florida Department of Law Enforcement
BA, University of Florida, 2007
JD, University of Florida, 2010
LLM, George Washington University, 2011

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
September 2018**

Approved by: David W. Brannan
Co-Advisor

Rodrigo Nieto-Gomez
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

For intelligence officials today, understanding the appropriate bounds of balancing security and liberty interests is more imperative than ever. Intelligence enterprises require the consent of their public stakeholders to be effective; running aground of public support threatens significant institutional harms. Leaders can avoid many of these harms if they develop a culture within their organizations that better balances security and liberty interests. This effort can ward off the dangers of a narrative discourse that advocates for “prevention at all costs,” which leads to harmful extremes of disregarding public concerns over privacy, civil liberties, and the rule of law. This thesis uses a case study to review the social dynamics in the Bush Administration following 9/11, as a handful of policymakers secretly and unilaterally created and implemented aggressive surveillance programs. Using the social identity perspective, this thesis demonstrates the harms that may befall an organization intent on thwarting all other considerations to prevent a terrorist attack. Ultimately, this thesis provides a model for creating a culture that better balances security and liberty interests, and that ensures a better understanding of how stakeholders view an intelligence enterprise’s authorities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

TABLE 1: TIMELINE OF MAJOR EVENTS IN THE CASE STUDY..... IX

TABLE 2: RECURRING INDIVIDUALS IN THE CASE STUDY XI

I. INTRODUCTION.....1

- A. PROBLEM STATEMENT1**
- B. RESEARCH QUESTION3**
- C. LITERATURE REVIEW3**
 - 1. The Supremacy of Security Interests4**
 - 2. Liberty Interests Correlate to Public Trust.....11**
- D. RESEARCH DESIGN14**

II. HOW PAST CURRENTS SHAPED TODAY’S PATH: OVERVIEW OF INTELLIGENCE NORMS AND THE CREATION OF STELLARWIND17

- A. INFLUENCING THE NARRATIVE17**
- B. OVERVIEW OF INTELLIGENCE NORMS AND LEGAL STANDARDS PRIOR TO 9/1123**
- C. STELLARWIND AND NSA SURVEILLANCE31**
- D. FIRST SIGNS OF CONFLICT37**

III. UNDERSTANDING THE TROUBLED WATERS OF SOCIAL CONFLICT47

- A. INTRODUCTION TO THE SOCIAL IDENTITY PERSPECTIVE.....47**
- B. SOCIAL GROUPS AND THE PREVENTION NARRATIVE.....54**
- C. THE WAR COUNCIL AND CONFLICT WITH OTHER SOCIAL GROUPS.....65**
- D. FACING OUTWARD TOWARD EXTERNAL STAKEHOLDERS74**
- E. DAMAGE DONE AND TAKEAWAYS78**

IV. NAVIGATING TROUBLED WATERS THROUGH EFFECTIVE LEADERSHIP95

- A. THE ROLE OF LEADERSHIP IN INFLUENCING THE INGROUP CULTURE100**

V.	STEERING A TEAM OF TEAMS: RECRUITING PROTOTYPICAL LEADERS TO BALANCE SECURITY AND LIBERTY	115
A.	REACHING OUT TO STAKEHOLDERS	124
VI.	CONCLUSION	129
	APPENDIX. TABLE SOURCES	135
	LIST OF REFERENCES	137
	INITIAL DISTRIBUTION LIST	147

TABLE 1: TIMELINE OF MAJOR EVENTS IN THE CASE STUDY*

- September 11, 2001: Terrorists hijack four commercial airliners, crashing them into the World Trade Center in New York City, the Pentagon in Washington, D.C.; the fourth airliner (United Flight 93) crashed in a field in Somerset County, Pennsylvania.
- October 4, 2001: President Bush signs an order authorizing the creation of the Stellarwind surveillance program.
- October 26, 2001: President Bush signs the PATRIOT Act into law.
- January 31, 2002: Representatives of the National Security Agency and the Department of Justice inform Judge Lamberth of the Foreign Intelligence Surveillance Court about the Stellarwind program.
- March 10, 2004: Alberto Gonzales and Andrew Card confront James Comey, Patrick Philbin, and Jack Goldsmith at the George Washington University Hospital in an effort to convince Attorney General John Ashcroft to reauthorize the Stellarwind program.
- March 11, 2004: President Bush reauthorizes Stellarwind without the approval of the Department of Justice.
- March 12, 2004: President Bush meets with James Comey and Robert Mueller, agreeing to make the Stellarwind program comport with Department of Justice requirements.
- July 14, 2004: The Foreign Intelligence Surveillance Court approves the first section of Stellarwind surveillance.
- December 16, 2005: The *New York Times* publishes a story discussing the classified Stellarwind program.
- December 17, 2005: In a weekly address, President Bush acknowledges the existence of the surveillance program leaked to the New York Times (a.k.a. Stellarwind).

*Sourcing for these dates can be found in the appendix.

- April 3, 2007: Foreign Intelligence Surveillance Court Judge Robert Vinson rejects the Department of Justice's attempt to bring a final portion of the Stellarwind program under the court's authorities.
- August 5, 2007: President Bush signs the Protect America Act of 2007 into law.
- July 10, 2008: President Bush signs the FISA Amendments Act of 2008 into law.

TABLE 2: RECURRING INDIVIDUALS IN THE CASE STUDY*

- George W. Bush, President of the United States
- Richard Cheney, Vice President of the United States
- John Ashcroft, Attorney General
- General Michael V. Hayden, Director, National Security Agency
- Alberto Gonzales, White House Counsel (during the time of the case study, he later became Attorney General)
- David Addington, Counsel to the Vice President
- Andrew Card, White House Chief of Staff
- Robert Deitz, General Counsel, National Security Agency
- James Comey, Deputy Attorney General, Department of Justice
- Robert Mueller, Director, Federal Bureau of Investigation
- Jack Goldsmith, Assistant Attorney General, Office of Legal Counsel, Department of Justice
- John Yoo, Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice
- Patrick Philbin, Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice (during the time of the case study, he later became an Associate Deputy Attorney General)
- James Baker, Counsel for Intelligence Policy, Office of Intelligence Policy and Review, Department of Justice
- Royce Lamberth, Chief Judge, Foreign Intelligence Surveillance Court
- Colleen Kollar-Kotelly, Chief Judge, Foreign Intelligence Surveillance Court (following Chief Judge Lamberth)
- Robert Vinson, Judge, Foreign Intelligence Surveillance Court

*Sourcing for these references can be found in the appendix.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABA	American Bar Association
ACLU	American Civil Liberties Union
CIA	Central Intelligence Agency
DNI	Director of National Intelligence
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISA Amendments Act	Foreign Intelligence Surveillance Act Amendments Act
FISC	Foreign Intelligence Surveillance Court
IC	Intelligence Community
INS	Immigration and Naturalization Services
IRI	Intergroup Relational Identity theory
NSA	National Security Agency
NYPD	New York City Police Department
ODNI	Office of the Director of National Intelligence
OLC	Office of Legal Counsel
USA PATRIOT ACT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Intelligence stakeholders increasingly expect intelligence officials to be more transparent in the twenty-first century.¹ Stakeholder support is important because intelligence organizations operate most effectively when they have the support of their respective stakeholders, including legislative bodies who give intelligence organizations their authorities, the courts who often review intelligence activities, the media who frame public narratives about intelligence activities, and most importantly the public from whom all authority for intelligence activities derive in a democratic society. This thesis asks the question of how intelligence enterprises can effectively meet stakeholder demands in a manner that sufficiently balances security and liberty interests, thereby maintaining the support of stakeholders and the public writ large.

This thesis uses the social identity perspective as a tool for analysis in the case study methodology. This social psychological framework makes clear how harmful conflicts between groups within organizations and among intelligence stakeholders are to organizational efficacy. The case study in this thesis focuses on the small group of policymakers who controlled U.S. counterterrorism policy in the period immediately after 9/11. By highlighting their unilateral, secretive, and hostile tactics to implement aggressive, norm-changing intelligence programs, the case study denotes the dangers incumbent upon social groups within a security-based organization who embrace the “prevention at all costs” narrative. In the twenty-first century, intelligence officials must be cognizant of the pitfalls awaiting organizations that attempt to unilaterally and aggressively enhance their capabilities in an all-out effort to prevent another terrorist attack. The case study highlights several of those potential consequences, to primarily include the loss of capabilities and authorities, and the threat of institutional instability. Here, the Bush Administration unnecessarily created several potential threats to the efficacy of their own policies through the decisions they made.

¹ See Julian Richards, “Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy,” *Intelligence and National Security* 27, no. 5 (October 2012): 761.

By focusing on the social identity perspective to analyze the case study, this thesis makes clear that effective leadership is a critical component to strong organizations.² Leadership does not equal raw, coercive positional power.³ Instead, leadership of a group comes from the group's acceptance and support.⁴ According to the social identity perspective, a prototypical leader is an individual who most strongly identifies with a group's perceived vision of the ideal group member, and who can then take that correlation and use the group's acceptance to influence group norms.⁵ Those in positions of power in organizations must recognize the distinction between power and leadership, and strive to use leadership qualities to positively influence their organization and their surrounding stakeholders.

Looking forward, this thesis provides a foundation upon which future researchers and policymakers may build. Through the Intergroup Relational Identity (IRI) theory, this thesis provides one potential method for improving the ability of intelligence enterprises to balance the equities between security and liberty. The IRI theory is thoroughly steeped in the social identity perspective discussed in this thesis, but it is distinct in the field of social identity in that it focuses on the necessity of intergroup relations as a defining characteristic of groups' identities.⁶ This method recognizes the need to grasp social dynamics when seeking to institute cultural change and uses those forces to the leader's advantage. Specifically, this application of the IRI theory compels an organizational chief to use certain communication techniques while recruiting and fostering a leadership coalition.⁷ Those leaders set the stage for social influence among themselves and among

² See Michael A. Hogg, "A Social Identity Theory of Leadership," *Personality and Social Psychology Review* 1, no. 3 (August 2001): 193.

³ Hogg, 194.

⁴ See Deborah J. Terry, Michael A. Hogg, and Julie M. Duck, "Group Membership, Social Identity, and Attitudes," in *Social Identity and Social Cognition*, ed. Dominic Abrams and Michael A. Hogg (Oxford: Blackwell, 1999), 301.

⁵ Hogg, "A Social Identity Theory of Leadership," 194.

⁶ Michael A. Hogg, Daan Van Knippenberg, and David E. Rast, III, "Intergroup Leadership in Organizations: Leading Across Group and Organizational Boundaries," *Academy of Management Review* 37, no. 2 (April 2012): 241–42.

⁷ See Hogg, Van Knippenberg, and Rast, 243–45.

their respective ingroups.⁸ Through their dialogue, the leadership coalition can mirror stakeholder concerns over intelligence and better prepare the organization for those stakeholder interests. A similar use of the IRI model can also improve relationships with external stakeholders.

By working with external stakeholders and fostering an internal organizational culture that seeks to reasonably balance security and liberty interests, officials lessen the likelihood that stakeholders will one day question and scrutinize their actions for potential abuses of authority or violations of stakeholder expectations. Officials can also use these concepts to prevent many of the dire scenes of social conflict outlined in the case study.⁹

⁸ See Hogg, Van Knippenberg, and Rast, 244; see also Hogg, “A Social Identity Theory of Leadership,” 187.

⁹ For examples, see James Comey, *A Higher Loyalty: Truth, Lies, and Leadership* (New York: Flatiron Books, 2018), 87–90; see also Timothy Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (Washington, DC: Brookings Institution Press, 2017), 46.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Just like anything wherein one hopes to be successful, this document is the fruit a team effort. This team provided significant insights, support, and guidance to me over the course of the past eighteen months as I have navigated the thesis process and my overall studies at the Center for Homeland Defense and Security. Without these people, I could not be successful in anything I have done during this time; this is particularly true with this thesis project.

First, I would like to thank the incredible support apparatus at CHDS and the Naval Postgraduate School. To David Brannan and Rodrigo Nieto-Gomez, thank you for serving as my advisors. You were instrumental in guiding me toward the completion of this project. Perhaps more importantly, your qualities as educators provided me with fundamental underpinnings that contributed to the substance of this document. Additionally, I would like to express thanks to Christopher Bellavita and Carolyn Halladay for helping me find the direction of this project as it evolved in the early days of my time at CHDS. To Greta Marlatt and Noel Yucuis, thank you for your assistance in research and formatting, particularly as Chicago Turabian is a foreign citation style to me. Finally, I would like to thank Alison Scharmota from the Graduate Writing Center for offering an independent review, for helping me to organize this paper, and for helping me find a more coherent way to express my positions.

Next, I must thank my colleagues at the Florida Department of Law Enforcement for their support and patience as I traveled across the country to undertake this program. I could not be successful were it not for superiors and colleagues who so willingly allowed me this opportunity to improve myself. I hope that my time at CHDS will have positive benefits for the organization.

I must also thank my colleagues in CHDS Cohort 1701/1702. I did not know what to expect of my colleagues entering this program, but I continually find myself in awe of the quality of people who surround me here. The diversity of areas of expertise, backgrounds, and skills makes this program a truly unique learning environment. I am a

better professional for having spent time with you all. If each cohort is as impressive as 1701/1702, this nation's homeland security is in excellent hands.

Finally, and most importantly, I must thank my wife, Brittany, though words could never sufficiently express my appreciation. I would not be where I am today without her. From our first conversation about this program, her support has been unwavering. She pushes me when I am frustrated, and yet she keeps me grounded. She always offers an ear to bend and provides sage guidance. For this project, she brought her immense skills to the task, painstakingly reviewing several iterations of this thesis to provide suggestions and guidance, even while balancing her own demanding schedule. Brittany, thank you for your support and love, for being my rock, and for always being there. I love you.

I. INTRODUCTION

A. PROBLEM STATEMENT

This thesis begins with the presumption that officials in charge of intelligence and law enforcement enterprises, or any other enterprise deeply related to counterterrorism and homeland security, have an unbridled passion for preventing acts of terror or violence against the people within their jurisdictions. Public servants who comprise the core of those working forces have the same desire. Nothing in this thesis should suggest any malicious intent on the part of intelligence officials, even in events of overreach.

There is a problem, however, in that intelligence and law enforcement officials' drive for security can come at the cost of awareness of the importance of legal and societal privacy considerations and strictures. Particularly in intelligence enterprises, the organizational culture places an understandable emphasis on preventing terrorist acts, and internal social psychological influences build up pressure to meet the organization's goals. This leads to social dynamics wherein leadership's one-sided emphasis and overzealousness on security trickles down throughout subordinates and the agency as a whole. Numerous examples demonstrate that domestic intelligence efforts can lead to overreach and infringements on civil rights and civil liberties—essentially harming the very populations these agencies swore to protect and serve. As James Comey, former director of the Federal Bureau of Investigation, once described from the position of the legal advisor:

It can be hard, instead, because the stakes couldn't be higher. Hard because we are likely to hear the words: "If we don't do this, people will die." You can all supply your own this: "If we don't collect this type of information," or "If we don't use this technique," or "If we don't extend this authority." It is extraordinarily difficult to be the attorney standing in front of the freight train that is the need for "this." Because we don't want people to die. In fact, we have chosen to devote our lives to institutions whose sworn duty it is to prevent that, whose sworn duty it is to protect our country, our fellow Americans.¹

¹ James B. Comey, "Intelligence Under the Law," 10 *Green Bag* 2D 439 (May 2005), 442.

General Michael Hayden, the former director of the Central Intelligence Agency and the National Security Agency, famously described his counterterrorism efforts after September 11, 2001, as “playing to the edge,” meaning that he would do everything in his authority to check Islamic extremist terrorists. He wanted to be aggressive, so much so that—in using a football analogy—he would stay inbounds of the playing field, but his cleats would have chalk on them.² The difficulty for people in General Hayden’s position is that “the edge” in the realm of privacy considerations can be ill-defined and difficult to navigate, to the point that one may not know where troubled waters threaten until one is in neck deep. Because of the focus on security, intelligence leaders often pay little attention to the murkier waters beyond the dangers of strict Fourth Amendment territory, thereby underestimating the institutional harms that may arise from societal concerns attached to other constitutional notions like freedom of speech, freedom of association, due process or equal protection. Inevitably, leaders who are focused so highly on security also underestimate societal concerns of what the people may be willing to have their intelligence leaders do in their name.

The social dynamics of intelligence cultures can provoke intelligence leaders to push the envelope past what is arguably appropriate from legal or societal privacy considerations. Within the bubble of the intelligence ingroup, a single-minded focus on preventing bad acts and the determination of the ingroup’s patrons leaves little awareness on how to handle nuanced issues of public consent. When individuals warn of issues or violations, their positions in an outgroup render their opinions moot, at least until situations reach untenable breaking points.

Just as it is the responsibility of intelligence officials to maintain safety and security for the citizens they protect, it is also the responsibility of every intelligence official to secure the privacy rights, civil rights and civil liberties of the citizenry.³ It can be difficult for intelligence leaders to keep an eye on protected liberties when they are zealously

² Michael V. Hayden, *Playing to the Edge: Intelligence in the Age of Terror* (New York: Penguin Books, 2016), xiv.

³ See Hayden, 65, 430.

focused on security, and that focus of leaders will likely trickle down throughout an intelligence enterprise. This research considers the challenge of how leaders of intelligence enterprises may best prepare their organizations for balancing liberty and security concerns through cultural change and more effective policy implementation. This project analyzes intelligence leadership and organizational efforts of the past to consider how implementing potentially overzealous security efforts have previously destroyed the delicate balance between liberty and security.

The difficulty for intelligence leaders intending to play to “the edge” is often in understanding that the edge does not merely include that which will get someone arrested or sued for violations of law. The edge also includes societal privacy expectations, violations for which intelligence enterprises may find swift and harsh backlash. By seeking a greater emphasis on better understanding the contours of “the edge,” this thesis hopes to provide guidance on how to mitigate risks associated with violations of legal and privacy concerns. Producing better, more targeted intelligence, while also keeping intelligence enterprises out of legal or public relations trouble, requires an increased appreciation for legal and privacy considerations within intelligence enterprises. Incorporating legal and privacy concerns into the intelligence enterprise’s organizational culture creates significant benefits beyond simply protecting citizens’ rights including improving the efficacy of intelligence efforts.

B. RESEARCH QUESTION

How should intelligence leaders respond to increasing demands on transparency and privacy when attempting to effectively implement novel intelligence efforts?

C. LITERATURE REVIEW

Scholars and practitioners view liberty and security as two ends on a spectrum.⁴ Security is a simple enough concept to understand—in this realm it refers to the prevention of bad acts, typically in regard to terrorism. Trying to grapple with a singular definition of

⁴ From this point forward, this thesis uses “liberty” to mean a series of interchangeable concepts, including “privacy,” and “rule of law.”

privacy, however, would be akin to standing in front of a shouting crowd and parsing out a singular, coherent sentiment. Understanding privacy is important because it is from this notion that both laws and societal considerations derive. This section provides an analysis of the debate between security and liberty, the primary arguments surrounding that discussion, and the general need for balance recognized by most parties in a liberal democracy. The discussion reveals the difficulties intelligence enterprises face when attempting to balance aggressively acting to keep the citizenry safe with maintaining the public's trust and support. The framers of the Constitution were concerned with creating and executing a government that could effectively balance both liberty and security.⁵ The following outline of the debate's modern-day arguments will show that balance is still of great concern to many scholars.

1. The Supremacy of Security Interests

The importance of maintaining the liberties established at the founding of the United States is a critical goal for many advocates. Professor Solove notes that protecting liberty is critical during crises because that is when liberty is most likely to fall under siege, rather than during peacetime when leaders are separated from the fog of war.⁶ Indeed, the discussion in Chapters II and III of this thesis on the post-9/11 National Security Agency (NSA) surveillance programs speaks directly to the loss of emphasis on privacy in a time of war. Authors in favor of protecting liberty often note similar concerns about security overtaking liberty during crises.⁷ Dragu considers it widely accepted that security enhancements automatically erode liberties.⁸ It is difficult to conjure more enhanced security efforts in the modern age that do not at least threaten the status quo of individual privacy expectations, at least without certain restrictions and safeguards in place. Pro-

⁵ James J. Lopach and Jean A. Luckowski, "National Security and Civil Liberty, Striking the Balance," *Social Studies* 97, no. 6 (November/December 2006): 246.

⁶ Daniel J. Solove, "Data Mining and the Security-Liberty Debate," *University of Chicago Law Review* vol. 75, no. 1 (Winter 2008): 350.

⁷ Tiberiu Dragu, "Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention," *American Political Science Review* 105, no. 1 (February 2011): 64–65.

⁸ Dragu, 64.

liberty arguments sometimes insist that terrorists “win” when security wins out over liberty because that destroys our way of life.⁹ For instance, Donovan argues that any legislation that would reduce privacy inherently risks the underpinnings of a liberal democracy.¹⁰ Similarly, Dragu and many other scholars note the threat of a “chilling effect” that can result from increased surveillance, which refers to the probability that people will be less likely to make overt expressions or demonstrate certain associations based on concerns that the government may be watching or may take some negative action in response.¹¹ Dragu also notes that there is no empirical evidence to date that diminished privacy substantially improves security.¹² The difficulty of the federal government to cite instances wherein new surveillance programs prevented specific terrorist efforts is telling in this regard.

When discussing the importance of liberty, some advocates point to more than purely academic concerns. To make the determination that society generally recognizes privacy freedoms, Nelson referenced a 2003 Harris poll that asked the surveyed population about privacy concerns. In that poll, roughly one third of those surveyed deemed themselves privacy fundamentalists, which were people who said privacy rights were critical to them.¹³ Only approximately ten percent were wholly unconcerned with privacy rights. Most people, though, considered themselves privacy pragmatists who weighed privacy concerns with conveniences and/or security needs.¹⁴ All told, roughly ninety percent of those polled considered privacy considerations important. “Non-trivial” percentages of the American public are concerned with domestic surveillance.¹⁵ As such, these numbers play directly into the concerns of chilling effects presented above; moreover, these polling numbers suggest concerns in the general population that, while maybe not

⁹ James J. Lopach and Jean A. Luckowski, “Striking the Balance,” 245.

¹⁰ Tiberiu Dragu, “Is There a Trade-off between Security and Liberty?” 72.

¹¹ Dragu, 66.

¹² Dragu, 65.

¹³ Lisa Nelson, “Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era,” *Public Administration Review* 64, no. 3 (May/June 2004): 267.

¹⁴ Nelson, 267.

¹⁵ Nelson, 267.

today, by putting in place robust domestic surveillance efforts, they too could one day be the subject of domestic surveillance. In other words, people are likely to be nervous about both terrorism and counterterrorism surveillance programs.¹⁶ This becomes especially true when government activities appear to potentially target civilians; Huddy et al. find that many seem to distinguish surveillance activities that target “guilty criminals” versus the public writ large.¹⁷

Polling shows that people consistently fear surveillance when they believe they will be the targets.¹⁸ Citizens do not like losing either security or liberty.¹⁹ Government monitoring makes the public anxious, but they are more likely to allow such policies when they are afraid of terrorism.²⁰ Significant anxiousness in the public, however, is likely to lead to risk aversion in the allowance of aggressive policies.²¹ Thus, the need for the people to trust the government is critical in achieving maximum efficacy. Gould notes that the public makes balancing calculations in debating relevant issues of security and liberty.²² He also expresses concern that many of the post-9/11 security enhancements have served to separate the public from government, raising concerns about trust and cooperation moving forward.²³ This rise in distrust can significantly harm security efforts moving forward, perhaps leading to the removal of tools or less flexibility in emergencies to come, thereby diminishing efficacy.

Yet privacy and liberty are rarely absolute. There are frequently tradeoffs with privacy, and not just between privacy or liberty and security. Pozen also finds that there

¹⁶ Samuel J. Best, Brian S. Kreuger, and Shanna Pearson-Merkowitz, “Al Qaeda Versus Big Brother: Anxiety About Government Monitoring and Support for Domestic Counterterrorism Policies,” *Political Behavior* 34, no. 4 (December 2012): 612.

¹⁷ Leonie Huddy et al., “Threat, Anxiety, and Support of Antiterrorism Policies,” *American Journal of Political Science* 49, no. 3 (July 2005): 595.

¹⁸ Jon B. Gould, “Playing with Fire: The Civil Liberties Implications of September 11th,” *Public Administration Review* 62, no. s1 (September 2002): 75.

¹⁹ Best, Kreuger, and Pearson-Merkowitz, “Al Qaeda Versus Big Brother,” 608.

²⁰ Best, Kreuger, and Pearson-Merkowitz, 612.

²¹ Best, Kreuger, and Pearson-Merkowitz, 612.

²² Gould, “Playing with Fire,” 75.

²³ Gould, 77.

are “distributional tradeoffs,” wherein privacy increases for one group may mean less privacy for others.²⁴ An example of a distributional tradeoff might mean increased airport security measures, with enhanced invasions of privacy, which might lead to lowered privacy intrusions elsewhere.²⁵ Pozen notes that New York’s now-defunct Muslim surveillance program could also be an example of distributional tradeoffs—the scrutiny on one group significantly increases while it slightly decreases for others.²⁶ Pozen also notes the phenomena of “directional tradeoffs,” wherein greater privacy in some manner may mean greater intrusions elsewhere.²⁷ A prime example, as Benjamin Wittes once noted, would be an Amazon Kindle book: reading on one’s Kindle hides the name and content of the reading material from the surrounding people on the subway, so that people cannot tell whether someone chose to read *Fifty Shades of Gray* or some other buzzworthy book title. However, by reading on a Kindle, Amazon collects significant amounts of information about readers that would be unavailable to the company were they to read a paperback.²⁸

Counteracting privacy and liberty advocates, the pro-security framework often begins with the Hobbesian analysis that liberty cannot exist without security, thus security is an essential building block to ensuring liberty.²⁹ The pro-security contingent focuses on the need to protect the population.³⁰ Many security proponents advocate that liberty concerns should take a back seat to security in times of emergency. Former Supreme Court Chief Justice William Rehnquist noted that the pendulum balancing security and liberty swings towards security in times of great emergency, and swings back to equilibrium once

²⁴ David E. Pozen, “Privacy-Privacy Tradeoffs,” *University of Chicago Law Review* 83, no. 1 (Winter 2016): 229.

²⁵ Pozen, 229.

²⁶ Pozen, 229.

²⁷ Pozen, 229.

²⁸ Benjamin Wittes and Jodie C. Liu, “The Privacy Paradox: The Privacy Benefits of Privacy Threats,” Center for Technology Innovation at Brookings, Brookings Institution, May 21, 2015, https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf.

²⁹ See Thomas Hobbes, *Leviathan* (Baltimore, MD: Penguin Books, 1968).

³⁰ Jeffrey L. Vagle, “Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance,” *Indiana Law Journal* 90, no. 1 (Winter 2015): 105–6.

emergencies subside.³¹ Some scholars view World War II and the curtailment of liberties as a relevant example, though others, like Professor Solove, note that many of those curtailments, such as the internment of citizens of Japanese descent, have ultimately proven to be unnecessary.³² This also ignores the detriment to civil liberties at the time, such as the internment of U.S. citizens for reasons many ultimately deemed illegitimate and false. Some counteract the deference argument by asserting that laws should never be silent in emergencies.³³ Security proponents again respond by noting that security and liberty are not mutually exclusive, but it is difficult to maintain liberty when society cannot ensure security.³⁴ These arguments ignore the ultimate core of liberal democracies, wherein freedoms determine who the people choose to be as a society. To eliminate freedoms for need of security creates a slippery slope, dangerously so when the threat is undefined with no expectation of subsiding for potentially decades.

A common argument made by many security advocates is that losing privacy should not be of any great concern to someone who has “nothing to hide.” Posner argues that the societal conception of privacy today is most closely associated with secrecy, and he ties the greatest threats to such secrecy to improper disclosure of information.³⁵ This ignores the legitimate concerns of individuals to block from public view protected relationships and associations, particularly in heavily scrutinized times. In regard to the security vs. liberty debate, he notes the extreme natures of both sides of proponents; while complete transparency or opacity are impractical in practice, civil libertarians want government to be open and individuals hard to find, meanwhile pro-security forces want the reverse.³⁶ It is obvious that Posner ultimately falls in favor of security considerations, noting that privacy allows terrorists to hide in society, and that the warrant is an ill-fit tool

³¹ William H. Rehnquist, *All the Laws but One: Civil Liberties in Wartime* (New York: Knopf, 1998), 225.

³² Daniel J. Solove, “Data Mining and the Security-Liberty Debate,” 350.

³³ Lopach and Luckowski, “Striking the Balance,” 246.

³⁴ Lopach and Luckowski, 246.

³⁵ Richard A. Posner, “Privacy, Surveillance, and Law,” *University of Chicago Law Review* 75, no. 1 (Winter 2008): 245.

³⁶ Posner, 246.

for counterterrorism efforts today.³⁷ Like Posner, Richards notes that the dangers in surveillance come from potential threats of blackmail, selective enforcement, discrimination, or coercion, or some other non-security related tangent by maladjusted actors working on behalf of security.³⁸

Professor Solove finds that the “I’ve got nothing to hide” argument is rather weak when taken to the extremes, such as suggesting that putting a video camera in someone’s bedroom is then appropriate.³⁹ Yet, the argument is more persuasive when considered as a tradeoff on privacy protections: if there is little justification to protect certain types of privacy, there is less harm of erosion of privacy in favor of security.⁴⁰ This is in line with Judge Posner’s interpretation of privacy as being a defense for someone who has something to hide. Particularly in light of significant security concerns, as in the counterterrorism realm, if the population has few concerns about protecting privacy, those security concerns will likely win out. Going back to civilian anxiousness, as described by Best et al., government actors who choose a discursive framing in line with Posner’s assertions are likely to exacerbate the distance between government actors and those they are sworn to protect. Engaging in a balanced discussion on the spectrum of privacy rights and security concerns will likely further the cause of security more substantially by promoting public consent.

Pro-security advocates also believe that the professionalism of intelligence officials mitigates many of the concerns expressed by privacy and liberty advocates. Posner finds that privacy interests are less at threat when security agencies that collect information control it as tightly as possible, and when those agencies hire individuals who act and use such information in a professional manner.⁴¹ Posner likens the threat to personal

³⁷ Posner, 255.

³⁸ Neil M. Richards, “The Dangers of Surveillance,” *Harvard Law Review* 126, no. 7 (May 2013): 1935.

³⁹ Daniel J. Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” *San Diego Law Review* 44 (2007): 751.

⁴⁰ Solove, 751–52.

⁴¹ Richard A Posner, “Privacy, Surveillance, and Law,” 251.

information by intelligence officials to the privacy threat inherent when doctors view the human body; people tend not to be overly concerned about doctors viewing them because they believe it is for purely professional reasons.⁴² Having the same considerations for intelligence professionals should similarly reduce privacy concerns. Likewise, John Yoo asserts that computers, which lack personal biases, cannot “search” information pursuant to the Fourth Amendment because a search can only occur when government employees view information.⁴³ These arguments are challenging on a number of grounds. Regarding Professor Yoo’s assertion, the counterbalancing argument is that a search occurs upon collection of information for Fourth Amendment purposes; in the physical world, a search or seizure occurs at the time of government collection, not at some later point in time when a computer algorithm may cross the information. To challenge Posner’s point, a doctor’s prognosis tends to rarely have a nexus to the patient’s political, religious, ideological, or potential criminal activities.

Counterterrorism agencies will always want less privacy in society, according to Dragu.⁴⁴ Reduced privacy eliminates barriers between agencies and sources of information for collection, and also eliminates places that bad actors can hide. Such agencies will always lack incentives to give up enhanced authorities, temporary or otherwise.⁴⁵ This argument makes sense from a certain point of view. If a counterterrorism agency’s primary goal is to keep people safe from bad actors, the more information that agency can obtain, the more possible it may be that the agency can prevent bad acts. It is tempting to think that any additional information may assist in security efforts, so collecting any possible additional information should be done to further that security focus. Substituting an intelligence enterprise for the narrower “counterterrorism agency” would not alter the calculus here. If one’s primary focus is security, then having every possible resource at one’s disposal is a natural inclination. To that end, this project will hopefully elicit is a

⁴² Posner, 251.

⁴³ John Yoo, *War by Other Means: An Insider’s Account of the War on Terror* (New York: Atlantic Monthly Press, 2006), 110.

⁴⁴ Tiberiu Dragu, “Is There a Trade-off between Security and Liberty,” 64–65.

⁴⁵ Dragu, 64–65.

conversation within intelligence enterprises that asks the question “should every resource be obtained, and where are the reasonable boundaries that society places upon us?” Supporting Dragu’s argument is not to suggest that security officials are ambivalent to privacy rights. To the contrary, many, including General Hayden, have expressly invoked those concerns publicly.⁴⁶ Yet, in an environment solely focused on security, the increasing ingroup narrative will likely lead to one-sided debates on this subject, as this thesis will outline in depth.

2. Liberty Interests Correlate to Public Trust

Balancing the considerations between security and liberty is difficult for government actors, particularly in intelligence, because of the needs for secrecy in intelligence collection. Democratic societies expect government actors to stop bad actors while avoiding any undermining norms and laws.⁴⁷ The suspicion of eroding privacy rights for security runs deep in the United States, and intelligence overreaches have frequently led to new constraints.⁴⁸ Now, Richards argues that intelligence enterprises find themselves with a new “intelligence dilemma,” wherein the post-Cold War American society increasingly expects them to act with openness, which contravenes the need for secrecy.⁴⁹ There is today, he argues, an increased focus on asking how intelligence enterprises should act in a liberal democracy, and the appropriate lines of limitation are not clear.⁵⁰ The public’s expectations of openness and transparency have increased immensely.⁵¹ He maintains that ethics are at the center of the intelligence dilemma, sparking the question of how intelligence enterprises can maintain an ethical role while

⁴⁶ Hayden, *Playing to the Edge*, 421–26.

⁴⁷ Jennifer Sims, “Intelligence to Counter Terror: The Importance of All-Source Fusion,” *Intelligence and National Security* 22, no. 1 (February 2007): 39.

⁴⁸ Sims, 46, 48.

⁴⁹ Julian Richards, “Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy,” *Intelligence and National Security* 27, no. 5 (October 2012): 761.

⁵⁰ Richards, 761.

⁵¹ Richards, 762.

still enhancing capabilities in the Information Age.⁵² Richards also notes the “proactive response dilemma” that intelligence enterprises face today, wherein too weak a response to perceived threats may cause diminished confidence in and support for intelligence organizations, while too active a role risks undermining democratic values in the eyes of the citizenry and risks alarming the population.⁵³ This proactive response dilemma is one of the primary factors of the “never again” mantra driving so many one-sided discussions within intelligence enterprises, as Chapters II and III discuss in greater depth. A recognition of this issue will be one of the issues this thesis hopes to tackle, leading to a discussion on better balancing of the relevant interests.

Among the arguments discussed thus far is how to find a balance between security and liberty. Sunstein views the debate between security and liberty as a battle between “Cheneyism” and “Snowdenism,” using popular public figures to characterize the extreme arguments of the debate.⁵⁴ According to Cheneyism, the state’s primary responsibility is to protect its citizens; today, that requires mass surveillance.⁵⁵ The standard for judging whether or not that is effective is the amount of lives saved.⁵⁶ If there is even the slightest chance that a major attack could take place, the government should treat the threat like a certainty.⁵⁷ It is natural for the government and security officials to want every possible tool to ensure the safety of the people.⁵⁸ Conversely, Snowdenism argues that government actors in national security are a greater threat than ever before, with personal privacy and First Amendment considerations at their greatest risk in recent memory.⁵⁹ Government actors that may be incompetent or may have malicious intentions can jeopardize privacy,

⁵² Richards, 762.

⁵³ Richards, 765.

⁵⁴ Cass R. Sunstein, “Beyond Cheneyism and Snowdenism,” *University of Chicago Law Review* 83, no. 1 (Winter 2016): 272–73.

⁵⁵ Sunstein, 271–72.

⁵⁶ Sunstein, 272.

⁵⁷ Sunstein, 280.

⁵⁸ Sunstein, 281.

⁵⁹ Sunstein, 272.

and so simply trusting the government to do the right thing is insufficient; there must be reforms and regulations in place to protect the people.⁶⁰ Edward Snowden revealed many major abuses of privacy, and government actors could engage in even greater privacy violations in the future should there be no changes.⁶¹ Sunstein ultimately argues for a middle ground that finds a balance through cost/benefit analyses. He contends that government actors should enact a “privacy precautionary principle”— “best understood as involving a form of risk management”—when engaged in the context of security concerns.⁶² However, a concern in Sunstein’s approach is that in characterizing the opposing sides in such effectively descriptive terms, those characterizations also serve to radicalize the opposing sides of the debate into further extremes. The discursive narrative in such characterizations, while again serving well to explain current stances, tends to ignore the moderating forces in either camp. Most in the Snowdenism camp recognize the need to establish effective security, and most in the Cheneyism realm likely recognize the need to prevent a liberal democracy from descending into a fascist state.

To that end, Dragu also notes that security and liberty do not necessarily conflict.⁶³ He finds that most people attack the debate from a balancing perspective, noting that it is “almost unthinkable” to consider going all in for security or liberty exclusively, which would render a liberal democracy either fascistic or completely vulnerable.⁶⁴ Courts also engage in balancing considerations of security and liberty. The Fourth Amendment bars only unreasonable searches. Courts will regularly “weigh both core values,” though the media, intellectuals and officials tend to talk of the debate in a zero-sum fashion.⁶⁵

Solove focuses on balancing security and liberty but notes the problem of most security/liberty debates today. He highlights that most debates begin from a position of

⁶⁰ Sunstein, 282.

⁶¹ Sunstein, 283.

⁶² Sunstein, 282–83.

⁶³ Tiberiu Dragu, “Is There a Trade-off between Security and Liberty?” 64.

⁶⁴ Dragu, 64.

⁶⁵ Amitai Etzioni, “NSA: National Security vs. Individual Rights,” *Intelligence and National Security* 30, no. 1 (2015): 102.

focusing on the importance of the security needs, thus leaving the liberty concept in a defensive crouch.⁶⁶ For instance, he notes how Stuntz once called privacy and transparency “diseases,” believing that there needed to be an immediate cure for them.⁶⁷ Stuntz argued that, in a post-9/11 world, those notions are “perverse,” and those ideas that are untenable today.⁶⁸

Finally, Sutherland argues that leaders have an obligation to promote innovation on issues related to the balance between security and liberty.⁶⁹ To him, it is too easy to argue the extremes of the debate—that terrorists win if we erode liberties in favor of security, or to say that there is little room for liberties without security—but the true challenge comes in incorporating both sides of the debate into a single framework.⁷⁰ Security enhancements can be narrowly tailored in ways to prevent erosions of liberty, and yet truly compromising civil liberties would mean compromising our principles and way of life.⁷¹

D. RESEARCH DESIGN

This thesis studies the deleterious effects of the “prevention at all costs,” pro-security drive observed so often in public officials and the potential unintended consequences that derive from that single-sided viewpoint. More specifically, this thesis studies the leadership and decision-makers in perhaps the most publicized post-9/11 scenario, when the desire to prevent bad acts such as terrorism overrode legal and privacy concerns. The case study methodology guides this research. The thesis analyzes the social dynamics surrounding the Stellarwind program (also known as the Terrorist Surveillance Program or the President’s Surveillance Program) and the related operations that the NSA and other federal entities created after 9/11 in an effort to prevent another attack on the

⁶⁶ Daniel J. Solove, “Conceptualizing Privacy,” 1107.

⁶⁷ Solove, 1107.

⁶⁸ William J. Stuntz, “Secret Service: Against Privacy and Transparency,” *New Republic*, April 17, 2006, 12.

⁶⁹ Daniel W. Sutherland, “Homeland Security and Civil Liberties: Preserving America’s Way of Life,” *Notre Dame Journal of Law, Ethics and Public Policy* 19, no. 1 (February 2014): 292.

⁷⁰ Sutherland, 292.

⁷¹ Sutherland, 303.

homeland. The focus of this case study is not on the individual organizations involved, but rather on the leadership cluster in the White House and the associated leaders of respective agencies who drove policy after 9/11. Focusing on social dynamics and conflict through the lens of the social identity perspective, this case study highlights the ingroup/outgroup dynamics that pushed an enterprise in a single-minded direction of preventing another 9/11. Case study methodology provides the best opportunity for effective analysis here given the subject matter of the thesis. This thesis recognizes that there are several perspectives that could analyze or rationalize many of these events. However, the thesis specifically uses the social identity perspective as the tool for analysis because of its value in understanding people through the importance of their respective social groups.

Several reasons support the use of this case study. This scenario is well-known publicly, with a wealth of data, reporting, and prior accounts from which to draw lessons from a social psychological analysis of the relevant players involved. Sources will include prior academic research, investigative journalism, and primary sources, such as legal documents, historical books, first-hand accounts, and agency reports. Through this post-9/11 case study, this project highlights how the social identity perspective explains the failures of intelligence leadership to understand the boundaries of appropriate security actions, and how those failures can lead to harmful and debilitating results. This methodology demonstrates that the Bush Administration could have avoided or mitigated many of the problems its post-9/11 programs created by taking certain actions to garner broader support from the respective executive agencies and external stakeholders.

The thesis concludes by turning to the importance of leadership and establishing a culture of balance within intelligence enterprises. This thesis provides lessons learned from the implementation of the president's surveillance programs to offer intelligence officials with considerations related to how social dynamics influence organizational culture that are important to policymakers who wish to enact organizational change. The literature, and the case example outlined herein, highlight the limitations of individual leadership over broad swaths of organizational personnel. This thesis recommends implementing the Intergroup Relational Identity Theory as a model for better implementing liberty concerns into the social culture of an intelligence enterprise in order to highlight the importance of

leadership through the social identity perspective.⁷² By analyzing the leaders involved in the case study, the following analysis provides intelligence leaders with guidance on how to more effectively balance security and liberty interests within their organizations through the lens of social identity perspective, thereby giving them the tools to succeed in their long term endeavors. Understanding that officials cannot immediately will certain principles into the cultural zeitgeist of their organizations, the thesis defines the steps necessary to effectively implement organizational change through a social identity analysis in order to ensure a better balancing of security and liberty interests.

⁷² See Michael A. Hogg, Daan Van Knippenberg, and David E. Rast, III, "Intergroup Leadership in Organizations: Leading Across Group and Organizational Boundaries," *Academy of Management Review* 37, no. 2 (April 2012): 232-55.

II. HOW PAST CURRENTS SHAPED TODAY'S PATH: OVERVIEW OF INTELLIGENCE NORMS AND THE CREATION OF STELLARWIND

As this project's analysis relies heavily on the social identity perspective and the harms created by certain discursive narratives and social conflicts, it is important to begin this chapter with an overview of several notable stories that set the backdrop for the ensuing analysis. The first story highlights the perils of social conflict for officials who apply exclusive strategies to initiate policy, noting one incident that almost led to the collapse of a secret government surveillance program. The second set of stories underscore the well-known events that led to aggressive policymaking tactics in this case.

A. INFLUENCING THE NARRATIVE

On a cool, late winter night in early March 2004, the executive branch's secret counterterrorism surveillance programs faced a dire threat of lapsing as two separate vehicles rushed to the George Washington University Hospital. James Comey, then the Deputy Attorney General for the U.S. Department of Justice, ordered his security detail to get to the George Washington University Hospital with lights and sirens on, hoping to beat another party to the hospital bed of a beleaguered John Ashcroft. The hospital admitted Ashcroft, the Attorney General, for an acute pancreatic illness days before. Comey, temporarily serving as the Acting Attorney General, told staffers for President George W. Bush that he could not reauthorize a continuation of several highly classified counterterrorism surveillance programs, collectively known as Stellarwind. Comey was not confident in the legality of some of the programs, to the point that he could not personally aver to their lawfulness, in part because he believed government actors were engaging in activities beyond what President Bush authorized.⁷³

After a contentious conversation with presidential staffers on the night of Wednesday, March 10, 2004, Comey learned that White House Chief of Staff Andrew Card

⁷³ James Comey, *A Higher Loyalty: Truth, Lies, and Leadership* (New York: Flatiron Books, 2018), 81, 83, 85–87.

and White House Counsel Alberto Gonzales sought to go around Comey's authority by seeking out the Attorney General himself at his hospital bedside.⁷⁴ The White House required the authorization to renew the surveillance programs immediately, otherwise the programs would lapse. March 11th was the last day for reauthorization before the initiatives lapsed, and every prior authorization included the Attorney General's signoff.⁷⁵

Comey learned of Card's and Gonzales' intentions as he left his office for the night.⁷⁶ Upon receiving information about what Card and Gonzalez planned, Comey immediately diverted his security detail to the hospital. During the race to the hospital, Comey contacted several people to meet him at Ashcroft's room, including the Director of the Federal Bureau of Investigation Robert Mueller, as well as Patrick Philbin, one of Comey's top associates in the Department of Justice, and the lead attorney for the Office of Legal Counsel in the Department of Justice, Jack Goldsmith.⁷⁷ When he arrived at the George Washington University Hospital, Comey bolted up the hospital's stairs to reach Ashcroft's room as quickly as possible. Comey had Mueller provide orders to the security detail that Comey was not to be removed from the hospital room, no matter what.⁷⁸ Within minutes, Comey, Philbin, Goldsmith, and Ashcroft's wife, Janet, stood at Ashcroft's side as Andrew Card and Alberto Gonzales entered the room, one of them holding an envelope for Ashcroft's review.

There are varying descriptions of what exactly occurred next, but the consensus in public versions describes an attempt by Card and Gonzales to get Ashcroft to reauthorize the program. Ashcroft, who was still quite ill at this point, looked like he might "expire" right there in his bed.⁷⁹ In response to the request by Card and Gonzales, Ashcroft lifted his head off the bed and provided a reportedly detailed and eloquent justification for why

⁷⁴ Comey, 87.

⁷⁵ Comey, 83.

⁷⁶ Comey, 87.

⁷⁷ Comey, 87–88.

⁷⁸ Comey, 88.

⁷⁹ Jack Goldsmith, "Interview Jack Goldsmith," PBS Frontline, August 22, 2007, <https://www.pbs.org/wgbh/pages/frontline/cheney/interviews/goldsmith.html>.

he could not legally reauthorize the surveillance programs. After his exposition, he concluded that his opinion in the moment was irrelevant anyways because Comey was the Acting Attorney General.⁸⁰ Card and Gonzales left the room quietly. Shortly thereafter, Comey received a phone call from Card, demanding he appear at the White House immediately.⁸¹ Tempers flared, and suspicions were high. Comey advised Card that he would not appear without a witness considering what had just transpired.⁸²

The next day, President Bush reauthorized the surveillance programs without the approval of the Department of Justice.⁸³ The president quickly found himself facing down a threat of resignations *en masse* from leadership in the Department of Justice, including Comey, Mueller, Goldsmith, Philbin, and other senior department leaders, including FBI General Counsel Valerie Caproni. Many were ready to resign that Friday, but Ashcroft's chief of staff, who also wished to resign, asked people to wait until the Attorney General was also well enough to resign.⁸⁴ The president asked to meet with Comey and Mueller separately. After speaking with Mueller and Comey, President Bush gave the edict for the Department of Justice to do what was necessary to make the program legally sufficient to the department's leadership.⁸⁵ In the following months, Comey, Goldsmith, and other department leaders sought to do just that.

It was drama fit for the silver screen; Jack Goldsmith described it as “the most amazing thing [he had] ever seen.”⁸⁶ Later in congressional hearings, one senator

⁸⁰ Goldsmith, “Interview.”

⁸¹ Comey, *A Higher Loyalty*, 90.

⁸² Comey, 90.

⁸³ Comey, 95.

⁸⁴ Comey, 92; Eric Lichtblau, *Bush's Law: The Remaking of American Justice* (New York: Pantheon Books, 2008), 183; Goldsmith, “Interview”; *Hearing on the U.S. Attorney Firings before the Senate Judiciary Committee*, Senate, 110th Cong., 1st sess., May 15, 2007, 19–21, http://gulcfac.typepad.com/georgetown_university_law/files/comey.transcript.pdf; Department of Justice, *A Review of the Department of Justice's Involvement with the President's Surveillance Program* (Washington, DC: Department of Justice, 2009) (DOJ IG Report), 153, <https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf>.

⁸⁵ Comey, *A Higher Loyalty*, 98; DOJ IG Report, 157.

⁸⁶ Goldsmith, “Interview.”

described the spoken testimony of the event as the “most dramatic” story he had heard in twenty-five years.⁸⁷ All of this took place just months before a presidential election, outside of the public’s knowledge until those involved later spoke publicly about the incident.⁸⁸

Two more scenes precede the race to the George Washington University Hospital in March 2004; these next two scenes also influence the narrative for everything to come. Both scenes surround the fateful events of September 11, 2001, an otherwise peaceful and beautiful day until the hijacking and crashing of four transcontinental airliners by Al Qaeda terrorists. The horrors of the stories of the victims of 9/11 necessarily shade all of the actions by executive intelligence leaders in the wake of the attacks, including the guilt of allowing these events to occur (justifiable or not), and the resolution to prevent them from ever happening again. These stories include the words of victims on the airliners prior to their fateful end, when people on the planes called loved ones, sometimes speaking directly to others or leaving voicemails for them to hear later. The accounts include the words of Amy Sweeney, a flight attendant aboard one of the flights. As she was aboard one of the planes headed for the Twin Towers, her words over the phone led to significant insights for the 9/11 Commission in unfolding what exactly happened that day.⁸⁹ Her own words described the mayhem inside the plane, how the terrorists killed people in the cabin when overtaking the plane, and how they commandeered the cockpit.⁹⁰ She even provided the seats of the hijackers, allowing investigators to determine their identities after the fact.⁹¹ Then, Sweeney’s own final words detailed the horror of the realization, in the moments before crashing into one of the towers, that the plane was flying startlingly low to New York City’s skyscrapers. “We are flying low. We are flying very, very low. We are flying

⁸⁷ Senate, *Hearing on the U.S. Attorney Firings*, 50.

⁸⁸ Many prior records and reporting discuss these events at length, perhaps most notably directly by Comey and Goldsmith (Comey, *A Higher Loyalty*; Goldsmith, “Interview;” Jack Goldsmith, *The Terror Presidency: Law and Judgment Inside the Bush Administration* (New York: W.W. Norton & Company, 2007); DOJ IG Report, 134–40).

⁸⁹ The National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: Norton, 2004), 5.

⁹⁰ *The 9/11 Commission Report*, 5–6.

⁹¹ *The 9/11 Commission Report*, 6.

way too low...[o]h my God we are way too low.”⁹² Her last words were believed to be, “I see water and buildings. Oh my God, oh my God!”⁹³

Records reviewed by investigators after the events include accounts of terror from those trapped inside the buildings. Detailed accounts of people faced with the options of suffocating and burning to death or alternatively leaping to their demise necessarily weighed on the minds of political and intelligence leaders in the coming days as they made critical determinations of what came next. That includes the final scene that overlays the narrative of this case study: a simple moment when, at a National Security Council meeting in the immediate aftermath of the attacks, President Bush gave an edict to Attorney General Ashcroft to never “let this happen again.”⁹⁴ More than any other, that intent drove everything that comes afterwards. That mantra drives the decision-making of executive branch policymakers going forward, and ultimately leads to many of the problems the Bush Administration unnecessarily created in the months and years to come.

The case study describes how the “prevention at all costs” narrative permeated the government and particularly the executive branch after September 11, 2001, and the effects that allowing the narrative to develop had on social groups within the executive branch. The primary focus of this project is to analyze the psychological ramifications that came from the actions of the decision makers who authorized the programs, particularly in regard to how the decisions on implementing and executing the program arose and how others received those decisions. This includes an analysis of the decisions made and actions taken during the Bush Administration through the lens of the social identity perspective. This thesis strongly intertwines Chapters II and III, as they provide the bulk of the analysis on the case study; Chapter II highlights the “prevention at all cost” narrative framing that drove the creation of social groups, secrecy, and conflicts within the executive branch, and begins to introduce the analysis of these events pursuant to the social identity perspective.

⁹² *The 9/11 Commission Report*, 6–7.

⁹³ Stevenson Swanson, “Phone Calls Played From 9/11 Planes,” *Chicago Tribune*, June 5, 2004, http://articles.chicagotribune.com/2004-06-05/news/0406050171_1_crew-members-american-airlines-flight-hijackers.

⁹⁴ John Ashcroft, *Never Again: Securing America and Restoring Justice* (New York: Center Street, 2006), 130.

Chapter III provides the bulk of social identity perspective analysis, primarily focusing on the social psychological harms that arose from the conflicts established in Chapter II. Chapter III ultimately summarizes key points found within the case study and highlights how the discursive framing of prevention skewed several relevant considerations necessary for the effective implementation of intelligence efforts.

Ultimately, the analysis highlights four points: first, that skewing the security vs. liberty debate entirely to the side of security and prevention influences decision-making in a manner that sets up an intelligence enterprise for failure and significant institutional harms. Emphasizing that narrative leads to increased and unnecessary secrecy and eliminates dialogue valuable to intelligence organizations on many levels. In this case, it mitigated vocal dissent and increased the likelihood of leakers and opponents willing to take extreme measures. Second, the Bush Administration and its key decision makers in the Stellarwind program failed to garner sufficient support from its stakeholders and overseers. From a social identity perspective, this failure is directly attributable to an established ingroup/outgroup conflict, with particular actors using the prevention at all costs narrative as a damaging enabler of negative social change. Third, the case study highlights that secrecy and tightening of ingroups do not kill dissenting opinions, but rather encourage dissenters to take more extreme responses by amplifying the urgency of the conflict. Outsiders who viewed themselves to be part of the nominal ingroup of government protectors engaged in social mobility insofar as they affirmatively separated themselves from the decision makers because of their choices. Finally, this case study demonstrates that the decision makers in this case so strongly wrapped their efforts in the “prevention at all costs” narrative and sought to enhance the ingroup value through efforts in social creativity that the decision makers blinded themselves to the dangers of their actions and the likely harms that followed. This included damaging morale within executive agencies, wasting resources, fostering an environment that bred damaging leaks, diminished authorities through legislative or judicial intervention, and weakened support and trust from the public.

B. OVERVIEW OF INTELLIGENCE NORMS AND LEGAL STANDARDS PRIOR TO 9/11

To fully appreciate the substance of this case study and the significance of the decisions by the people involved, this thesis uses a baseline review of the history, norms, and laws in place for surveillance and information collection prior to September 11, 2001. The decisions that the Bush Administration made fit within the greater context of America's history with federal surveillance activities and abuses. This paper does not portend to discuss the constitutionality of the Foreign Intelligence Surveillance Act or the legality of the surveillance programs created after September 11, 2001. That said, it is important for context to have a generalized, high-level overview of applicable authorities related to domestic and international intelligence collection that speak to the violation of norms that sprang up from the choices which this thesis discusses below.

Congress and the executive branch largely solidified standards and norms for the Intelligence Community (IC)—the sixteen federal agencies that comprise the executive branch's intelligence capabilities—after they enacted significant reforms in the aftermath of Watergate and Vietnam-Era abuses.⁹⁵ The reforms came out of revelations uncovered by media outlets and, later, congressional committees who exposed significant civil liberties abuses.⁹⁶ The nation learned that multiple administrations ordered, and several federal agencies like the FBI, CIA, and NSA engaged in, mass surveillance of political activities within the United States.⁹⁷

By the beginning of the twenty-first century, General Michael Hayden, the Director of the National Security Agency, described the NSA as playing “with two strikes” because of these prior abuses.⁹⁸ If “norms are shared cognitive representations” of a group, this

⁹⁵ The number would grow to seventeen in 2004 with the passage of the Intelligence Reform and Terrorism Prevention Act, which created the Office of Director of National Intelligence (ODNI). Congress intended the ODNI to be the head of the Intelligence Community instead of the Director of Central Intelligence (Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, *US Statutes at Large* 118 (2004): 3638–872, codified at *US Code* 50 (2013) §§ 401 et seq.)

⁹⁶ See Laura K. Donohue, *The Future of Foreign Intelligence* (New York: Oxford University Press, 2016), 5–8.

⁹⁷ Donohue, 5–8.

⁹⁸ Hayden, *Playing to the Edge*, 68.

characterization serves as an ingroup recognition of the already tenuous relationship intelligence agencies have with an American public who prize their own liberty and are concerned about government overreach in domestic spying.⁹⁹ As oversight stakeholders exposed revelations from the prior abuses, the American people suddenly turned on the intelligence agencies that for so long acted without many restrictions. Faith in the presidency and government agencies dipped significantly following the scandal of Watergate and the revelations of the Church Committee, which documented that federal agencies engaged in egregious surveillance of innocent citizens for political purposes.¹⁰⁰ The so-called era of the “Imperial Presidency” appeared to be in doubt, with presidential power significantly checked in a time that saw laws enacted such as the War Powers Resolution and the Foreign Intelligence Surveillance Act (FISA).¹⁰¹

Prior to this era, executive intelligence activities were a largely unregulated field of government operations.¹⁰² Indeed, it was not until 1947 with the passage of the National Security Act that Congress entered the realm of intelligence regulation at all, creating a role for itself as a stakeholder in the intelligence process with that legislation.¹⁰³ After the revelations of the Church Committee, Congress enhanced its stakeholder status in the field of intelligence by creating the House Permanent Select Committee on Intelligence, as well as the Senate Select Committee on Intelligence.¹⁰⁴ These bodies provide legislative oversight of the IC.

⁹⁹ See Michael A. Hogg & Scott A. Reid, “Social Identity, Self-Categorization, and the Communication of Group Norms,” *Communication Theory* 16, no. 1 (February 2006): 10.

¹⁰⁰ See Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee), Final Report, S. Rep. No. 94-755 (Washington, DC: Senate, April 29, 1976), <https://www.intelligence.senate.gov/resources/intelligence-related-commissions>.

¹⁰¹ See Arthur M. Schlesinger, Jr., *The Imperial Presidency* (Boston, MA: Houghton Mifflin, 1973); War Powers Resolution, Public Law 93-148, 93rd Cong., 1st sess. (November 7, 1973), 555–60; Foreign Intelligence Surveillance Act of 1978 (FISA), Public Law 95-511, 95th Cong., 2d sess. (October 25, 1978), 1783–98.

¹⁰² Yoo, *War by Other Means*, 114.

¹⁰³ See National Security Act of 1947, Public Law 80-253, 80th Cong., 1st sess. (July 26, 1947), 495–510.

¹⁰⁴ Resolution to Amend the Rules of the House of Representatives and Establish a Permanent Select Committee on Intelligence, H. Res. 658, 95th Cong. (1977); A Resolution to Establish a Standing Committee of the Senate on Intelligence Activities, S. Res. 400, 94th Cong. (1976).

In the shadow of the abuses of the era of Watergate and the Church Committee, and considering several critical legal precedents redefining Fourth Amendment considerations germane to the interception of personal communications and the concept of privacy more generally, Congress' role in setting standards for domestic intelligence authorities and restrictions changed dramatically. Several reforms in the 1960s and 1970s provided what are now baseline authorities and limitations for surveillance capabilities by federal actors. By the early period of the Reagan Administration, regulations and legislative oversight covered the gamut of surveillance activities and content collection. Neither the IC nor their overseers would significantly alter these cultural norms again until after 9/11.

First came legislation governing non-national security interceptions of communications, or “wiretaps.” Title III of the Omnibus Crime Control and Safe Streets Act of 1968 became one of the first legislative controls over government surveillance.¹⁰⁵ Given the colloquial term for “wiretapping,” or the interception of telephonic or electronic communications, Title III is also known as the Wiretap Act.¹⁰⁶ It arose out of the need for reconsidering Fourth Amendment concerns after the Supreme Court ruled in *Katz v. United States*.¹⁰⁷ *Katz* is a seminal case for modern Fourth Amendment legal study. In *Katz*, FBI agents used specialized technology to invade an individual's privacy while he spoke on the telephone within an enclosed phone booth.¹⁰⁸ In making its way through the appellate process, the government cited the then-standard belief that communications in public (outside of the home) are not shielded by the Fourth Amendment's prohibition on unreasonable searches and seizures.¹⁰⁹ In overturning *Olmstead v. United States*, which set this prior precedent in 1928, the Court concluded that *Katz* had a reasonable expectation of privacy in a phone call within an enclosed phone booth when he made attempts to shield

¹⁰⁵ Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351, *US Statutes at Large* 82 (1968): 211–25, codified at *US Code* 34 (2017), §§ 10101 et seq.

¹⁰⁶ See David Medine et al., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Washington, DC: Privacy and Civil Liberties Oversight Board, July 2, 2014), 99.

¹⁰⁷ *Katz v. United States*, 389 U.S. 347 (1967).

¹⁰⁸ *Katz*, 349–52.

¹⁰⁹ *Katz*, 352–53.

the outside world from hearing the call through ordinary means by closing the booth door.¹¹⁰ Essentially, the Court ruled that FBI agents who were able to listen in on Katz's side of the conversation violated his privacy rights. This significant change in legal precedent set off litigation for years to come on the new extent of a citizen's reasonable expectation of privacy and set the stage for the Wiretap Act to establish certain standards for law enforcement's interception of communications.

For the interception of communications, the Wiretap Act set forth certain limitations and considerations for review and prior judicial approval. Before the interception, government actors must obtain judicial authorization via a lengthy application process demonstrating that interception of communications is either the only reasonable option left because other remedies have been exhausted, or alternatively that no other remedy is reasonably likely to obtain success.¹¹¹ The Wiretap Act also attaches the legal standard of probable cause of criminal activity for approval, equivalent to a regular search warrant standard.¹¹² The judicial process pursuant to the Wiretap Act also requires certain judicially-ordered protections to ensure limited intrusions on irrelevant communications, otherwise known as minimization processes.¹¹³ To this day, the Wiretap Act serves as the standard for domestic law enforcement interception actions. State laws typically parallel the Wiretap Act, if not serve to be more restrictive.¹¹⁴ However, one area that Katz and the subsequent Wiretap Act did not legislate was collection for either foreign intelligence or national security purposes. In fact, the Court in Katz specifically reserved ruling on whether the same Fourth Amendment considerations applied in national security matters—the Katz case was merely an “ordinary crime” matter involving gambling.¹¹⁵

¹¹⁰ *Katz*, 350–52, 358.

¹¹¹ Omnibus Crime Control and Safe Streets Act of 1968, 218.

¹¹² Omnibus Crime Control and Safe Streets Act of 1968, 219.

¹¹³ Omnibus Crime Control and Safe Streets Act of 1968, 219–20.

¹¹⁴ See Chapter 934, Florida Statutes, as a reference (*West's Florida Statutes Annotated*, chapter 934, section 934.01 et al (2018)).

¹¹⁵ *Katz*, 354.

National security cases are not immune to Fourth Amendment concerns. In the Keith Case, the Supreme Court decided that the Fourth Amendment applied to domestic content collection on national security grounds when collecting on domestic persons or groups. The Supreme Court recognized (without ruling) that there may be a foreign intelligence exception to the Fourth Amendment.¹¹⁶ This could mean that there could be loopholes to Fourth Amendment applicability in certain activities with a foreign intelligence nexus. The matter before the Supreme Court, however, dealt with domestic extremists looking to destroy a Central Intelligence Agency building in Michigan.¹¹⁷ In justifying content collection without a warrant, the government argued to the Court that there was a national security exception to the Fourth Amendment, and that engaging in a search to prevent a hostile terrorist act like the one in question in that case did not require judicial process.¹¹⁸ The Court ruled in the contrary while leaving open the possibility that foreign intelligence collection efforts may not necessarily require a warrant.¹¹⁹ From there, FISA arose from a need to eliminate judicial and legislative confusion over the potential of a foreign intelligence exception to the Fourth Amendment and its possible scope, the need to give the executive necessary tools, and the need to restrict the executive due to fears from prior abuses.¹²⁰ The Second Circuit Court of Appeals found that “Congress passed FISA to settle what it believed to be the unresolved question of the applicability of the Fourth Amendment warrant requirement to electronic surveillance for foreign intelligence purposes...”¹²¹

FISA filled in gaps left by the Wiretap Act and prior court cases. This critical legislation distinguished itself from the Wiretap Act by setting certain requirements for domestic electronic surveillance, or the interception of electronic communications (a.k.a.

¹¹⁶ *United States v. United States District Court for the Eastern District of Michigan, Southern Division (the Keith Case)*, 407 US 297 (1972).

¹¹⁷ *The Keith Case*, 299.

¹¹⁸ *The Keith Case*, 303.

¹¹⁹ *The Keith Case*, 303–7.

¹²⁰ See Stephen Dycus et al., eds., *Counterterrorism Law*, 3rd ed. (New York: Wolters Kluwer, 2016), 262–63.

¹²¹ *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984), 73.

content) for foreign intelligence collection purposes.¹²² A different set of standards internal to the executive branch govern intelligence collection efforts on communications entirely outside of the country, as found in Executive Order 12333.¹²³ FISA governs the collection of foreign intelligence information on persons inside the United States.¹²⁴ Regardless of whether the target was overseas or within the United States, FISA applies if the government intercepts communications of a person within the United States.¹²⁵ FISA uses a unique, though significantly arduous and complex process to obtain content, while using a distinct evidentiary standard from the Wiretap Act. The FISA process requires the government to provide an application to a judge sitting on the Foreign Intelligence Surveillance Court (FISC).¹²⁶ The Chief Justice of the Supreme Court appoints judges to the FISC, who serve rotating terms for seven years.¹²⁷ As with the involvement of the courts in the Wiretap Act for the process of intercepting domestic communications, through the creation of the FISC, Congress emboldened the new court as a stakeholder in foreign intelligence collection.

The traditional FISA process requires a different standard than the demonstration of probable cause of the commission of a crime to obtain a lawful order. Instead, there must be a reasonable basis to believe that the collection efforts will retrieve foreign intelligence information.¹²⁸ To be the lawful target of a FISA order, the government must demonstrate by probable cause that the target is a foreign power, or an “agent of a foreign power,” which means the target engages in actions for or on behalf of a foreign sovereign, or a designated foreign terrorist group.¹²⁹

¹²² Foreign Intelligence Surveillance Act of 1978 (FISA), Public Law 95-511, *US Statutes at Large* 92 (1978): 1783–98, codified at *US Code* 50 (2015), §§ 1801 et seq.

¹²³ Ronald Reagan, Executive Order 12333, “United States Intelligence Activities,” *Code of Federal Regulations*, title 46 (1981): 59941.

¹²⁴ FISA, *US Code* 50, §§ 1802, 1812.

¹²⁵ FISA, *US Code* 50, §§ 1801, 1802, 1812.

¹²⁶ FISA, *US Code* 50, § 1804.

¹²⁷ FISA, *US Code* 50, § 1803; DOJ IG Report, 77, 59n.

¹²⁸ FISA, *US Code* 50, § 1804.

¹²⁹ FISA, *US Code* 50, § 1805.

Should a judge grant an application, the FISC will require certain minimization procedures to ensure government actors do not abuse uninvolved civilians' privacy rights.¹³⁰ This frequently involves "masking," or anonymizing, the names of uninvolved parties.¹³¹ Mechanisms exist to reveal those names if they are sufficiently relevant to a national security investigation.¹³² Additionally, a FISA application has to demonstrate specifically which "facilities" would be targeted for intelligence collection, requiring certain levels of specificity from the application.¹³³ The text of FISA makes clear Congress' intent that the legislatively-derived process would be the only method for foreign intelligence content collection on domestic soil.¹³⁴ Congress intended this process, like a standard warrant process, to be targeted and specific with particular actors in mind when the government sought the approval of an application. As these methods of content collection demonstrate, pre-action judicial authorization was a normative expectation for domestic law enforcement and intelligence officials long before September 11, 2001.

After the events of September 11, 2001, Congress and the Bush Administration quickly sought to determine what steps were necessary to ensure that the national security apparatus had the appropriate tools to combat terrorism in the new war with Al Qaeda. Within weeks of the attacks, both chambers of Congress passed the USA PATRIOT Act (PATRIOT Act), and President Bush signed the legislation on October 26, 2001.¹³⁵ Importantly, the PATRIOT Act amended intelligence collection authorities under FISA for federal law enforcement and intelligence officials, updating FISA's authorities to meet twenty-first century issues. It allowed for roving wiretaps in light of advancements in cellular telephone technology and the increased likelihood that targeted individuals may use multiple phones, devices, or facilities in short order to mitigate monitoring

¹³⁰ FISA, *US Code* 50, § 1805.

¹³¹ See Hayden, *Playing to the Edge*, 65-66; FISA, *US Code* 50, § 1805.

¹³² Hayden, 65-66.

¹³³ FISA, *US Code* 50, § 1804.

¹³⁴ FISA, *US Code* 50, § 1812.

¹³⁵ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Public Law 107-56, 107th Cong., 1st sess. (October 21, 2001): 272-402.

capabilities.¹³⁶ The PATRIOT Act also significantly changed the substance and importance of the business records provision of FISA through section 215 of that legislation.¹³⁷ Previously, the government could obtain certain records—for instance, car rental records—with individualized suspicion that an agent of a foreign power might have created or used them.¹³⁸ The legislation also altered the requirement that foreign intelligence collection be the “primary purpose” of a FISA application, amending the standard to only require “a significant” purpose, while also allowing for concurrent justifications such as criminal investigations.¹³⁹ In combination with changes in sharing authorities between law enforcement and intelligence officials, this change led to the elimination of “the wall” between intelligence collection and law enforcement agencies.¹⁴⁰ This metaphorical wall was a prohibition on sharing foreign intelligence information obtained through the FISA process based on constitutional concerns, and many believed it to be a leading detriment to the country’s intelligence capabilities prior to 9/11.¹⁴¹ After the PATRIOT Act, government actors had access to any “tangible things” that “the government believed would be helpful in a national security investigation,” “including books, records, papers, documents, and other items.”¹⁴² The legislation removed any individualized suspicion requirement for the government to obtain such records.¹⁴³ A 2004 reauthorization would also incorporate “lone wolf” singular actors of terrorism as permissible targets, in addition to foreign powers and agents of foreign powers.¹⁴⁴ Through

¹³⁶ USA PATRIOT Act of 2001, 282.

¹³⁷ USA PATRIOT Act of 2001, 287–88.

¹³⁸ See Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*, CRS Report No. RL30465 (Washington, DC: Congressional Research Service, 2004), 53–56, <https://fas.org/irp/crs/RL30465.pdf>.

¹³⁹ USA PATRIOT Act of 2001, 291.

¹⁴⁰ See Donohue, *The Future of Foreign Intelligence*, 26–31.

¹⁴¹ Donohue, 15.

¹⁴² USA PATRIOT Act of 2001, 287–88.

¹⁴³ USA PATRIOT Act of 2001, 287.

¹⁴⁴ IRTPA, 3742–43.

each of these authorizations, Congress established itself as a relevant stakeholder in the intelligence process.

In an example of how the prevention narrative can take hold in a social group outside of intelligence agencies, the cloud of 9/11 hung over Congress in the weeks after the attacks, stifling debate on the PATRIOT Act.¹⁴⁵ Some commentators at the time expressed concern that most members of Congress had not read the majority of the legislation even though it was the most substantial adjustment to foreign intelligence collection authorities in over a generation.¹⁴⁶ Even politicians who fervently aligned with civil liberties groups recognized the shadow of 9/11 hanging over the country and the urgency to prevent a future attack.¹⁴⁷ Federal authorities became “substantially broader” after passage of the PATRIOT Act.¹⁴⁸ For supporters, the PATRIOT Act served as a major boon to national security investigations. For detractors, it represented the possibility of significant government abuses of civil liberties.¹⁴⁹ Yet what the clear majority of Washington, D.C., did not know at the time was that select members of the executive branch were also discussing additional ways to amplify intelligence resources and capabilities in counterterrorism efforts.

C. STELLARWIND AND NSA SURVEILLANCE

Immediately after America’s worst domestic attacks since Pearl Harbor, the nation’s security apparatus kicked into high gear. Leadership at the National Security Agency quickly took steps to enhance the agency’s intelligence collection efforts. NSA Director Michael Hayden, an Air Force general and career intelligence officer, amended the expectations for “unmasking” U.S. persons in foreign intelligence collection.¹⁵⁰ Typically, intelligence officials anonymize U.S. persons’ information during the collection

¹⁴⁵ Edgar, *Beyond Snowden*, 19.

¹⁴⁶ Edgar, 19.

¹⁴⁷ Edgar, 18.

¹⁴⁸ Bazan, “The Foreign Intelligence Surveillance Act,” 54.

¹⁴⁹ Edgar, 18.

¹⁵⁰ Hayden, *Playing to the Edge*, 65–66.

process out of respect for personal privacy concerns when the government collects irrelevant U.S. person information. Officials can “unmask” U.S. person information, or have the anonymized information added back into the intelligence materials, when it is “critical to understanding the significance of intelligence.”¹⁵¹ In the aftermath of 9/11, Director Hayden ordered his analysts to “lower the bar” as to when officials unmasked U.S. person information in the course of collecting foreign intelligence information, meaning that NSA personnel could more easily identify specific U.S. persons in captured communications.¹⁵²

Shortly after 9/11, Hayden’s superiors—Director of Central Intelligence George Tenet, Vice President Dick Cheney, and President George W. Bush—raised questions about what exactly the NSA could do moving forward. Hayden gave those three men an explanation of his efforts to expand NSA capabilities within his current authorities. When Tenet, at the request of the Vice President, asked if there was anything else he could do, Hayden replied “not within my current authority.”¹⁵³ Next came a pointed question: what if authorities were not an issue? What would be the maximum capabilities of the NSA absent of any restrictions? Hayden told Tenet that he would need to think about how to respond.¹⁵⁴ With the weight of that question hanging on him, Hayden returned to the NSA facilities in Fort Meade, Maryland, where he met with his leadership team and legal counsel.¹⁵⁵ During the conversations that followed, NSA leadership conceived of the program that would be known as Stellarwind.¹⁵⁶ When Hayden brought the proposed program to the White House, he asserted that this program required new authorities to engage in novel intelligence collection efforts.¹⁵⁷ The president approved of the program,

¹⁵¹ Hayden, 65–66.

¹⁵² Shane Harris, *The Watchers: The Rise of America’s Surveillance State* (New York: Penguin Press, 2010), 167; Hayden, *Playing to the Edge*, 65.

¹⁵³ Hayden, 66.

¹⁵⁴ Hayden, 66.

¹⁵⁵ Hayden, 66–68.

¹⁵⁶ Hayden, 66–68.

¹⁵⁷ Hayden, 68.

and Hayden was informed that the NSA was to move ahead under the president's strict Article II constitutional authority.¹⁵⁸

Stellarwind primarily consisted of two new intelligence collection programs within the NSA. First, Stellarwind amended the NSA's typical practices of surveilling international telephone calls.¹⁵⁹ The expectation for the NSA after the civil liberties abuses of the 1960s and 1970s was that the NSA would have no involvement in domestic surveillance. The FBI was the agency in charge of domestic intelligence, and that was primarily from an investigative perspective as opposed to domestic intelligence collection. As noted earlier, government actors could not engage in domestic surveillance to collect the content of communications at this time unless done pursuant to the Wiretap Act or FISA processes, and as a normative principle the NSA took no part in domestic operations. Now, the Bush Administration sought to unilaterally reinterpret those expected norms. Hayden argued that the NSA would not take part in purely domestic content collection, instead focusing on foreign intelligence collection; however, under the new interpretation, international calls with one end located within the United States was sufficiently "foreign" when the target was suspected of association with Al Qaeda.¹⁶⁰ The location or citizenship status of the people on the call in the United States was now irrelevant. This new analysis was a significant departure from prior precedent, which historically would have described such communications as foreign or international.¹⁶¹ As Hayden described it, this was not any different than the distinctions between domestic and international flights as there is no such thing as a domestic flight that has one leg outside of the United States.¹⁶² Further,

¹⁵⁸ Hayden, 68; Article II authority is a reference to the president's authorities and obligations pursuant to Article II, section 2 of the U.S. Constitution as the commander in chief and its inherent defense war powers to repel attacks against the nation in times of war (see US Constitution, art. 2, sec. 2; see also *The Prize Cases*, 67 U.S. 635 (1862)).

¹⁵⁹ DOJ IG Report, 20–23.

¹⁶⁰ Hayden, *Playing to the Edge*, 109–10.

¹⁶¹ Harris, *The Watchers*, 158.

¹⁶² Hayden, *Playing to the Edge*, 109–10.

NSA personnel argued that the evolution of communications systems drastically changed the relevancy of FISA.¹⁶³

These arguments may have some merit, but the unilateral development of this analysis requires emphasis here. This analysis that quickly went through the National Security Agency and the White House—through only a handful of decision makers without the value of other perspectives from relevant stakeholders—presented a massive shift in normative expectations about the world’s most powerful spy agency. Relatively speaking, this analysis worked through little to no debate. On October 4, 2001, while the PATRIOT Act was still working through Congress, President Bush signed an order authorizing the Stellarwind program.¹⁶⁴ Counsel to the Vice President David Addington drafted the order to authorize Stellarwind without recognizing any FISA obligations.¹⁶⁵ Prior to the president signing the order on October 4, 2001, the order was “pushed in front of” John Ashcroft to aver to its legality.¹⁶⁶ Ashcroft signed off on the program. The order provided no legal analysis or justification for the program.¹⁶⁷ The signing of the order signified the first time that “foreign intelligence” included Americans’ private communications.¹⁶⁸

Still, even with this new interpretation, the NSA as an agency was strongly attached to the cultural norm of its mission to collect foreign intelligence information, so when David Addington suggested that the Stellarwind authorization would actually allow the collection of any communication related to Al Qaeda, even if purely domestic, Hayden refused to engage in such actions.¹⁶⁹ Hayden believed there had to be some international nexus to justify this new interpretation.¹⁷⁰ Prior to Stellarwind, the NSA already had

¹⁶³ Hayden, 97, 106–7; Edgar, *Beyond Snowden*, 130.

¹⁶⁴ DOJ IG Report, 28.

¹⁶⁵ Charlie Savage, *Power Wars: Inside Obama’s Post-9/11 Presidency* (New York: Little, Brown and Company, 2015), 183–84.

¹⁶⁶ DOJ IG Report, 30.

¹⁶⁷ DOJ IG Report, 31, 33.

¹⁶⁸ See DOJ IG Report, 29.

¹⁶⁹ Hayden, *Playing to the Edge*, 72–73.

¹⁷⁰ Hayden, 72–73.

domestic telecommunication hubs staked out with technological surveillance capabilities, but only collected purely foreign-to-foreign information because of privacy concerns and respect for the FISA process.¹⁷¹

From the program's inception, secrecy surrounded its existence. The few Department of Justice members who were aware of Stellarwind called it "the program."¹⁷² Stellarwind was also known by another name inside the NSA's technology groups: The Big Ass Graph, or "BAG" for short.¹⁷³ It was an attempt to turn "big data" into visual representations of heretofore unseen anomalies. Within the NSA, this representation of the BAG was a culmination of the rise of the wave of big data that had been looming for years, threatening to leave the NSA in the dark unless they kept up with the times.¹⁷⁴ Now, with new authorities and increased tools, the NSA could use increasing amounts of seemingly innocuous data points and run that information through algorithms so that intelligence officials could visualize anomalies.¹⁷⁵ In theory, this was not dissimilar from another intelligence-led program called Total Information Awareness, led by John Poindexter, which Congress shut down in 2003 over concerns of domestic spying.¹⁷⁶ While it was not made public at the time, parts of the Total Information Awareness program secretly moved over to NSA control after the program's shuttering.¹⁷⁷ However, in practice the program led to a technological system overstuffed with data points and without effective means of discerning the value of the underlying data.¹⁷⁸

The secrecy of the Stellarwind program was clearly intentional. Few people knew about Stellarwind, and the White House allowed even fewer into any discussions about execution or implementation. Decision makers who implemented Stellarwind kept people

¹⁷¹ Savage, *Power Wars*, 181.

¹⁷² Lichtblau, *Bush's Law*, 140.

¹⁷³ Shane Harris, *The Watchers*, 199.

¹⁷⁴ Harris, 199.

¹⁷⁵ Harris, 199, 204–5.

¹⁷⁶ Harris, 164, 251.

¹⁷⁷ See Harris, 246–51.

¹⁷⁸ Harris, 208–9.

who, by their positions in their respective agencies would have known of a program like Stellarwind, in the dark. By the end of 2003, only five Department of Justice officials were fully read into the Stellarwind program, and Counsel to the Vice President David Addington's preference was to further limit people being "read in."¹⁷⁹ The self-described "War Council" was the primary body of decision makers involved in counterterrorism efforts in the early days of the Bush Administration's response to the 9/11 attacks.¹⁸⁰ This group included White House Counsel Alberto Gonzales, White House Deputy General Counsel Tim Flanigan, General Counsel for the Department of Defense Jim Haynes, Counsel to the Vice President David Addington, and John Yoo, an attorney within the Office of Legal Counsel (OLC) in the Department of Justice who specialized in executive and war power authorities.¹⁸¹ Public accounts suggest that an even smaller number of individuals within the War Council held any actual influence.

As a general matter, the War Council met privately to preemptively steer or eliminate important decisions before interagency processes could work through legal or policy issues related to wartime or counterterrorism decisions.¹⁸² Notably, Jay Bybee, the head lawyer at OLC (and Yoo's supervisor), was not on the Council even though the OLC was frequently equated to the general counsel of the Department of Justice.¹⁸³ He also did not know about Stellarwind.¹⁸⁴ Even the attorney general, John Ashcroft, was not in the War Council, though he knew about Stellarwind. After making the determination to move forward with Stellarwind, the White House asked Yoo to provide legal guidance authorizing the program.¹⁸⁵ Yoo's analysis was fundamental in providing legal cover to political and operational members involved in Stellarwind. Yoo concluded that any communications including foreign persons made the entirety of the conversation "foreign

¹⁷⁹ DOJ IG Report, 103, 110, 191.

¹⁸⁰ Goldsmith, *The Terror Presidency*, 22.

¹⁸¹ Goldsmith, 22.

¹⁸² Goldsmith, 22.

¹⁸³ Goldsmith, 22.

¹⁸⁴ DOJ IG Report, 40.

¹⁸⁵ DOJ IG Report, 25, 101–2.

intelligence,” consistent with Hayden’s perspective.¹⁸⁶ Yoo also argued that FISA and other statutory obligations were subservient to the president’s wartime authorities, arguing that the president did not need to comply with any laws that hindered his constitutional authorities in defending the country.¹⁸⁷ These legal arguments were made in an unusually narrow informational stove pipe and kept there to avoid, at the minimum, contradictory legal interpretations. David Addington did not even allow the general counsel for NSA, in trying to determine the legality of the program himself for Director Hayden’s satisfaction, to review Yoo’s memorandum upon request, though Addington did read out some elements of Yoo’s arguments over the phone to Hayden’s legal advisor.¹⁸⁸

D. FIRST SIGNS OF CONFLICT

However, an initiative as massive and consequential as Stellarwind proved difficult to keep quiet. Questions quickly started arising in the Department of Justice regarding from where certain information in FISA applications came. The attorney general told Larry Thompson, the deputy attorney general who was in charge of the Department of Justice’s Office of Intelligence Policy and Review (a critical part of the process for reviewing FISA applications), that Thompson did not need to know where the information came from.¹⁸⁹ “I’m sworn to secrecy by the president and the vice president,” he told Thompson.¹⁹⁰ In his position, Thompson had a hand in reviewing, approving, and legally swearing to the factual basis of information articulated in FISA order applications. Similarly, the White House did not originally tell James Baker, the top intelligence lawyer at the Department of Justice, about the Stellarwind program.¹⁹¹ When he figured out that Stellarwind

¹⁸⁶DOJ IG Report, 29; John Yoo, “Memorandum for the Attorney General” (official memorandum, Washington, DC: Department of Justice, November 2, 2001), <https://www.justice.gov/sites/default/files/olc/legacy/2011/03/25/johnyoo-memo-for-ag.pdf>.

¹⁸⁷ DOJ IG Report, 34; Yoo, “Memorandum for the Attorney General,”; John Yoo, “Authority for Warrantless National Security Searches” (letter to Judge Colleen Kollar-Kotelly, May 17, 2002), <https://www.justice.gov/olc/page/file/936196/download>, 7.

¹⁸⁸ Hayden, *Playing to the Edge*, 70; DOJ IG Report, 111.

¹⁸⁹ Lichtblau, *Bush’s Law*, 140–41.

¹⁹⁰ Lichtblau, 141.

¹⁹¹ DOJ IG Report, 70.

information was seeping into the department's standard FISA applications, Baker wanted the FISC informed about the program so as to not threaten the department's relationship with the Court.¹⁹² At one point, Baker refused to sign a FISA order application that included Stellarwind information, even when Addington wanted to fire Baker for insubordination.¹⁹³

Initially, despite their positions as stakeholders in the collection of foreign intelligence information, the White House prevented judges on the FISC, as well as members of Congress, from learning about Stellarwind.¹⁹⁴ Some people, like Director Hayden, had concerns that a lack of knowledge by the other branches of government could enhance the executive's vulnerability when (not if) the program leaked.¹⁹⁵ This concern highlights one element of the potential value in garnering stakeholder support: obtaining better awareness and acceptance from relevant parties can provide a more substantial foundation of support from which to engage novel intelligence efforts.

After pressing from within the Department of Justice, General Hayden, John Ashcroft, Robert Mueller, John Yoo, and James Baker notified Chief Judge of the Foreign Intelligence Surveillance Court Royce Lamberth about the operational details and legal framework of the program.¹⁹⁶ However, sources assert that Hayden, Yoo and Baker were there to inform Lamberth about Stellarwind, not to request approval. Lamberth "wasn't being asked to do anything...it was clear no one was asking him to approve it. That was absolutely clear," one official said.¹⁹⁷ Yoo and Hayden sensed that the meeting was cordial and professional, walking away comfortable with their efforts to bring the FISC into the fold of the operation.¹⁹⁸ However, while not speaking up in the meeting, Lamberth had significant concerns about the legality of the program and took substantial steps with Baker

¹⁹² DOJ IG Report, 74.

¹⁹³ DOJ IG Report, 75–76.

¹⁹⁴ Savage, *Power Wars*, 187; Hayden, *Playing to the Edge*, 77; DOJ IG Report, 75.

¹⁹⁵ Hayden, 76–77.

¹⁹⁶ DOJ IG Report, 77.

¹⁹⁷ Lichtblau, *Bush's Law*, 167; DOJ IG Report, 77.

¹⁹⁸ Hayden, *Playing to the Edge*, 80–82.

and other professionals in the Department of Justice to ensure that any applications for FISA orders that came before the FISC did not include any information from the Stellarwind program to ensure the FISC process was not tainted; Lamberth once said that “[i]f anything was presented to the FISA court that came from the program, the FISA court had to be told about it.”¹⁹⁹

This conflict between the executive branch and the FISC, though hardly anyone saw it, created significant unintended consequences; the time and resources that went into sufficiently separating Stellarwind information from other FISA application materials became a staggering practice. Ashcroft signed applications that included such information because Thompson could not aver to the legality of the collection of the information without being read into the NSA program.²⁰⁰ Numerous attorneys chose to opt out of handling such issues when given the opportunity.²⁰¹ At the time, Lamberth was the only judge on the FISC to know about the program, but upon his departure from the FISC the White House informed his successor, Colleen Kollar-Kotelly, of the program.²⁰² Kollar-Kotelly continued the practices established by Lamberth when she took over as chief judge of the FISC, and she would grow tired of increasing information creeps of Stellarwind information into FISA applications.²⁰³ She even demanded senior officials aver to the legitimacy of the information sources and threatened perjury charges for those who did not disclose Stellarwind information that crept into FISA applications.²⁰⁴ These demands actually once led to the temporary shuttering of the program.²⁰⁵

Once it started again, there were concerns within the Department of Justice that any more improper Stellarwind information in FISA applications could lead the FISC to take

¹⁹⁹ Greg Gordon, “Bush Domestic Spying Program Flawed, Former FISA Court Chief Says,” *McClatchy Newspapers*, June 23, 2007, <https://www.mcclatchydc.com/news/nation-world/national/article24465583.html>; Lichtblau, *Bush’s Law*, 171; DOJ IG Report, 78–83.

²⁰⁰ Lichtblau, 172; DOJ IG Report 82.

²⁰¹ Lichtblau, 172.

²⁰² DOJ IG Report, 78, 83.

²⁰³ Lichtblau; 172–73; DOJ IG Report, 84–88.

²⁰⁴ Lichtblau, 173.

²⁰⁵ Lichtblau, 173.

more strident countermeasures.²⁰⁶ Stellarwind would continue to prove controversial among FISC judges for years to come.²⁰⁷ After the *New York Times* first revealed the Stellarwind program to the nation, and after the President's swift confirmation of Stellarwind (or what he would dub the "Terrorist Surveillance Program") in his weekly news address, Judge James Robertson resigned from the FISC in protest.²⁰⁸ It appears that critical decision makers either did not know or care about this conflict, which played out between attorneys at the Department of Justice and the FISC judges.

Over time, new players disrupted the Bush Administration's efforts at secrecy. In 2003, the White House appointed Jack Goldsmith to lead the OLC, replacing Jay Bybee. This happened after Attorney General John Ashcroft blocked the nomination of John Yoo, who left government shortly thereafter to return to teaching.²⁰⁹ Goldsmith, himself a law professor, had the support of Jim Haynes and Yoo to be a suitable replacement on the War Council.²¹⁰ Once in office, Goldsmith began to learn some of the government's most closely held secrets, including several controversial OLC opinions. Upon review, Jack Goldsmith found legal opinions from John Yoo to be "sloppily reasoned, over broad, and incautious..."²¹¹ He was greatly concerned that several of the most sensitive counterterrorism policies "rested on severely damaged legal foundations."²¹² When Goldsmith concluded that he needed to repeal and rewrite several memoranda, he expected conflict with the White House.²¹³ Goldsmith believed that certain aspects of Stellarwind, including some aspects of the bulk metadata collection efforts, were likely illegal.²¹⁴

²⁰⁶ Lichtblau, 173.

²⁰⁷ See Savage, *Power Wars*, 200–7.

²⁰⁸ Keith Garvin, "Judge Resigns from Surveillance Court," *ABC News*, December 21, 2005, <https://abcnews.go.com/Politics/story?id=1429647> (accessed July 1, 2018).

²⁰⁹ Goldsmith, *The Terror Presidency*, 24.

²¹⁰ Goldsmith, 25.

²¹¹ Goldsmith, 10.

²¹² Goldsmith, 10.

²¹³ Goldsmith, 11.

²¹⁴ Savage, *Power Wars*, 190–91; "Goldsmith said that not a single critical eye reviewed Yoo's work on a program that Goldsmith described as 'flying in the face' of the conventional understanding of the law at the time" (DOJ IG Report, 194).

In 2003, Goldsmith notified Ashcroft that he wanted to get the NSA program on more solid legal footing. This effort accelerated with the appointment of James Comey as the Deputy Attorney General. Comey, like his predecessors, initially did not know about the program.²¹⁵ Director Hayden briefed Comey on the program after Patrick Philbin and Jack Goldsmith pushed Addington to read Comey into the program.²¹⁶ In another illustration of the norm-defying nature of the Stellarwind program, Comey found himself “stunned” that the government was intercepting communications of Americans without a warrant or any judicial review.²¹⁷ In early March 2004, Comey informed the White House that he did not believe he could reauthorize the Stellarwind program as the Acting Attorney General in place of Ashcroft, who had fallen ill and was hospitalized.²¹⁸ For the prior nine months, Jack Goldsmith at the Department of Justice warned the White House that the program was on untenable footing.²¹⁹

On March 10, 2004, eight congressional leaders met in the White House Situation Room for another briefing with Hayden and the vice president on the Stellarwind program.²²⁰ One of the purposes of this meeting was to determine what remedies might be available in light of concerns over waning DOJ support.²²¹ The group tabled discussions of legislative remedies over concerns that public discussions would disrupt too much of the program.²²² Chief of Staff Andrew Card and White House Counsel Alberto Gonzales perceived an implicit backing from the select members of Congress in attendance. The

²¹⁵ DOJ IG Report, 118.

²¹⁶ DOJ IG Report, 118.

²¹⁷ Lichtblau, *Bush's Law*, 178; “Comey told us that his initial reaction to the program was ‘unprintable’” (DOJ IG Report, 118).

²¹⁸ Comey, *A Higher Loyalty*, 85; DOJ IG Report, 198.

²¹⁹ DOJ IG Report, 197–98.

²²⁰ DOJ IG Report, 131–32.

²²¹ DOJ IG Report, 131–33.

²²² DOJ IG Report, 133–34.

support from this meeting led Card and Gonzales to seek Ashcroft's authorization at the George Washington University Hospital.²²³

Two particular concerns prompted the infamous hospital dispute related at the outset of this chapter, according to reporting by Charlie Savage of the *New York Times*: specifically, Goldsmith, Comey, and other Department of Justice officials expressed concerns about the legality of the bulk records collection program in Stellarwind, notably the email component.²²⁴ They were also concerned with the collection of content against targets tied to international terrorism that were not associated with Al Qaeda.²²⁵ After review of John Yoo's OLC opinion, Jack Goldsmith demurred on the broad, expansive Article II authorities cited by Yoo, instead focusing a legal footing for Stellarwind on the Authorization for the Use of Military Force passed by Congress after 9/11.²²⁶ The administration shuttered the bulk email collection component to Stellarwind to appease Comey, Mueller, and Goldsmith.²²⁷ The president ordered several elements of the program shut down altogether to ensure compliance with Department of Justice demands. This edict also contributed to a push to bring the Stellarwind program under the authority of the FISC.²²⁸ Through efforts from 2004 to 2006, the Department of Justice obtained authorization from the FISC for two-thirds of the surveillance programs.

Even though the administration began to normalize Stellarwind after the incident at the George Washington University Hospital, the White House still maintained unusual levels of secrecy about the program. Not long after that incident, the *New York Times*

²²³ *Hearing on Oversight of the Department of Justice*, Senate Judiciary Committee, 110th Cong., 1st sess., July 24, 2007, http://www.washingtonpost.com/wp-srv/politics/documents/gonzalez_transcript_072407.html; Hayden, *Playing to the Edge*, 87.

²²⁴ Savage, *Power Wars*, 191.

²²⁵ Savage, 191.

²²⁶ Charlie Savage, "Redactions in U.S. Memo Leave Doubts on Data Surveillance Program," *New York Times*, September 6, 2014, <https://www.nytimes.com/2014/09/07/us/redactions-in-us-memo-leave-doubts-on-data-surveillance-program.html>; DOJ IG Report, 182–86.

²²⁷ Savage, *Power Wars*, 193–94.

²²⁸ Savage, 194.

published its story revealing Stellarwind.²²⁹ Despite the press report and presidential acknowledgement, government access to the program remained tight.²³⁰ The White House blocked Glenn Fine, Inspector General for the Department of Justice, from investigating anything related to the program.²³¹ Likewise, the White House prevented Marshall Jarrett, who ran the Office of Professional Responsibility in the Department of Justice, from obtaining access to the program—leaving Jarrett with no other option than to close an opened investigation.²³² The administration also blocked The Privacy and Civil Rights Oversight Board, an office within the White House, from accessing the program even after its public disclosure.²³³ Later, at a hearing before the Senate Judiciary Committee, Alberto Gonzales said that the president himself made determinations of who was read into the program.²³⁴

Still, the normalization process continued. For legalizing the final leg of Stellarwind, the government sought to bring the warrantless surveillance program involving content collection with one end of a communication residing within the United States under the FISC’s authority. In December 2006, the government issued an application to the FISC to authorize the program.²³⁵ The application sought to re-envision the term “facility” in FISA, typically applied to a target like a particular phone number or email address, to apply to an entire communications hub or switch through which significant numbers of calls or electronic communications may flow.²³⁶ The FISC gave the

²²⁹ James Risen and Eric Lichtblau, “Bush Lets U.S. Spy on Callers Without Courts,” *New York Times*, December 16, 2005, <https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>.

²³⁰ After the *New York Times* revealed the program, President Bush used a weekly address to acknowledge and attempt to mitigate concerns about the “Terrorist Surveillance Program” (see Savage, 196; Lichtblau, *Bush’s Law*, 212-13; David Sanger, “Bush Says He Ordered Domestic Spying,” *New York Times*, December 18, 2005, <https://www.nytimes.com/2005/12/18/politics/bush-says-he-ordered-domestic-spying.html>).

²³¹ Lichtblau, *Bush’s Law*, 226–27.

²³² Lichtblau, 227–29.

²³³ Lichtblau, 226.

²³⁴ Lichtblau, 229.

²³⁵ DOJ IG Report, 245.

²³⁶ DOJ IG Report, 240–41.

government a blanket authorization to target individuals who met this standard for content collection, without a particularized authorization on a certain phone number or identifier.²³⁷ This order also limited collection only to targets who were believed to be located outside the United States, though the other end of the communications could be within the country.²³⁸ This new event led Attorney General Alberto Gonzales on January 17, 2007, to announce that the executive branch had reached an “innovative” agreement with the FISC to ensure “speed and agility” for the controversial surveillance programs within the purview of FISA.²³⁹

Yet, in April, another FISC judge balked at his colleague’s interpretation of “facility”; Judge Robert Vinson argued against the highly generalized probable cause finding authorized by his colleague on the FISC and did not consent to the NSA unilaterally determining when a particular individual fit into that categorization.²⁴⁰ Vinson told the government that it would have to demonstrate particularized probable cause to the FISC for content collection of this sort.²⁴¹ If the government did not care for this ruling, through his heavy reliance on Congressional statutory intent, he suggested that the executive branch should go to Congress for a resolution.²⁴² The creative lawyering had gone on far enough and threatened to completely obfuscate the law. The administration once again saw the FISC as a roadblock to its goals rather than an integral stakeholder. The rejection led Alberto Gonzales to say Vinson’s opinion “confirmed our concern about going to” the FISC at all.²⁴³

²³⁷ DOJ IG Report, 241–42, 246.

²³⁸ DOJ IG Report, 245–46; *In re [redacted]*, Order (FISA Ct., 2007), <https://www.documentcloud.org/documents/1379006-large-content-fisa-order-documents.html>, 129–48.

²³⁹ Alberto Gonzales, “Correspondence Regarding Foreign Intelligence Surveillance Court Order” (letter to the Honorable Patrick Leahy and the Honorable Arlen Specter, January 17, 2007), <https://www.documentcloud.org/documents/1018118-alberto-gonzales-bsp-letter.html>.

²⁴⁰ DOJ IG Report, 253; *In re [redacted]*, Order and Memorandum Opinion (FISA Ct., 2007), <http://goo.gl/dL3eHm>, 6–12.

²⁴¹ DOJ IG Report, 253–54; *In re [redacted]*, Order and Memorandum Opinion (FISA Ct., 2007), 14–16.

²⁴² DOJ IG Report, 252; *In re [redacted]*, Order and Memorandum Opinion (FISA Ct., 2007), 12–16.

²⁴³ DOJ IG Report, 255.

Though Judge Vinson’s decision led to panic in the IC, the administration obtained a legislative resolution in short order. The immediate fear after Judge Vinson’s denial of the government’s application led to a rushed process wherein the executive branch finally sought legislative authorization for its activities or risk shuttering the unsanctioned efforts altogether. The end result was the passage of the Protect America Act of 2007, followed just a few months later by the FISA Amendments Act.²⁴⁴ The FISA Amendments Act allowed the Attorney General and Director of National Intelligence (DNI) to authorize targeted collection on non-US persons for one year when reasonably believed to be overseas.²⁴⁵ The FISA Amendments Act also prohibited the government from collecting wholly domestic communications outside of the traditional FISA process, which David Addington suggested his draft order signed by the president on October 4, 2001, already allowed.²⁴⁶ The FISA Amendments Act also expanded the purpose justifications from those being related to Al Qaeda and associated terrorist organizations to those with foreign intelligence value.²⁴⁷ These pieces of legislation resolved the immediate conflicts surrounding the Stellarwind surveillance program, but left remaining several institutional harms, as outlined in the following chapter.

The preceding facts make clear that the Bush Administration, and specifically the War Council, intentionally used excessive secrecy as a tool, which ultimately became harmful to the administration’s goals. Instead of an efficient intelligence process, the administration’s exclusion of key stakeholders led to a continual roller coaster of panic and uncertainty when more integral actors learned of Stellarwind. From the perspective of efficiency, these inconsistent and sporadic shocks to the system proved damaging. In the next chapter, this thesis examines additional harms unnecessarily created by the administration through these events. The next chapter also introduces the social identity

²⁴⁴ Protect America Act of 2007, Public Law 110-55, 110th Cong., 1st sess. (August 5, 2007): 552–57; Foreign Intelligence Surveillance Act of 1978 Amendments Act (FISA Amendments Act) of 2008, Public Law 110-261, *US Statutes at Large* 122 (2008): 2436–478, codified at *US Code* 50 (2015), §§ 1801 et seq.

²⁴⁵ FISA Amendments Act, 2438.

²⁴⁶ FISA Amendment Act of 2008, 2438.

²⁴⁷ FISA Amendments Act of 2008, 2440.

perspective as an analytical tool to understand the social dynamics at play in this case, and to understand why certain actors fostered the “prevention at all costs” narrative.

III. UNDERSTANDING THE TROUBLED WATERS OF SOCIAL CONFLICT

This chapter reviews publicly available information about the actions of the decision makers involved in the creation and implementation of the post-9/11 NSA surveillance programs. Using the social identity perspective, this case study focuses on the conflict and social dynamics between the War Council and several other social groups. Specifically, this study provides evidence for leaders of intelligence organizations that certain actions and methods—intentional or perceived—can lead to conflict or resolution among social groups. This is important because intelligence enterprises, like any organization, have employees who associate with other people in social groups who work with or for other groups in an organization. Through the publicly recorded acts and comments of officials involved, this study also demonstrates how the “prevention at all costs” narrative (“the prevention narrative”) shades the analysis of leaders in charge of security, and why leaders must recognize the effect of this trend on their subordinate groups. Importantly, this analysis begins with an introduction to the social identity perspective, a model of analysis from the field of social psychology, to understand relevant dynamics.

A. INTRODUCTION TO THE SOCIAL IDENTITY PERSPECTIVE

The social identity perspective focuses on the way people interact in social groups. Henri Tajfel defined social identity as “the individual’s knowledge that he belongs to certain social groups together with some emotional and value significance to him of this group membership.”²⁴⁸ In other words, people derive some sense of their identity from the associations they hold. This definition provided three critical components of a social identity approach—how a person perceives group associations, how a person evaluates

²⁴⁸ Henri Tajfel, English Manuscript of “La Catégorisation Sociale,” in *Introduction à la Psychologie Sociale*, ed. Serge Moscovici (Paris: Larousse, 1972), 292, quoted in Michael A. Hogg, “A Social Identity Theory of Leadership,” *Personality and Social Psychology Review* 1, no. 3 (August 2001): 186.

those associations, and how a person emotionally values those associations.²⁴⁹ Social identity views the existence of one's group associations through a comparative evaluation with other groups.²⁵⁰ The value of one's membership in a particular ingroup largely comes from comparisons to other outgroups; as such, in an effort to be better or sufficiently distinct to justify their existence, social groups collectively seek to establish their value and worth in comparison with other groups, which inherently triggers the possibility of conflict between groups.²⁵¹ In other words, group members will try to establish that they are distinct from or better than other groups to justify a group's value.²⁵² Social groups also strive for stability and certainty, trying to reduce uncertainty whenever possible.²⁵³ People join social groups to obtain those benefits, and seek to positively rationalize their ingroup's value so as to improve their own sense of identity.

The social identity perspective includes a number of relevant theories and sub theories, including social identity theory and social cognition theory.²⁵⁴ Social identity theory grew out of Tajfel's work in social psychology, eventually leading to Tajfel's articulation of the theory in his work with John Turner in 1979.²⁵⁵ Turner later built upon this theory by focusing on the cognitive processes to create social cognition theory.²⁵⁶

²⁴⁹ Don Operario and Susan T. Fiske, "Integrating Social Identity and Social Cognition: A Framework for Bridging Diverse Perspectives," in *Social Identity and Social Cognition*, ed. Dominic Abrams and Michael A. Hogg (Oxford: Blackwell, 1999), 42.

²⁵⁰ Hogg, "A Social Identity Theory of Leadership," 186.

²⁵¹ Hogg, 186.

²⁵² John C. Turner, "Social Comparison and Social Identity: Some Prospects for Intergroup Behaviour," *European Journal of Social Psychology* 5, no. 1 (January/March 1975): 8.

²⁵³ Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 38; David E. Rast, III, et al., "Leadership Under Uncertainty: When Leaders Who Are Non-Prototypical Group Members Can Gain Support," *Journal of Experimental Social Psychology* 48, no. 3 (May 2012): 646–47.

²⁵⁴ Michael A. Hogg, "A Social Identity Theory of Leadership," 186.

²⁵⁵ Michael A. Hogg and Barbara A. Mullin, "Joining Groups to Reduce Uncertainty: Subjective Uncertainty Reduction and Group Identification," in *Social Identity and Social Cognition*, ed. Dominic Abrams and Michael A. Hogg (Oxford: Blackwell, 1999), 249; see Henri Tajfel and John Turner, "An Integrative Theory of Intergroup Conflict," in *The Social Psychology of Intergroup Relations*, ed. William G. Austin and Stephen Worchel (Monterey, CA: Brooks/Cole, 1979), 33–47.

²⁵⁶ See John C. Turner, "Social Categorization and the Self Concept: A Social Cognitive Theory of Group Behaviour," in *Advances in Group Processes*, vol. 2, ed. Edward Lawler (Greenwich, CT: JAI Press, 1985), 77–122.

Some consider these ideas to be distinct, but Hogg and Terry emphasize they are part of an inclusive social identity perspective.²⁵⁷ Tajfel first introduced the concept of social identity to understand how individuals view the world through the concept of groups, and how people view their own identity through the lens of group membership.²⁵⁸

Turner's self-categorization theory, which is closely tied to social identity, focuses on the psychology of group formation.²⁵⁹ The cognitive component of the social identity perspective looks at how people categorize themselves and others into ingroups based upon observed characteristics. Turner's work on self-categorization theory focused on the cognitive function of social identity rather than evaluative or emotional functions.²⁶⁰ Turner himself admitted that self-categorization theory could also be called "the social identity theory of the group."²⁶¹ In this categorization process, groups and people depersonalize and define themselves by the prototypical (ideal) characteristics of an ingroup. The cognitive process of the self-categorization theory essentially matches people up with groups based upon perceived characteristics. In this process, the mind accentuates perceived prototypical characteristics of a group to highlight distinctions between groups.²⁶² The theory essentially provides for the mind to highlight and exaggerate similar and distinct characteristics as it processes relationships and associations situationally.²⁶³ Self-categorization theory suggests that people will willingly assimilate towards the

²⁵⁷ Michael A. Hogg and Deborah J. Terry, "Social Identity and Self-Categorization Processes in Organizational Contexts," *Academy of Management Review* 25, no. 1 (January 2000): 123; Michael A. Hogg and Craig McGarty, "Self-Categorization and Social Identity," in *Social Identity Theory: Constructive and Critical Advances*, ed. Dominic Abrams and Michael A. Hogg (New York: Springer-Verlag, 1990), 11.

²⁵⁸ Henri Tajfel, "Introduction," in *Social Identity and Intergroup Relations*, ed. Henri Tajfel (Cambridge, MA: Cambridge University Press, 1982), 2–3.

²⁵⁹ Turner, "Social Categorization and the Self Concept," 78.

²⁶⁰ Hogg and Mullin, "Joining Groups to Reduce Uncertainty," 250.

²⁶¹ John C. Turner, "Preface," in *Rediscovering the Social Group: A Self-Categorization Theory*, ed. John C. Turner et al. (New York: Basil Blackwell, 1987), ix.

²⁶² Penelope J. Oakes, S. Alexander Haslam, and Katherine J. Reynolds, "Social Categorization and Social Context: Is Stereotype Change a Matter of Information or of Meaning?" in *Social Identity and Social Cognition*, ed. Dominic Abrams and Michael A. Hogg (Oxford: Blackwell, 1999), 60.

²⁶³ Hogg and McGarty, "Self-Categorization and Social Identity," 12; Michael A. Hogg, Deborah J. Terry, and Katherine M. White, "A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory," *Social Psychology Quarterly* 58, no.4 (December 1995): 261.

prototypical group ideal in both internal thoughts and external behaviors, particularly so if saliency is high.²⁶⁴ This is known as the metacontrast principle. The prototype—the individual who most strongly reflects the group ideal—will reflect “beliefs, attitudes, feelings, and behaviors that optimally minimize ingroup differences and maximize intergroup differences...”²⁶⁵ Those prototypical characteristics are situationally contextual and constantly evolving; thus, prototype models are broad characterizations of the group’s ideal in context, with a comparison to the outgroup often driving those characterizations.²⁶⁶ In the continually-evolving cognitive process, people will recall their understanding of group prototypes when categorizing people. Tajfel described social groups as “processes,” not static organisms.²⁶⁷

Group saliency may be the most important element for understanding the importance of a group association or one’s attraction to a group prototype. Saliency refers to the importance of a group to one’s identity in a particular context.²⁶⁸ Saliency is also tied to the fit and accessibility of a group’s characteristics when people use cognitive processes to categorize themselves or others into perceived groups.²⁶⁹ The more salient the group, the more likely the group’s norms will affect personal behavior.²⁷⁰ Again, these categorization processes constantly evolve; group saliency and existence “is a complex sequence of appearances and disappearances, of looming large and vanishing into thin air.”²⁷¹

²⁶⁴ Deborah J. Terry, Michael A. Hogg, and Julie M. Duck, “Group Membership, Social Identity, and Attitudes,” in *Social Identity and Social Cognition*, ed. Dominic Abrams and Michael A. Hogg (Oxford: Blackwell, 1999), 283–84.

²⁶⁵ Hogg and Terry, “Social Identity and Self-Categorization Processes in Organizational Contexts,” 123; Terry, Hogg, and Duck, “Group Membership, Social Identity, and Attitudes,” 284.

²⁶⁶ Hogg, Terry, and White, “A Tale of Two Theories,” 261.

²⁶⁷ Henri Tajfel, “Instrumentality, Identity, and Social Comparisons,” in *Social Identity and Intergroup Relations*, ed. Henri Tajfel (Cambridge, MA: Cambridge University Press, 1982), 485.

²⁶⁸ Terry, Hogg, and Duck, “Group Membership, Social Identity, and Attitudes,” 284.

²⁶⁹ Hogg & Reid, “Social Identity, Self-Categorization, and the Communication of Group Norms,” 12; see also Terry, Hogg, and Duck, 287–88.

²⁷⁰ Terry, Hogg, and Duck, 285.

²⁷¹ Tajfel, “Instrumentality, Identity, and Social Comparisons,” 485.

Leaders have important roles in social groups. From the social identity perspective, leaders are part of a social group system, bound together with followers in the group system.²⁷² The cognitive processes of group members play a role in determining leaders, including their use of self-categorization and depersonalization.²⁷³ Leaders rise based on the perceptions and categorizations of the followers.²⁷⁴ These activities compel individuals to categorize people as leaders based on ingroup-consensual characteristics.²⁷⁵ Despite common myths, the charisma of a leader is not as important as the overlap of the leader's characteristics with the characteristics of the ingroup's prototypical ideal.²⁷⁶ Instead, group members determine the prototypical ideal in a consensual manner; one individual does not solely determine a prototype for a larger group.²⁷⁷ If a position-based leader attempts to establish a social group's prototype inconsistently with the ingroup's understandings of the prototype, the group may reject that individual's attempts. That ingroup consensus also serves to reduce uncertainty, for it is the centralized basis of the group's understanding of what makes the group distinct or valuable.²⁷⁸ It is important to note that these processes occur rapidly and almost subconsciously based on situational factors.²⁷⁹

Hogg argues that true leadership is a byproduct of group dynamics: “[l]eadership is about how some individuals or cliques have disproportionate power and influence to set agenda define identity, and mobilize people to achieve collective goals.”²⁸⁰ Leaders use influence to affect group attitudes and behaviors, or the direction of the group's

²⁷² Hogg, “A Social Identity Theory of Leadership,” 186.

²⁷³ Hogg, 186–88; Hogg & Reid, “Social Identity, Self-Categorization, and the Communication of Group Norms,” 10–11.

²⁷⁴ Hogg, 188, 191.

²⁷⁵ Hogg, 189–91; Hogg & Reid, “Social Identity, Self-Categorization, and the Communication of Group Norms,” 11.

²⁷⁶ Hogg, “A Social Identity Theory of Leadership,” 186, 192.

²⁷⁷ Hogg, 191; Hogg, Van Knippenberg, and Rast, “Intergroup Leadership in Organizations,” 236.

²⁷⁸ Hogg, “A Social Identity Theory of Leadership,” 187–88, 193–94.

²⁷⁹ Hogg, 188.

²⁸⁰ Hogg, 188.

trajectory.²⁸¹ Leaders, if they embody the group prototype, can do this according to the social identity perspective because they have the consensual authority of the ingroup's members.²⁸² Implicit in this analysis is the understanding that leadership and power are distinct elements. The person who embodies the group prototype can influence group behavior, and the leader embodying that prototype can use the power of the prototype to influence and affect group change, to even include altering the group's vision of the prototype.²⁸³ Context is king here, and the group's interpretation of the prototype will constantly shift based on the situation. For example, in some circumstances, a group may expect its prototype to be silent and contemplative, while in other situations the prototype may need to be assertive.

The person who most strongly represents the vision of a group prototype attracts group members to them. So long as the group is salient, this attraction will generally take hold over other considerations like personal relationships.²⁸⁴ This hypothesis stems from the understanding that ingroup members prefer to be more like their ingroup prototype, or at least more consistent with ingroup members rather than outgroup members.²⁸⁵ People in an ingroup who consider themselves to be less like a prototype than others tend to make more changes to mirror the prototype.²⁸⁶ The more salient the group identification, the stronger the desire to mirror the prototype. People do this because the prototype serves as the iconoclastic figure to compare the ingroup in a positive light to other outgroups.²⁸⁷ This does not mean that people act like lemmings and conform to group stereotypes just to garner acceptance. Rather, the prototypical characteristics at play are constantly evolving

²⁸¹ Hogg, 188.

²⁸² Hogg, 188–89.

²⁸³ Hogg, 191; Hogg & Reid, "Social Identity, Self-Categorization, and the Communication of Group Norms," 13.

²⁸⁴ Hogg, 195.

²⁸⁵ Hogg, 187; Terry, Hogg, and Duck, "Group Membership, Social Identity, and Attitudes," 284.

²⁸⁶ See Rast et al., "Leadership Under Uncertainty," 646–47; see also Hogg, "A Social Identity Theory of Leadership," 189.

²⁸⁷ Rast et al., "Leadership Under Uncertainty," 646–47; Terry, Hogg, and Duck, "Group Membership, Social Identity, and Attitudes," 301.

and are based on salient considerations. If one's identity is a continuum wherein a person derives his or her identity from either totally interpersonal relationships on one end of the spectrum to intergroup associations on the other extreme, according to the social identity perspective one's self-identity is constantly in flux somewhere on that continuum; the extent of one's group-derived identity depends largely on a group's saliency.²⁸⁸ People process information individually, but their analyses can be influenced based on group norms.²⁸⁹ Ingroup members will tend to view leaders as those who most strongly exemplify those characteristics based on context. In another scenario, an ingroup may view different characteristics as the most salient, thus redefining the prototype based on the context of the moment. Group members regulate themselves based at least in part on group norms, especially when group saliency is high.²⁹⁰ Group saliency will most likely be highest when a person or groups perceive threats to a group's distinctiveness, sustainability, stability or image.²⁹¹

In the social identity perspective, the Bush Administration's effort to use the prevention narrative was an attempt to use social creativity to reframe the ingroup narrative, to increase group saliency around the government protector role, and to improve group value. Social creativity is a term used within the social identity perspective to describe efforts by a social group to redefine a salient narrative.²⁹² There are several social groups involved in this case study, but to some extent they all fit within the superordinate social group of government security and intelligence professionals. Each official, from the President of the United States at the top of the group down to individuals who leaked information to the media, fit into this overarching group. In this case, after the attacks of September 11, 2001, leadership within the executive branch quickly sought to redefine the

²⁸⁸ Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 34–35; Oakes, Haslam, and Reynolds, "Social Categorization and Social Context," 57.

²⁸⁹ See Oakes, Haslam, and Reynolds, 58–60.

²⁹⁰ Bertjan Doosje, Naomi Ellemers, and Russell Spears, "Commitment and Intergroup Behaviour," in *Social Identity*, ed. Naomi Ellemers, Russell Spears, and Bertjan Doosje (Oxford: Blackwell, 1999), 85–86.

²⁹¹ Doosje, Ellemers, and Spears, 92.

²⁹² David Brannan, Kristin Darken, and Anders Strindberg, *A Practitioner's Way Forward: Terrorism Analysis* (Salinas, CA: Agile Press, 2014), 59.

group narrative to alter norms within the security and intelligence apparatus of the government to assert “never again.” The overriding preoccupation of every member of this social group, according to its leadership, was that another terrorist attack was inexcusable, and all other considerations were necessarily secondary. Using the social identity lens of analysis, this case study serves as an example of social creativity in demonstrating how the narrative changed after the terrorist attacks. Whether intentional or merely perceived as such, the prevention narrative that arose after 9/11 was an effort at social creativity for redefining the battle moving forward: by “never letting it happen again,” the narrative created an absolutist battle of good versus evil that the protectors must win. As evidenced below, the motivations for this narrative came from multiple sources, both internal and external to the executive. With the distinction between coercive positional power and influential leadership in mind, this study also demonstrates the dangers of radical normative shifts without necessary consensus building.

B. SOCIAL GROUPS AND THE PREVENTION NARRATIVE

Group members in large organizations tend to find more saliency in closer, more direct subgroups rather than larger, superordinate structures like large bureaucratic organizations.²⁹³ Being more closely aligned with their subordinate ingroup, people are only intrinsically motivated by the superordinate group’s goals when they align with the goals of the salient subgroup, with the superordinate viewed as a potential outgroup during times of misalignment.²⁹⁴ This brings into question the potential distinctions between leadership or influence of the president or vice president compared to raw coercive power. Leadership “is not a coercive process in which power is exercised over others”; rather, leadership is “a process of influence that enlists and mobilizes the involvement of others in the attainment of collective goals.”²⁹⁵

²⁹³ Naomi Ellemers, Dick De Gilder, and S. Alexander Haslam, “Motivating Individuals and Groups at Work: A Social Identity Perspective on Leadership and Group Performance,” *Academy of Management Review* 29, no. 3 (July 2004): 462–64.

²⁹⁴ Ellemers, De Gilder, and Haslam, 465–66.

²⁹⁵ Hogg, “A Social Identity Theory of Leadership,” 194.

By virtue of his elected position, President Bush served as the patron of the executive branch after 9/11. The roles of the president and vice president are interesting and somewhat difficult to pinpoint within this case study. While not directly involved in many of the decisions referenced in this case study, Goldsmith argues that President Bush was the metaphorical invisible hand driving all decisions based on the need to never “let this happen again.”²⁹⁶ The president’s intentions served as the impetus and one of the strongest factors internal to the executive branch in fostering the prevention narrative. The day after the 9/11 attacks, while at a National Security Council meeting, the president took it upon himself to set a standard. It was there that President Bush warned Attorney General Ashcroft, who himself had been a stark detractor of perceived government abuses in the past, to never let something like this happen again.²⁹⁷ The edict from President Bush became the marching orders upon which the IC would focus from there on out. Ashcroft’s response was to warn his subordinates that no plot or lead could go unchecked.²⁹⁸ The overriding concern of the President and, thereafter Ashcroft, penetrated the entirety of the administration.²⁹⁹

In November 2001, Vice President Cheney ordered the Central Intelligence Agency to treat all threats as highly credible regardless of the analytical conclusions.³⁰⁰ Cheney’s order was dubbed the One Percent Doctrine: if there was even a one percent chance of a legitimate lead, officials must work the lead until proven otherwise.³⁰¹ Oftentimes, FBI agents were unaware as to how the NSA came up with leads that it provided to them, but they frequently called these tips “Pizza Hut leads” because they were more likely to lead to a pizza delivery driver rather than a suspected terrorist.³⁰² FBI agents complained that

²⁹⁶ Goldsmith, *The Terror Presidency*, 74, 213.

²⁹⁷ Ashcroft, *Never Again*, 130.

²⁹⁸ Lichtblau, *Bush’s Law*, 4–5.

²⁹⁹ Goldsmith, *The Terror Presidency*, 74–75.

³⁰⁰ Ron Suskind, *The One Percent Doctrine: Deep Inside America’s Pursuit of Its Enemies Since 9/11* (New York: Simon & Schuster, 2006), 62.

³⁰¹ Suskind, 62.

³⁰² Lichtblau, *Bush’s Law*, 160.

they had already addressed many of these leads before receiving them from the NSA.³⁰³ Yet, for all the focus on running down every lead, questions of efficacy still arose. According to audits pursued by FBI General Counsel Valerie Caproni, 1.2 percent of leads generated by Stellarwind from 2001 to 2004 were useful, with usefulness defined as “those that made a substantive contribution to identifying a terrorist, deporting a suspected terrorist, or identifying a potential confidential informant.”³⁰⁴ From March 2004 through January 2006, the review in a second study deemed zero of the leads useful.³⁰⁵ In later reviewing the bulk metadata collection program, the Privacy and Civil Liberties Oversight Board found that not one lead from the program led to any “concrete difference in the outcome of a counterterrorism investigation.”³⁰⁶ Of twelve cases believed to obtain some value from the NSA program, the FBI already had access to that information in each case.³⁰⁷ The Board recommended the termination of the program.³⁰⁸ This recommendation may have contributed to the Intelligence Community conceding to the passage of the USA Freedom Act in 2015 as the first major legislation on surveillance authorities after the Snowden leaks.³⁰⁹ Multiple court cases in recent years suggest that elements of Stellarwind were either statutory violations of the PATRIOT Act or

³⁰³ DOJ IG Report, 68.

³⁰⁴ Savage, *Power Wars*, 196; DOJ IG Report, 302–3.

³⁰⁵ Savage, 196; DOJ IG Report, 305.

³⁰⁶ David Medine et al., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (Washington, DC: Privacy and Civil Liberties Oversight Board, January 3, 2014), 11.

³⁰⁷ Medine et al., 145–46.

³⁰⁸ Medine et al., 16–17.

³⁰⁹ Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline of Monitoring (USA Freedom Act) of 2015, Public Law 114-23, 114th Cong., 1st sess. (June 2, 2015): 268–313; David Medine and Patricia Walde, “Is the Freedom Act More Effective Than the PATRIOT Act?” *Newsweek*, December 27, 2015, <http://www.newsweek.com/freedom-act-more-effective-patriot-act-409127>.

unconstitutional.³¹⁰ There may be entirely appropriate and legitimate reasons for these numbers, but such evidence should at least raise a question: to what extent were these decisions to use resources in this manner predicated on norms influenced by group members pushing the prevention narrative?

To Goldsmith, these responses by the President and Vice President were obvious reactions to the events of 9/11.³¹¹ Bradford Berenson, an aide to Alberto Gonzales in the White House Counsel's Office, described running roughshod over some people's liberties and rights as "regrettable," but "inevitable."³¹² In the memorandum arguing for the legality of Stellarwind, John Yoo found that in light of the 9/11 attacks and the conflict at hand, "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of civil liberties."³¹³ Years later, after the PRISM mass electronic surveillance program began under the authorities given to the executive under the Protect America Act, President Bush told then-Director of the NSA Keith Alexander "to take these authorities and defend America."³¹⁴

These are examples of a social group allowing the prevention narrative to take hold and affect cultural norms. Whereas before 9/11 government security officials arguably attempted to balance security and liberty, after the terrorist attacks, many government actors swept away any balance of security and liberty in favor of an effort to ensure total security moving forward. This came from multiple sources both internal and external to

³¹⁰ See *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), vacated and remanded, 800 F. 3d 559 (D.C. Cir. 2015); see also *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) affirmed in part, vacated in part, remanded, 785 F.3d 787 (2d Cir. 2015); additionally, in light of the Supreme Court's recent decision in *Carpenter v. United States* that required a warrant for the collection of historical cell site location information for a period longer than seven days, some commentators suggest the program might be unconstitutional if it were still in effect today (see *Carpenter v. United States*, 138 S. Ct. 2206 (2018); David Kris, "Carpenter's Implications for Foreign Intelligence Surveillance," *Lawfare* (blog), June 24, 2018, <https://www.lawfareblog.com/carpenters-implications-foreign-intelligence-surveillance>).

³¹¹ Goldsmith, *The Terror Presidency*, 75.

³¹² "Less Safe, Less Free: The 'Preventive Paradigm' and the War on Terror," C-SPAN, video, 1:55, September 25, 2007, <https://www.c-span.org/video/?201188-1/less-safe-free>.

³¹³ James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, <https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>.

³¹⁴ Hayden, *Playing to the Edge*, 410.

those actors' social groups. Examples of internal sources included those that originally came from edicts of the president and the vice president, so it is worthwhile to analyze the role of these men in this described social group of government intelligence and security professionals. The president relied on the coercive positional power of the office of the president to seek changes in IC cultural norms rather than relying on influential leadership based on social dynamics. This may have contributed to some of the difficulties that followed, particularly as they relate to intergroup conflict and leakers.

People in positions of power must always be wary to not abuse those positions, for that may sever a leader's influence in patron/client relationships.³¹⁵ President Bush and Vice President Cheney may have been prototypical leaders for many executive branch officials, including the aforementioned War Council, because they may have shared an affinity for prevention at all costs; but the distinction between political appointees who shared the president's agenda and career civil servants may be relevant here. Many civil servants steeped in cultures of legal compliance may well have believed that fostering the prevention narrative to extremes was a bridge too far. Since those times of turmoil after the Church Committee, agencies such as the FBI, the CIA, and the NSA have learned many lessons from the past outcry over the surveillance activities exposed through news reporting and investigations.³¹⁶ Based on the public record, it is fair to say that federal intelligence agencies—notably the FBI, the CIA, and the NSA—have created significant cultures of compliance.³¹⁷ In that sense, President Bush and Vice President Cheney may have begun to separate themselves from the prototypical ideal of many government employees. However, even if government employees questioned their influence as leaders, as the elected officials in charge of the executive branch President Bush and Vice President Cheney served as patrons of the “government protectors” superordinate structure; these

³¹⁵ See Brannan, Darken, and Strindberg, *A Practitioner's Way Forward*, 74–76.

³¹⁶ See Church Committee, *Final Report*.

³¹⁷ See *The Lawfare Podcast*, Episode 172, “The Role of Transparency in Intelligence Programs,” produced by the Brookings Institution, May 28, 2016, <https://www.lawfareblog.com/lawfare-podcast-role-transparency-intelligence-programs>; see also Timothy Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (Washington, DC: Brookings Institution Press, 2017), 7, 41, 77; Hayden, *Playing to the Edge*, 73–74.

men clearly held coercive power over the executive branch, even if their social influence waned.³¹⁸ Members of these groups could easily construe demands that something like 9/11 never happen again as a negative honor challenge against the superordinate group, which in effect questions the social group's past efficiency.³¹⁹ Depending on how these social groups view their patrons as leaders, these demands could trigger numerous responses by intelligence professionals in the government.

The president was not the only source of the prevention narrative's influence. In other halls of Washington, D.C., even before the president's edict, people inside the executive branch already embraced the prevention narrative as officials held discussions about how to increase security capabilities. Those conversations started on September 11, 2001, when leaders of several executive branch law enforcement agencies met within the confines of the Department of Justice as panic gripped the nation. As the horror of the day unfolded, conversations among those leaders quickly escalated to discuss tools to engage in mass surveillance or interrogations based on race or religion. Hours after the attack, James Ziglar, Commissioner of the Immigration and Naturalization Services (INS), sat in the Strategic Information Operation Center after the attacks on 9/11. He heard leaders of other executive agencies discussing what he believed to be a discourse on general warrants against Muslim populations in the United States.³²⁰ He raised concerns to the leaders in the room, including Attorney General Ashcroft's Chief of Staff David Ayres, but the faces around the table only looked at him questioningly.³²¹ Others in the room either viewed him oddly or dismissed his concerns.³²² He immediately considered himself to be a deviant challenging ingroup perspectives. Ziglar eventually retired from INS, but not after several contentious confrontations with the attorney general. "You were either for national

³¹⁸ See Brannan, Darken, and Strindberg, *A Practitioner's Way Forward*, 74–76.

³¹⁹ Brannan, Darken, and Strindberg incorporate honor challenges into the social identity perspective through their research on analytical markers in Mediterranean-based social groups. Their noted analytical markers include the patron/client relationship, a paradigm regarding honor and shame within social groups, the process of issuing challenges and responses within groups, and an application of the "limited goods" (see Brannan, Darken, and Strindberg, 67–82).

³²⁰ Lichtblau, *Bush's Law*, 5–7.

³²¹ Lichtblau, 5–7.

³²² Lichtblau, 5–7.

security, or you were against it,” Bo Cooper, General Counsel for INS, would later say.³²³ This false dichotomy stemmed from an over-embrace of the prevention narrative and an imbalance of group norms as a result of social groups creatively reestablishing norms to fit a perceived deficit.

The aggressive rhetoric referenced to this point is also important from a social identity perspective. Czarniawska and Joerges note that conversation is a critical element of change, in that it serves as a method for disseminating concepts of change.³²⁴ Change in organizations like those seen after 9/11 do not happen in a vacuum; rather, discourse propels group change.³²⁵ Group members alter discourse through conversations and the written word, as they use these tools to amend previous group narratives.³²⁶ Bakhtin notes that groups constantly reinterpret narratives in light of changing events.³²⁷ Language and communication are crucial for establishing the social construction surrounding new initiatives; the narratives shaped by groups and their leaders will often dictate how people address problems as they arise.³²⁸

The use of narrative-altering discourse here can have potential ramifications on communications within social groups. The categorization of activities as either “a threat” or “an opportunity” will influence how others respond to an activity.³²⁹ The same idea applies to how leaders use language to root new initiatives in either familiar or new

³²³ Lichtblau, 61.

³²⁴ Barbara Czarniawska and Bernward Joerges, “Travel of Idea,” in *Translating Organizational Change*, ed. Barbara Czarniawska and Guje Sevón (Berlin: Walter de Gruyter & Co., 1996), 13–48, quoted in Donald L. Anderson, “What You’ll Say Is...: Represented Voice in Organizational Change Discourse,” *Journal of Organizational Change Management* 18, no. 1 (2005): 64.

³²⁵ Anderson, “What You’ll Say Is...,” 64.

³²⁶ Anderson, 65.

³²⁷ M.M. Bakhtin, “Toward a Methodology for the Human Sciences,” in *Speech Genres and Other Late Essays*, ed. Caryl Emerson and Michael Holquist, trans. Vern W. McGee (Austin: University of Texas Press, 1986), 170.

³²⁸ Liselore A. Havermans, Anne Keegan, and Deanne N. Den Hartog, “Choosing Your Words Carefully: Leaders’ Narratives of Complex Emergent Problem Resolution,” *International Journal of Project Management* 33, no. 5 (July 2015): 974.

³²⁹ Jane E. Dutton and Susan E. Jackson, “Categorizing Strategic Issues: Links to Organizational Action,” *Academy of Management Review* 12, no. 1 (January 1987): 77.

terrain.³³⁰ Leaders continually use narratives to frame how they, their organization, and the organization's members fit into new initiatives.³³¹ Leaders shape narratives through how they set the use of language and frames in clear, systematic terms.³³² Leaders take a primary role in shaping narratives, and their ability to do so is directly tied to their level of social influence.³³³ Language creating a false dichotomy such as “you are either for national security or against it” all too easily establishes threats rather than positive opportunities for group members.

For reasons both internal and external, the potential for the discursive framework of the prevention narrative to alter analysis within social groups is significant. One example from this case study is that of Attorney General John Ashcroft who, when he was a U.S. senator in 1998, vehemently opposed a government-favored resolution to encryption, stating “there has been an insistence that we turn over the keys to our individual privacy to the federal government, but there has been no talk of safeguards or privacy.”³³⁴ Speaking against the “trust the protectors” narrative that would be common from Bush Administration officials after the leak of Stellarwind to the public, he said, “[a]pparently, innocent citizens are expected to trust the bureaucracy not to abuse them...In no way [did the founding fathers] favor the notion that a key to every home, diary, bank account, medical record, business plan, or investment should be provided to the federal government for use without the individual's knowledge.”³³⁵

After 9/11, and after the president's edict, many of those concerns appeared to vanish based on concerns of preventing another attack. Ashcroft described the attacks as being just as critical as a heart attack to a hospital patient, even going so far as to question the likelihood of the country's existential survival after the attack.³³⁶ In Ashcroft's eyes,

³³⁰ Havermans, Keegan, and Den Hartog, “Choosing Your Words Carefully,” 974.

³³¹ See Havermans, Keegan, and Den Hartog, 974–76.

³³² Havermans, Keegan, and Den Hartog, 975.

³³³ Havermans, Keegan, and Den Hartog, 975–76.

³³⁴ Lichtblau, *Bush's Law*, 56–57.

³³⁵ Lichtblau, 56–57.

³³⁶ Lichtblau, 57.

even prosecution of terrorist suspects—and the significant incarceration and prevention that coincides with successful prosecution—came second to prevention at all costs. “Prosecution cannot be our top priority,” he told FBI Director Robert Mueller, “if we lose the ability to prosecute, that’s fine, but we have to prevent the next attack. Prevention must be our top priority.”³³⁷ In a similar example, NSA Director Hayden later asserted that during the conflict between James Comey, the Department of Justice, and the White House, he offered to continue Stellarwind even in the event that the program did not get legal authorization.³³⁸ This decision had the potential to put him and other policymakers in legal jeopardy. He based his justification in part on the then-recent Madrid bombings.³³⁹ White House Chief of Staff Andrew Card also explicitly referenced the Madrid bombings as justification for the executive’s efforts while briefing congressional leadership on Stellarwind.³⁴⁰

An individual derives his identity from his self-image.³⁴¹ In other words, it is the individual’s perception of him or herself that comprises that person’s identity. The social identity perspective argues that much of an individual’s self-identity stems from the individual’s perception of the value of his or her group associations. When the prevention narrative highlights certain group perceptions and attitudes, it has the effect of driving the salient factors of social identity. What drives the government protectors’ ingroup prevention narrative is not only what the prototypical leader dictates; norm-influencing narratives can also arise based on internal concerns from the collective group membership or based on perceived outward attacks on the ingroup. As demonstrated below, both internal and perceived external attacks about what the ingroup did (or failed to do) to prevent 9/11 from occurring further ignited social groups to foster the ingroup prevention narrative. The prevention narrative accentuated the saliency of the government protector

³³⁷ Lichtblau, 82.

³³⁸ Hayden, *Playing to the Edge*, 87.

³³⁹ Hayden, 88.

³⁴⁰ Hayden, 88.

³⁴¹ See Hogg, Terry, and White, “A Tale of Two Theories,” 259–60.

social identity within the superordinate executive branch and many subgroups in the intelligence and security arena.

From the internal member perspective, there is ample anecdotal information to suggest that certain groups clung to the prevention narrative because of the perceived failures of the ingroup and concerns that another failure would be detrimental to the group's value. This speaks to the need for the ingroup to establish positive evaluative and emotional components to the group's identity. From this perspective, the prevention narrative should be understood as the group's own negative evaluation of itself after the Twin Towers fell. A sense of blame for the attacks may drive a negative internal evaluation of the group and its own sense of efficacy. Another attack on the scale of 9/11 would have been detrimental, not only to the country generally or the people affected, but also to the intelligence and security ingroup and the evaluation of its own identity. As a result, the strong, overriding prevention narrative that formed in multiple places simultaneously—both from the leader of the group and throughout its ranks—demonstrated the group's need to creatively reframe the narrative, the group's priorities, and from where the group drew its value. Before 9/11, the calculus of security considerations was significantly different. For instance, the decision not to carpet bomb Afghanistan to eliminate Osama Bin Laden before 9/11 because of concerns over collateral damage is an example of how the analysis was different.³⁴² After 9/11, many government officials believed that prevention must take priority at all costs.

A belief that the public would not accept another attack compelled much of the perception driving the narrative. Psychologically, this was the articulation of a perceived potential threat to the ingroup from the amorphous public citizenry outgroup. Jack Goldsmith saw dual concerns in the Bush Administration's actions, both of a fear of "doing too much," and "fear of not doing enough to stop the next attack."³⁴³ Goldsmith asserted that "playing it safe" was no longer feasible after 9/11, thus risking "reputation, fortune,

³⁴² In early 1999, the Clinton Administration denied a missile strike that the CIA sought intending to kill Osama bin Laden because of questionable reliability of sourcing and the potential for significant collateral damage (*The 9/11 Commission Report*, 130–31).

³⁴³ Goldsmith, *The Terror Presidency*, 12.

and perhaps liberty” was a natural response to overcorrecting for cautious pre-9/11 policies and lawyering.³⁴⁴ Goldsmith openly acknowledged that the “fear” of allowing another attack drove aggressive decisions even in legal rulings from the OLC.³⁴⁵ He found that “[i]t was thus not easy for the men under pressure in the summer of 2002 to critically analyze John Yoo’s legal opinion.”³⁴⁶

Perceived external threats to the ingroup fostered the prevention narrative. In their writings, both Hayden and Goldsmith point to external commission findings (the Congressional Joint Inquiry Commission and the 9/11 Commission, respectively) as evidence of the view within the executive that future failures would be unacceptable.³⁴⁷ The fear of failing to err on the side of absolute security was obvious. Stuart Levey in the Department of Justice described detainee policy as “not up for debate,” and some were concerned of “catastrophic consequences” that should befall the administration were they to release someone who then committed an attack.³⁴⁸ The same concerns permeated Congress after 9/11. The concerns of either not giving the government the tools it needs or appearing weak were palpable on Capitol Hill, where even normal allies of civil liberties groups like the ACLU planned to vote for the PATRIOT Act.³⁴⁹ Many congressional members and staffers had not read significant portions of the wide-ranging bill.³⁵⁰ Reports suggest that congressional leaders in charge of writing the legislation sought more time from the administration to work on a solution, only to receive rebukes that they would be to blame if there were further attacks.³⁵¹ Each of these social groups could arguably trace back their actions to certain effects of the prevention narrative.

³⁴⁴ Goldsmith, 69.

³⁴⁵ Goldsmith, 11–12.

³⁴⁶ Goldsmith, 169.

³⁴⁷ Hayden, *Playing to the Edge*, 66–67; Goldsmith, 74–75.

³⁴⁸ Lichtblau, *Bush’s Law*, 46–47.

³⁴⁹ Edgar, *Beyond Snowden*, 18.

³⁵⁰ Edgar, 16.

³⁵¹ Edgar, 19.

C. THE WAR COUNCIL AND CONFLICT WITH OTHER SOCIAL GROUPS

This case study demonstrates the importance of social groups within organizations. While the superordinate social group involved here is defined as security and intelligence professionals within the federal government, smaller groups within that group conflicted significantly over the history of the Stellarwind program. To the extent that certain subgroups embraced the prevention narrative as an ingroup norm, subgroups conflicted with each other depending on how salient security became to its members, particularly as security related to other functions like internal debates and processes or legal concerns. However, single issues are a misnomer; multiple focuses can drive individuals and groups.³⁵²

A critical social group for understanding the intricacies of this case study is the aforementioned War Council, the informal body of senior level officials who sought to preempt and control legal and policy decisions related to counterterrorism. The War Council took significant efforts to control the flow of information and stifle discussion, which had the ulterior benefit of mitigating dissent or opposing viewpoints within a given debate.³⁵³ The ingroup narrative of the War Council focused on (1) the prevention narrative, and (2) an additional motive of reestablishing executive power to its perceived zenith. Other subgroups found the overarching “government protectors” ingroup less salient as the War Council took unusual measures to define the executive branch’s prototype, perhaps resulting in reduced social cohesion among the relevant subgroups. The War Council’s use of raw, coercive power rather than social influence to change cultural norms further accentuated the separation of subgroups, treating other executive branch members as clients for whom they had not earned patronage.

For a group of attorneys deeply engaged in both policy and legal discussions, David Addington arguably served as the prototypical leader for the War Council. It is clear from public accounts that Addington served as the de facto leader of the War Council, even if

³⁵² C. Marlene Fiol, Michael G. Pratt, and Edward J. O’Connor, “Managing Intractable Identity Conflicts,” *Academy of Management Review* 34, no. 1 (January 2009): 34.

³⁵³ Goldsmith, *The Terror Presidency*, 22, 167.

White House General Counsel Alberto Gonzales acted as the mediator and controller of group activities. A prototype serves as an individual with the “fuzzy sets...of attributes” that define a group.³⁵⁴ Prototypes often demonstrate the metacontrast principle of providing the clearest distinction for an ingroup of the group’s appropriate norms compared to an outgroup.³⁵⁵ By all accounts, Addington filled this role by focusing almost entirely on prevention and presidential powers.³⁵⁶ Moreover, he was perhaps the most experienced and distinguished attorney in the group. “Addington was known throughout the bureaucracy as the best-informed, savviest, and most conservative lawyer in the administration.”³⁵⁷ John Yoo spoke of Addington as a learned attorney in a highly respectful manner.³⁵⁸ Jack Goldsmith was impressed with his detailed knowledge on minutia not regularly understood by attorneys in such a high stature.³⁵⁹ Addington was known for relishing deep dives into case law and policy.³⁶⁰ Addington was almost always involved in national security meetings in the White House, despite the historically limited role of the office of the vice president in policymaking.³⁶¹ Alberto Gonzales often deferred to Addington because Gonzales’ background was not in matters of executive power or national security, but rather corporate law.³⁶² Addington’s background exemplified an experienced attorney in the federal government and national security. He had extensive experience in Washington, D.C., bureaucracy dating back to his time serving as a congressional staffer when the vice president served in Congress. Addington had prior experience as an attorney for the CIA and worked in the Reagan Administration. He served

³⁵⁴ Michael A. Hogg et al., “The Social Identity Perspective: Intergroup Relations, Self-Conception, and Small Groups,” *Small Group Research* 35, no. 3 (June 2004): 253; Hogg, Terry, and White, “A Tale of Two Theories,” 261.

³⁵⁵ Hogg, “A Social Identity Theory of Leadership,” 193.

³⁵⁶ See Goldsmith, *The Terror Presidency*, 86.

³⁵⁷ Goldsmith, 27.

³⁵⁸ Goldsmith, 27.

³⁵⁹ Goldsmith, 28.

³⁶⁰ Goldsmith, 28.

³⁶¹ Goldsmith, 76.

³⁶² Goldsmith, 76.

as general counsel for the Department of Defense under then-Secretary Cheney, and also as chief counsel for multiple House committees. Gonzales, in contrast, came to Washington after a career in corporate and Texas state legal matters, intending to be the attorney for a president primarily focused on domestic matters before 9/11.³⁶³

On the one occasion when Jack Goldsmith could recall Addington and Gonzales disagreeing, Addington's view won out with the president.³⁶⁴ In his position as counsel to the vice president, Addington wielded little actual power among members of the War Council; yet, in the War Council he could embody the attributes that best defined the group—smart, experienced, and entirely focused on policies aimed at preventing future attacks. Thus, he held influential power within the War Council.

Perhaps most importantly, many viewed Addington as the channel for the chief executive's authority. Solicitor General Ted Olson described Addington as "Cheney's 'eyes, ears, and voice.'"³⁶⁵ As a corollary, many viewed Addington as speaking with the voice of the vice president and also President Bush.³⁶⁶ On top of a gruff demeanor and significant knowledge base from which to pull, Addington shared the vice president's focus on restoring executive power after Congress put restrictions in place after the abuses of the Watergate era.³⁶⁷ That restoration of executive power was also a call to arms in how war and counterterrorism decisions were made after 9/11. Cheney and Addington explicitly viewed FISA, and the FISC itself, as objects of improper congressional overreach.³⁶⁸ "We're one bomb away," Addington once said of the FISC, "from getting rid of that obnoxious court."³⁶⁹ Addington was a known ideologue who refused to seek compromise with other attorneys. Addington, and by extension the vice president, attacked those who challenged their opinions on many occasions, notably blocking the promotion of Patrick

³⁶³ Goldsmith, 77.

³⁶⁴ Goldsmith, 128.

³⁶⁵ Goldsmith, 77.

³⁶⁶ See Goldsmith, 27, 77–78, 129, 132, 171.

³⁶⁷ Goldsmith, 89, 124.

³⁶⁸ Goldsmith, 181–82.

³⁶⁹ Goldsmith, 181; DOJ IG Report, 204.

Philbin, who aligned himself with James Comey during the dispute surrounding reauthorization of Stellarwind.³⁷⁰ Within that group of policy-oriented attorneys focused so strongly on prevention, Addington embodied the group prototype. Without 9/11, had the Bush Administration focused on domestic activities, the context for Addington's prototypical embodiment never would have come to pass.

As the prototype, Addington set the tone for the War Council's activities and kept the ingroup small. He "had a domineering reputation as the smartest lawyer in any room—and one who wasn't afraid to let the others know it."³⁷¹ In meetings, he pushed others in a manner consistent with a goal of stifling dissent. In situations where Goldsmith brought to the White House's attention that previous OLC opinions were flawed and needed alterations, starting with the issue of the application of the Geneva Conventions to combatant detainees, Addington shouted down Goldsmith. "You cannot question [the president's] decision," he once said.³⁷² In a meeting in the spring of 2004 with Philbin, Goldsmith, and Gonzales regarding a dissatisfactory opinion from the OLC, Addington barked, "[i]f you rule that way, the blood of the hundred thousand people who die in the next attack will be on your hands."³⁷³ Engaging people and groups in this manner is likely to have significant (negative) ramifications. The harsh nature of Addington's communications should be perceived as a negative honor challenge upon distinct groups, prompting potentially unexpected responses. These potential ramifications likely grew as the perception of Addington as a prototype faded outside of the narrow ingroup that he directly influenced. It is unlikely that Addington's behavior could have embodied a prototypical role in many contexts, yet here his aggressive attitude comported with the needs of the overriding ingroup prevention narrative.

With direct access to the president and vice president, the War Council kept its circle tight and tried to confine it to like-minded individuals. For instance, at the time

³⁷⁰ Addington blocked Philbin's promotion to Solicitor General in Bush's second term (Goldsmith, 170).

³⁷¹ Lichtblau, *Bush's Law*, 134.

³⁷² Goldsmith, *The Terror Presidency*, 40.

³⁷³ Goldsmith, 71; DOJ IG Report, 130.

Stellarwind went public, the civil liberties protection officer within the Office of the Director of National Intelligence (ODNI) was unaware of the program, as was the general counsel of the ODNI.³⁷⁴ This reinforced conflict with Attorney General John Ashcroft and the Department of Justice, who the War Council often bypassed to go to a subordinate, John Yoo. The perceived threats to the country largely drove the mindset of the War Council. Goldsmith described the attitude of the War Council and administration officials as follows: “[t]heir want of actionable intelligence combined with their knowledge of what might happen to produce an aggressive, panicked attitude that assumed the worst about threats and embraced a ‘better safe than sorry’ posture toward them.”³⁷⁵ He believed that the Council’s efforts to drive policy were often affected by their continual focus, day after day, on potential threats to the country.³⁷⁶ James Comey called the focus on threats so heightened that it became “an obsession” because of the extreme nature and number of threats.³⁷⁷ Goldsmith also believed that the primary justification for narrow decision-making circles and limiting access to legal decisions was to “control outcomes” and “minimize resistance,” despite the state justification of preventing leaks of sensitive information.³⁷⁸

Like-mindedness was important inside the War Council, and that contributed to conflict with other groups. In setting the standard of pushing for executive authority, Addington spoke of the awesome authorities of the president in wartime: “[w]e’re going to push and push and push until some larger force makes us stop.”³⁷⁹ Yoo also shared Addington’s view of significant constitutional wartime authorities incumbent in the presidency, to the point that Congress could not restrict them by statutes.³⁸⁰ Critics accused

³⁷⁴ Edgar, *Beyond Snowden*, 29, 235, 4n.

³⁷⁵ Goldsmith, 74.

³⁷⁶ See Goldsmith, 71–75.

³⁷⁷ Goldsmith, 72.

³⁷⁸ Goldsmith, 167.

³⁷⁹ Goldsmith, 126.

³⁸⁰ See John Yoo, “The Terrorist Surveillance Program and the Constitution,” *George Mason Law Review* 14, no. 3 (Spring 2007): 565, 596–600.

Yoo of working too closely within the War Council, to the point of claiming he worked directly for the Vice President, Addington, and Gonzales when his chain of command led directly to Ashcroft.³⁸¹ Ashcroft subsequently blocked Yoo's promotion to the head attorney at the OLC because of Ashcroft's suspicions of Gonzales, Yoo, and the War Council.³⁸² Yoo would soon depart the government for a return to academia. Jack Goldsmith was selected to replace Bybee to head the OLC and take Yoo's place on the War Council based on support from Jim Haynes and John Yoo.³⁸³ Gonzales recognized Ashcroft's suspicions of him, and he told Goldsmith during the vetting period that he would need to get Ashcroft's support because a recommendation coming from the War Council would be viewed skeptically.³⁸⁴ When Goldsmith met with Ashcroft, an overriding focus of discussions was to assure that Goldsmith, as the head of OLC, kept Ayres and Ashcroft continually apprised of what was occurring.³⁸⁵

Yet Goldsmith's appointment to lead the OLC and inclusion in the de facto War Council led to conflict within the group of policymakers. For the first time, Goldsmith bucked the group norms for concerns over the legal foundations of various counterterrorism policies. In his writings, Goldsmith highlights the clash of views that regularly took place in national security discussions in the White House, trying to balance the drive for security with concerns over violating the law.³⁸⁶ Of the members of the War Council, Goldsmith was the only one not in government service on September 11, 2001, and he considered himself to be primarily a legal scholar. The saliency of the War Council's norms was not as prescient as his commitment to certain legal standards and the rule of law, as evidenced by Goldsmith's view of the Council's efforts on surveillance: “[a]fter 9/11 [Addington and Cheney] and other top officials in the administration dealt with FISA the way they dealt with other laws they didn't like: they blew through them in secret based

³⁸¹ Goldsmith, *The Terror Presidency*, 24–25.

³⁸² Goldsmith, 24.

³⁸³ Goldsmith, 25–27.

³⁸⁴ Goldsmith, 30.

³⁸⁵ Goldsmith, 30.

³⁸⁶ Goldsmith, 90.

on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations.”³⁸⁷

In response to expressed concerns that certain OLC memoranda needed to be pulled and revised, the White House—and likely the War Council—felt as though Goldsmith “buckled” to public outrage ongoing in certain areas of counterterrorism policy.³⁸⁸ Addington openly mocked Goldsmith, arguing that “[s]ince you’ve withdrawn so many legal opinions that the President and others have been relying on, we need you to go through all of OLC’s opinions and let us know which ones you still stand by.”³⁸⁹ Increasingly, members of the War Council—particularly Addington—shouted down Goldsmith as his tenure in public office reached nine months. The prototype treated the ingroup member like a social deviant for refusing to conform to ingroup norms. Goldsmith instead found like-minded allies outside the White House in the Department of Justice who prioritized rule of law over an excessive form of the prevention narrative. As previously noted, the vast majority of relevant actors in the Department of Justice did not have access to Stellarwind because it was a closed program hidden within the confines of a “special access” program, which was quite unusual for its degree of secrecy.³⁹⁰

This evidence suggests that the War Council’s actions created conflicts with other social groups on multiple fronts. The War Council acted unilaterally and secretively, excluding personnel who would normally be involved in determining and executing critical counterterrorism policies like the Stellarwind surveillance program. Moreover, Addington’s interactions with Goldsmith evidence that, when members of other groups were involved, the War Council’s prototype shouted them down to suggest they were irrelevant. Collectively, this sort of rhetoric combined with these actions demonstrated a hostile environment wherein policymakers discouraged engaging in fruitful discussions on

³⁸⁷ Goldsmith, 181.

³⁸⁸ Goldsmith, 159.

³⁸⁹ Goldsmith, 161.

³⁹⁰ Lichtblau, *Bush’s Law*, 140.

the ramifications of policies. In this case, these actions caused significant isolation of the War Council from other subgroups within the Executive Branch.

Those within the Department that were aware of the program seemed to believe in similar legal norms as Goldsmith. Slowly, over the course of his tenure in the Department of Justice, Goldsmith moved out of the War Council. FBI Director Robert Mueller was among those who joined Goldsmith in a newly salient ingroup of “rule of law” based officials leading up to the incident at the George Washington University Hospital and the subsequent threats to resign. Mueller did not draw patronage lines to the White House; he instead drew on long-recognized norms of FBI independence from the president. He did not defer to presidential decisions on legality and did not look to the War Council for legal ruling. “Your office [OLC] is expert on the law and the President is not,” he once said to Jack Goldsmith.³⁹¹ James Comey and, increasingly, John Ashcroft also aligned themselves with this group focused on rule-of-law interests. Personal relationships had little to do with these alignments, as Comey insists Mueller was never more than a vaguely familiar colleague in whom Comey recognized similar characteristics in how they viewed their duties.³⁹²

At the peak of pressure from this group, President Bush ordered the Stellarwind program to come into compliance with the demands of Mueller, Comey, and the Department of Justice attorneys. The president made this decision while privately discussing the matter with Comey and Mueller, in the wake of unilaterally reauthorizing the program without the legal signoff by the Department of Justice.³⁹³ In that moment, President Bush faced an existential threat to both the superordinate and subgroups of government protectors for whom he served as patron. He faced a threat from the leadership of the Department of Justice and the FBI that they would resign. Such actions would have had resounding ramifications. Massive leadership resignations would have created significant negative values of group association within the Department, thereby

³⁹¹ Goldsmith, *The Terror Presidency*, 79.

³⁹² Comey, *A Higher Loyalty*, 8.

³⁹³ Comey, 96–98.

destabilizing agency morale in an organization already under intense pressure, and risking group cohesion.³⁹⁴ Additionally, with only months until a presidential election, the resignations would likely have spurred a series of questions about why the senior attorneys within the Department of Justice suddenly resigned in unison. The likelihood of glossing over that event would be low, possibly further damaged by others within the Department of Justice who would feel more inclined to talk to reporters to force change by exposing perceived norms violations from within the government.

Confronted by this threat, President Bush's decision to double back on unilaterally authorizing the Stellarwind program was also an example of social change: the president changed course, acting in a manner inconsistent with previous action to stabilize dissent in the ranks. This also required some level of social creativity via an alteration to the prevention narrative, conceding that legal boundaries were a co-equal consideration to security. The changes prompted by that decision had the subsequent effect of strengthening group cohesion by bolstering support within the government protector ranks across all three branches of government, thereby amending the desired group norms and expanding the ranks of potential group members to those concerned with both security and the rule of law.³⁹⁵ In theory, this could have weakened his position with high identifiers—organizational members who strongly attach their social identity to organizational values—like David Addington, who likely attempted to draft an order after the president's meetings with James Comey and Robert Mueller that negated the president's concession.³⁹⁶ Nonetheless, to a strong ingroup identifier, the president as a perceived group prototype had more flexibility to amend ingroup norms and act inconsistently with the previously-

³⁹⁴ In a more recent example, surveys suggest recent leadership turmoil in the FBI also led to damaging morale among the rank and file. See Scott R. Anderson and Benjamin Wittes, "Climate Change is Real at the FBI—and Here is the Data to Prove It," *Lawfare* (blog), July 15, 2018, <https://www.lawfareblog.com/climate-change-real-fbi-and-here-data-prove-it>.

³⁹⁵ The passage of the Protect America Act and FISA Amendments Act are public evidence of majority representative support for executive surveillance efforts (see Protect America Act of 2007, Public Law 110-55, *US Statutes at Large* 121 (2007): 552–57; see also Foreign Intelligence Surveillance Act of 1978 Amendments Act (FISA Amendments Act) of 2008, Public Law 110-261, *US Statutes at Large* 122 (2008): 2436–478, codified at *US Code* 50 (2015), §§ 1801 et seq.).

³⁹⁶ Comey, *A Higher Loyalty*, 99; see Doosje, Ellemers, and Spears, "Commitment and Intergroup Behaviour," 85; see also Terry, Hogg, and Duck, "Group Membership, Social Identity, and Attitudes," 293–95.

established embodiment of prototypical traits.³⁹⁷ Meanwhile, through creatively altering the narrative, the president also moved toward additional stakeholder support in counterterrorism surveillance programs.

D. FACING OUTWARD TOWARD EXTERNAL STAKEHOLDERS

Stakeholders in foreign intelligence processes include the FISC and Congress. Importantly, the media and general public are also stakeholders, for they are integral in public messaging and providing consent. Yet, despite the contentiousness within the executive branch over the Stellarwind program and other counterterrorism policies, the defensiveness of executive representatives when publicly discussing counterterrorism policies suggests that members of the protectors' ingroup perceived a sharp distinction between themselves and the outgroups of either Congress, the courts, the media, or the public more generally. The distinction between the public and government officials often becomes a more salient ingroup/outgroup dynamic in the face of public stakeholders' questions. There were many occasions where government officials discussed surveillance and counterterrorism policies in public during the Bush Administration, particularly as leaks brought these issues to national attention. Often, officials' outward statements illustrated a perceptually contentious group dynamic that wiped over any distinctions between subgroups within the government to present a unified front. The rhetoric used by officials in public often demonstrated a creatively reframed ingroup/outgroup narrative favoring a zero-sum version of the prevention narrative, which pitted those in favor of protecting innocent Americans against those in favor of helping the terrorists.

Public evidence of this distinction came shortly after the executive branch began its aggressive new counterterrorism policies. Just a few months after the 9/11 attacks, John Ashcroft appeared irritated at a Senate Judiciary Committee hearing over questions that legislators raised about the specter of aggressive executive activities. "We need honest, reasoned debate, and not fear-mongering....to those who scare peace-loving people with phantoms of lost liberty, my message is this: your tactics only aid terrorists, for they erode

³⁹⁷ See Doosje, Ellemers, and Spears, "Commitment and Intergroup Behaviour," 95; see also Hogg & Reid, "Social Identity, Self-Categorization, and the Communication of Group Norms," 21.

our national unity and diminish our resolve.”³⁹⁸ Ashcroft’s own public words set such a strong dichotomous narrative that suggested, to paraphrase President Bush, “you’re either with us or against us.”³⁹⁹ Ashcroft’s words set a tone that denied compromise, reasoned dissents or avenues for questions. In other words, they echoed the traits of the War Council and their superiors. In response to Ashcroft, Senator Patrick Leahy responded from behind the dais, “[e]veryone is against terrorists. This is about whether we are adequately protecting civil liberties.”⁴⁰⁰ This exchange was a microcosm of the security versus liberty debate after 9/11, wherein the protectors viewed as social outsiders anyone who failed to hyperbolically advocate for security.

This absolutist attitude was more than simply rhetoric; instead, this rhetoric illustrated the deeply entrenched mindset of the ingroup’s logic and actions. Several weeks after an announcement regarding detainee policy, Alberto Gonzales found himself surprised at questions he received while giving a speech at an American Bar Association event.⁴⁰¹ Gonzales’ surprise struck Suzanne Spaulding, herself a former attorney for the CIA, as “oblivious” to the potential public concerns, causing her to note the difficulties created by decisions made from the “bunker” that was the White House in the early period after 9/11.⁴⁰² Later, in 2004, when Gonzalez reportedly had a better understanding of the outgroup’s criticisms of counterterrorism policies, he spoke again before the ABA, this time describing the Bush Administration’s critics as those who “fundamentally misunderstood the nature of the threat this country is facing.”⁴⁰³ Similarly, in a speech at a press event after the *New York Times* broke the story on the surveillance programs, NSA

³⁹⁸ Terry Frieden, “Justice Defends Ashcroft’s Congressional Testimony,” *CNN*, December 7, 2001, <http://www.cnn.com/2001/ALLPOLITICS/12/07/inv.ashcroft.testimony/index.html>.

³⁹⁹ See “‘You’re Either With Us or Against Us,’” *CNN*, November 6, 2001, <http://edition.cnn.com/2001/US/11/06/gen.attack.on.terror/>.

⁴⁰⁰ Dan Eggen, “Ashcroft Defends Anti-Terrorism Steps,” *Washington Post*, December 7, 2001, https://www.washingtonpost.com/archive/politics/2001/12/07/ashcroft-defends-anti-terrorism-steps/6eb0037f-509a-4832-a3d7-5fe1c77fdefe/?utm_term=.06150c349a3f.

⁴⁰¹ Lichtblau, *Bush’s Law*, 39–40.

⁴⁰² Lichtblau, 40.

⁴⁰³ Alberto R. Gonzales, “Remarks to the American Bar Association Standing Committee on Law and National Security” (presentation, Washington, DC, February 24, 2004), <https://fas.org/irp/news/2004/02/gonzales.pdf>.

Director Michael Hayden told members of the press that he would rather be in the position he was in—publicly discussing controversial leaked surveillance programs—than being forced to talk about how the government failed to prevent an attack.⁴⁰⁴ These speeches provide insight into an ingroup’s adoption of a zero-sum version of the prevention narrative.

These distinctions with public media outlets accentuated the saliency of the government protector role, thereby highlighting the prevention narrative adopted in so many circles. That adoption, as in the example of when Alberto Gonzales spoke before the American Bar Association, can also lead to a lack of awareness or outright mitigation of the “non-righteous” views of other stakeholders. When ingroup members strongly embrace their group narrative, they risk discounting outgroup perspectives so significantly that they become unaware of the ability of those outgroup narratives to also gain traction in society as a whole. Put bluntly, the outgroup may also have valid arguments, but the ingroup blinds itself from seeing them. Interestingly, before 9/11, Hayden made great efforts to seek out public trust and support when he was first appointed director of the NSA. Not long after the release of a popular Will Smith movie, “Enemy of the State,” Hayden had significant concerns of a loss of public trust in government intelligence agencies. As an advocate for the IC, he became the first NSA director to appear on a Sunday political talk show.⁴⁰⁵ He was a rare public advocate for legitimate intelligence efforts and continues to be one today.⁴⁰⁶ Yet, when in the midst of controversy over the president’s surveillance programs, Hayden’s words referenced a simple dichotomy of options—act or face another attack—that eliminates all nuance. Here, even Hayden, the most contemplative individual on the nature of the security versus liberty debate in this case study based on the public record, was prone to fall back into an overly simplistic defensive framing when speaking to an outgroup.

⁴⁰⁴ Michael V. Hayden, “What American Intelligence & Especially the NSA Have Been Doing to Defend the Nation” (address to the National Press Club, Washington, DC, January 23, 2006), <https://fas.org/irp/news/2006/01/hayden012306.html>.

⁴⁰⁵ See Hayden, *Playing to the Edge*, 10, 119.

⁴⁰⁶ See Michael V. Hayden, *The Assault on Intelligence: American National Security in an Age of Lies* (New York: Penguin Press, 2018).

Members of the Bush Administration spoke to members of the media even more aggressively in private meetings, particularly they when saw a threat to the efficacy of their efforts. During discussions with representatives of the *New York Times* regarding the potential reporting of the surveillance programs, the president threatened leadership of the newspaper by arguing to them that in the event of another attack those reporters would be sitting before Congress with the leaders of the IC to provide testimony about why they let another attack occur. President Bush warned one of the paper's editors that, "there'll be blood on your hands."⁴⁰⁷ He asserted that the American people wanted him to "do everything in [his] power, under our laws and Constitution, to protect them."⁴⁰⁸ This use of rhetoric by the president demonstrates an attempt to creatively set the framework for the discussion: work with us or you'll be to blame for the next attack. It was an aggressively negative challenge to the outgroup. These types of statements can have multiple effects, to include increasing resolve within the ingroup but also increasing resolve in the outgroup, thereby setting the stage for increased levels of conflict instead of cooperation.

The writings of John Yoo, the attorney from the OLC who originally provided memoranda establishing the legal framework for many early Bush Administration counterterrorism policies, further demonstrate the outright dismissal of outgroup views. Yoo's language attempted to drive the administration's detractors to an extreme: "(t)he idea that all the lawyers in the Department of Justice, the White House, and the Defense Department are engaged in a conspiracy to twist the law of the land to authorize an illegal war is simply ridiculous."⁴⁰⁹ By putting a critical argument of, as he describes, "human rights lawyers, liberal interest groups, and political activists," on far-edged footing, he discounted any merits there may have been in the arguments.⁴¹⁰ Yoo also recast Republican concerns over PATRIOT Act reauthorization in 2003 as "a serious threat to the civil liberties of terror suspects..."⁴¹¹ "Excessive worry about civil liberties prevents us

⁴⁰⁷ Lichtblau, *Bush's Law*, 208.

⁴⁰⁸ Lichtblau, 213.

⁴⁰⁹ Yoo, *War by Other Means*, 21.

⁴¹⁰ Yoo, 21.

⁴¹¹ Yoo, 76.

from thinking more aggressively about electronic surveillance. The threat of an out-of-control executive seeking to harass its political enemies is not what looms before us. Legitimate political activities and speech by American citizens are not being suppressed,” Yoo calmly asserted in his book, *War by Other Means*.⁴¹² These discounts of outgroup messages highlight the point that people are more likely to view outgroup messages based on the messenger rather than the content of the message. If the message is not from an accepted ingroup source, ingroup members can easily discount the message.⁴¹³

Social groups that embrace the prevention narrative risk straining relationships with outgroup stakeholders. The allowance of this outward framing in response to stakeholder questions serves little more purpose than to drive distinctions between social groups and create more likelihood for conflict. The natural correlation is that these actions decrease the likelihood of cooperation and support among stakeholders. The evidence suggests that the executive branch too commonly put itself in a “bunker” mentality, driven by an embrace of the prevention narrative and its perceived sources, both internal and external to the group.

E. DAMAGE DONE AND TAKEAWAYS

The War Council’s embrace of the prevention narrative led to its isolation among other executive branch social groups and outside stakeholders like Congress, the courts, the media, and the public. Even if the Administration’s legal justifications were correct and upheld over time, the Bush Administration unnecessarily created significant risks for itself in implementing Stellarwind unilaterally. Both Michael Hayden and Jack Goldsmith assert that the administration could have limited its personal and institutional damage had it taken different avenues to achieve its goals.⁴¹⁴ Based on this case study, the social identity

⁴¹² Yoo, 96.

⁴¹³ See Katharine H. Greenaway et al., “Shared Identity is Key to Effective Communication,” *Personality and Social Psychology Bulletin* 41, no. 2 (February 2015): 172, 178–79; see also Daan Van Knippenberg, “Social Identity and Persuasion: Reconsidering the Role of Group Membership,” in *Social Identity and Social Cognition*, ed. Dominic Abrams and Michael A. Hogg (Oxford: Blackwell, 1999), 318–22.

⁴¹⁴ Goldsmith, *The Terror Presidency*, 217; Hayden, *Playing to the Edge*, 80.

analysis applied here, and the universality of how security officials can easily lean on the prevention narrative for similar reasons as those described in this thesis, it is likely that security and intelligence officials who embrace the prevention narrative and the effects of extreme discursive framing will continue to risk intelligence activities moving forward unless they take efforts to balance the equities of security and liberty.

This case study demonstrates that social groups who embrace the prevention narrative and ignore or mitigate liberty interests risk the dangers of unnecessary secrecy. In this case, the War Council created a bunker mentality for itself around the prevention narrative, which warped the ingroup framing. The results were often decisions or plans based on a narrow perspective of options, which ultimately placed the administration and executive agencies in a dangerous position of losing capabilities or authorities. This case study, through its social identity analysis, demonstrates how excessive secrecy leads to intergroup conflict, poor decision-making options, leaks, stakeholder pushback and lack of public support.

Referring to the words of Jack Goldsmith, the War Council likely felt the overriding considerations of security trumped any dissenting views; thus, security considerations drove a new narrative after 9/11. This resulted in the creation of a new, smaller ingroup of the decision-makers who thought along similar lines.⁴¹⁵ As that group of decision-makers tightened ranks, the potential for effective dissent diminished, either by numbers or in value, as the ingroup shouted down any dissenting voice as a negative deviant, left to either conform or eventually mobilize into a different social group.⁴¹⁶ The contentiousness of the relationship between the decision-making ingroup and outgroup members allowed the ingroup to discount the merits of the dissenter's concerns. It quickly devolved into "they don't see the big picture" or "they don't understand the consequences of inaction here."⁴¹⁷ The narrow ingroup fed upon its own narrative, increasing the pressure to build upon the

⁴¹⁵ See Goldsmith, *The Terror Presidency*, 167.

⁴¹⁶ See Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 35.

⁴¹⁷ For example, see John Yoo's mitigation of outgroup concerns as extreme (Yoo, "The Terrorist Surveillance Program and the Constitution," 579).

prevention narrative to the point that it incorporated tools and methods less important than the ingroup goals would originally suggest, as evidenced by the “one percent doctrine.”

The War Council’s hostile challenges to outgroups increased conflict between social groups. In this case, those challenges often involved excluding persons and groups who would normally be part of the interagency process for determining legal and policy matters. The conflict boiled over during the incident at the George Washington University Hospital. Social groups will always try to hold themselves in high esteem compared to other groups, and a failure to recognize other groups’ need for self-esteem will inevitably invite conflict. Conflict may be common at low levels, but the heightened levels of dynamic group conflict evidenced in the hospital scene demonstrate the extreme to which fervor for the various ingroup narratives grew. Even though the president resolved the issue quickly in the following days, the hospital incident echoed through the IC for years to come according to one attorney in 2007.⁴¹⁸ The conflict stirred up by these negative honor challenges serve as an affront to the outgroups involved, prompting a need for those groups to respond more aggressively or become submissive.⁴¹⁹ When controlling parties intentionally stifle the normal discussion process, the more likely response becomes a rarer outlet of more extreme actions. This may sometimes even include trying to effect social change through unusual methods when the subordinate group culture reaches an untenable stage. Leaks to the press are one such method.

Leaks of secret or classified information were perhaps the greatest threat to intelligence efficacy from this case. To a large extent, this threat may have been attributable to social conflict within the executive branch driven by the prevention narrative. The War Council’s efforts to centralize and consolidate power over legal and policy decisions had negative effects elsewhere in the executive branch. Other social groups within the executive branch likely viewed efforts by the Council to eliminate other viewpoints as a negative honor challenge against them, raising questions of their value or importance. Such efforts suggest the War Council considered these other groups irrelevant if they did not

⁴¹⁸ Edgar, *Beyond Snowden*, 41.

⁴¹⁹ See Brannan, Darken, and Strindberg, *A Practitioner’s Way Forward*, 69.

align themselves with their arguments. Certainly, the members of the War Council were group elites based on their range of knowledge and experience, as well as their held positions. Yet, this study shows that other social groups did not conform to the demands of those in power merely because they received orders, especially when those orders were in stark contrast to previously-held group norms. The failure of these other groups to conform suggests that the War Council isolated itself, in part through its advocacy of the prevention narrative. With greater isolation from subgroups it sought to influence came less influential leadership over those subgroups.

Both Michael Hayden and Jack Goldsmith assert that the Administration could have limited its personal and institutional damage (notably regarding leaks) had it taken different avenues to achieve its goals.⁴²⁰ “The main cause of leaks was...the perception within the government of illegitimate activity,” Goldsmith wrote.⁴²¹ Most famously in recent memory, this could apply to Edward Snowden, who leaked classified NSA program information—some of which originally arose from Stellarwind—purportedly to change how the federal government viewed privacy. But Snowden was not the only leaker: NSA member Russell Tice and Department of Justice attorney Thomas Tamm were the first to leak information related to the Stellarwind program in 2005.⁴²²

According to the social identity perspective, group members might feel compelled to leak information when they believe they have no other legitimate way to influence groups norms. Government protector ingroup members generally consider leaking secret information to the media to be a violation of injunctive group norms. Injunctive norms are those that group members follow for fear of social retribution for noncompliance.⁴²³ IC professionals maintain the secrecy of government information for fear of official retribution, whether it be reprimand, loss of group respect, loss of access to information, criminal prosecution, or loss of their job. However, studies demonstrate that high identifiers

⁴²⁰ Hayden, *Playing to the Edge*, 422; Goldsmith, *The Terror Presidency*, 217.

⁴²¹ Goldsmith, 27

⁴²² Edgar, *Beyond Snowden*, 41.

⁴²³ Hogg & Reid, “Social Identity, Self-Categorization, and the Communication of Group Norms,” 12; see also Terry, Hogg, and Duck, “Group Membership, Social Identity, and Attitudes,” 282–85.

are more likely to violate norms for what their group perceives as the greater good, particularly if they feel there are no other available options.⁴²⁴ In other words, it is possible that a leaker is willing to violate injunctive norms to better the organization in dire situations. This is often a reflection of the member's individual worldview and may often be wrong, but nonetheless may be a direct consequence for stifling dissent through excessive secrecy.

Social groups that implicitly embrace the prevention narrative also harm intelligence efficacy in the long run because they foster uncertainty and instability within social groups, creating risk aversion. Those groups create confusion among intelligence personnel who hear the sometimes-contradictory edicts of doing everything they can while also staying within laws, rules, and procedures.⁴²⁵ This dichotomy sets intelligence professionals up for dangerous cycles of inefficiency. Inconsistent messaging and fears of trouble from external oversight groups can have a deleterious effect on professionals' positive self-evaluation and certainty of performance, leading to an erosion of positive self-value.⁴²⁶ Director Hayden once described the stance of NSA professionals prior to 9/11 as similar to a baseball player standing at the plate with two strikes on the count.⁴²⁷ Past aggressive NSA programs like Shamrock and Minaret (from the Watergate era) led to a cautious and defensive NSA culture intent on not "striking out," to play on Hayden's sports metaphor.⁴²⁸ Many NSA officials themselves considered Minaret "disreputable if not outright illegal."⁴²⁹ Minaret ensnared many Americans in watch lists, including Dr. Martin Luther King, Jr., and politicians such as Frank Church, whose Senate committee investigated IC abuses.⁴³⁰ When information about the programs went public and the

⁴²⁴ See Doosje, Ellemers, and Spears, "Commitment and Intergroup Behaviour," 92.

⁴²⁵ See Goldsmith, *The Terror Presidency*, 92.

⁴²⁶ Whereas social groups seek stability and certainty (Turner, "Social Categorization and the Self Concept," 78).

⁴²⁷ Hayden, *Playing to the Edge*, 68.

⁴²⁸ Edgar, *Beyond Snowden*, 34.

⁴²⁹ Edgar, 34.

⁴³⁰ Edgar, 34.

hammer of stakeholder outrage dropped on the NSA, it caused ripples of risk aversion in the IC moving forward.⁴³¹

In a similar vein, the 9/11 Commission found that the CIA was “institutionally averse to risk,” as part of a continuing cycle that evolved over the years following major civil liberties abuses and the subsequent backlash.⁴³² This risk aversion in turn later led to questions when the organization failed to be aggressive and prevent future attacks. Likewise, NSA personnel were so reliant on a culture of compliance for fear that they appear to step out of line again.⁴³³ Edgar found that intelligence professionals inside the IC were deadly serious about compliance with rules and regulations.⁴³⁴ Yet, the dichotomy of “playing to the edge” creates conflict and confusion within the social group. It also leads to weaker efficacy moving forward should the tide of public opinion turn against new intelligence endeavors, increasing the odds of “striking out” in the future. Former ODNI attorney Timothy Edgar channels law professor Geoffrey Stone in asserting that the NSA has a deeply held commitment to the rule of law.⁴³⁵ It is important to put NSA employees, and other intelligence officials, in a position to be as effective as possible, which will often include enhancing the group’s value and stability. It is also important to understand, as NSA attorney John DeLong once advised, that privacy failures not only compromise civil liberties, but also endanger security through this cycle of risk aversion.⁴³⁶ For instance, in 2004, sources within the NSA told Eric Lichtblau of the *New York Times* that the possibility of a John Kerry presidency led them to suspect the end of the Stellarwind program and potential criminal prosecutions.⁴³⁷ This sort of instability is dangerous and untenable in a social group.

⁴³¹ Edgar, 46.

⁴³² *The 9/11 Commission Report*, 93; Goldsmith, *The Terror Presidency*, 95.

⁴³³ Edgar, *Beyond Snowden*, 41.

⁴³⁴ Edgar, 36.

⁴³⁵ Edgar, 7.

⁴³⁶ Edgar, 60.

⁴³⁷ Lichtblau, *Bush’s Law*, 203–4.

Social groups face the threat of destabilization in times of uncertainty, and at times during the Bush Administration uncertainty reigned. From the beginning, this thesis placed significant emphasis on the threats of resignation from members of the Department of Justice in 2004; however, this thesis cannot understate the panic and fear that also swept over personnel in the NSA after Judge Vinson's rejection of the FISA application in 2007. The NSA already had thousands of foreign targets at that point, and suddenly the agency found itself without legal authorization to move forward because it acted before cooperating with an external stakeholder.⁴³⁸ Alberto Gonzales lamented going to the FISC at all, but the reality is that the Bush Administration should have brought Stellarwind to the Congress and FISC from the beginning. Edgar notes that even intelligence professionals who supported the surveillance programs knew it would be political suicide to bring back that program without approval from the FISC.⁴³⁹ Even worse, the development of the prevention narrative within the executive branch had harmful repercussions on government officials. The stress that mounted from the singular focus of trying to prevent the possibly unpreventable also weighed heavily on those within the FBI. In an extreme case, the stress is believed to have led to a suicide.⁴⁴⁰ Panicked late-night phone calls were common in the years immediately following 9/11 for FBI and Department of Justice personnel such as David Kris, a former DOJ attorney, who often found himself being asked how to handle complicated, nuanced legal issues in the blink of an eye.⁴⁴¹ More common than not, he found himself erring on the side of the prevention narrative.⁴⁴²

The compliance process for Judge Vinson's orders caused an immediate and significant drop in targeted persons under surveillance.⁴⁴³ "For the first time since 9/11,

⁴³⁸ Edgar, *Beyond Snowden*, 46.

⁴³⁹ Edgar, 46.

⁴⁴⁰ Susan Doucette, the wife of Brad Doucette, believes the FBI member committed suicide under the weight of the pressure to prevent another attack (Lichtblau, 85–6; Greg Krikorian, "After 9/11, a Fatal 24/7," *Los Angeles Times*, May 3, 2005, <http://articles.latimes.com/2005/may/03/nation/na-counter3/3>).

⁴⁴¹ Lichtblau, *Bush's Law*, 86–87.

⁴⁴² Lichtblau, 87.

⁴⁴³ DOJ IG Report, 258.

the NSA was going dark,” Edgar wrote.⁴⁴⁴ This directly led to the administration finally reaching out to Congress in search of legislative remedies, first under the Protect America Act in August 2007, and then six months later through the FISA Amendments Act. Edgar notes that there was never any real resistance from Congress to the executive’s engagement in transnational intelligence collection; the questions only applied to how the executive could reasonably do so.⁴⁴⁵ The subsequent legislative effort led to privacy protections and authorized increased access to information for the government. By working through the legislative process, the Bush Administration obtained greater capabilities and more overt support from Congress, who acts as both an overseer and as a peer stakeholder on issues of national security.

In the aftermath of the Snowden revelations, the executive also faced multiple threats from Congress that inhibited its efficacy in surveillance and intelligence collection. Those threats included the removal of bulk collection authorities pursuant to the USA Freedom Act, threats to sunset critical provisions of the PATRIOT Act, and even threats to temporarily lapse provisions during debates over reauthorization of authorities that would have been easier without shocking headlines framing narratives in Congress. Despite these issues, when the executive branch finally participated in the legislative process to legalize Stellarwind it obtained more authority than it originally sought from the Congress. Through the PATRIOT Act, the Authorization for the Use of Military Force,⁴⁴⁶ the Protect America Act, and the FISA Amendments Act, the Bush Administration greatly expanded its surveillance and intelligence authorities beyond its unilateral efforts under Stellarwind. Indeed, the legislative process also codified greater privacy protections and oversight, increased support among stakeholders through the buy-in of the public’s elected representatives, and instilled more effective intelligence collection.

⁴⁴⁴ Edgar, *Beyond Snowden*, 46.

⁴⁴⁵ Edgar, 49.

⁴⁴⁶ Joint Resolution to Authorize the Use of United States Armed Forces Against Those Responsible for the Recent Attacks Against the United States, Public Law 107-40, 107th Cong., 1st sess. (September 18, 2001), 224–25.

The support of those stakeholders—Congress, the courts, and the public—could have sharply changed how this story played out from the beginning. In his memoir, Michael Hayden highlighted the importance of collaborating with stakeholders, including engaging the public in a dialogue.⁴⁴⁷ He wrote forcefully for the need to engage as a society on the terms of what actions the citizenry will accept from its intelligence professionals.⁴⁴⁸ He has publicly said that the people of the United States plan for the IC “to use every inch we’re given to protect her fellow citizens.”⁴⁴⁹ The question in response to that assertion is what space are intelligence professionals actually given? How much authority do they have? Authority does not necessarily correlate to a lack of restrictions, for often elected officials and the public do not contemplate intelligence efforts heretofore not previously attempted. Yet, officials driven by the prevention narrative become dismissive of outgroup concerns or critiques, justifying outgroup mitigation to cling to their narrative. Therefore, Hayden notes the need to engage in a civic discussion—perhaps without delving into details that could harm efficacy—of the general parameters acceptable for intelligence efforts.⁴⁵⁰ In theory, this would include a political dialogue within the Congress; in this case, administration officials intentionally evaded that dialogue through restricting the ingroup and, to paraphrase NSA General Counsel Robert Deitz, “drinking the bath water.”⁴⁵¹ While the White House brought in some congressional officials in the early days of the program, the Bush Administration did not inform the full House and Senate committees charged with intelligence oversight prior to the *New York Times*’ publication of Stellarwind’s existence.

Instead, David Addington viewed seeking congressional approval for counterterrorism policies as relinquishing the president’s authorities.⁴⁵² Addington refused to view Congress as a stakeholder or as holding any sort of legitimate oversight role. He

⁴⁴⁷ Hayden, *Playing to the Edge*, 426.

⁴⁴⁸ Hayden, 426.

⁴⁴⁹ Hayden, 119.

⁴⁵⁰ Hayden, 424.

⁴⁵¹ See Savage, *Power Wars*, 184.

⁴⁵² Goldsmith, *The Terror Presidency*, 78.

pushed the War Council into an intentionally antagonistic role based on decades of qualms. Addington attacked and antagonized those he deemed as irrelevant social outgroups. Addington questioned how Congress might try to restrict presidential authorities and counterterrorism policies.⁴⁵³ Jack Goldsmith viewed Addington's view of power "as the absence of constraint," and that he likely never believed that working with the Congress could actually enhance the executive's authorities.⁴⁵⁴ Conversely, Goldsmith calls for leaders to understand "the importance of consultation and consent, even during a crisis."⁴⁵⁵ He argues that spreading consent diffuses accountability to more actors.⁴⁵⁶ This directly mitigates risk as it can serve as a means of reframing the narrative back to the value of the collective government protectors, to include Congress, as representatives of the people. By acting in a solitary fashion, the administration and executive agencies took the brunt of criticism upon public disclosure of the programs when it could have shared responsibility through cooperation with other stakeholders like Congress. Additionally, engaging Congress at an earlier date could have opened a dialogue about appropriate authorities and responsibilities. Here, the administration only went to Congress for help when the deflating "constraints" of the FISC hindered its efforts; in turn, the administration only went to the FISC to prevent mass internal resignations. In the end, Congress gave the administration what it wanted and what it believed it needed in the name of national security. Only the suggestion of abuses within the executive led to Congressional threats of losing capabilities; otherwise, Congress has been a more-than-willing partner in the national security arena.

Despite Congress' willingness to cooperate, the War Council's focus on increasing executive power also increased the odds of conflicting with Congress and the courts. The War Council inflicted negative honor challenges upon Congress and the courts by asserting its unilateral authority to engage in the discussed surveillance activities, dismissing their positions as stakeholders in this arena. The administration made a legal argument to this

⁴⁵³ Goldsmith, 131.

⁴⁵⁴ Goldsmith, 126.

⁴⁵⁵ Goldsmith, 202.

⁴⁵⁶ Goldsmith, 182; Hayden, *Playing to the Edge*, 80-81.

end, but this case study demonstrates that is far from a foregone conclusion. In a famous Supreme Court case that discussed presidential authorities, *Youngstown Sheet & Tube Co. v. Sawyer*, Justice Jackson authored a heavily-cited concurrence outlining his views on the various levels of power held by the executive in engaging defensive constitutional authorities.⁴⁵⁷ Justice Jackson argued that the presidency can exert its strongest constitutional authority when acting in concurrence with congressional and judicial authorities.⁴⁵⁸ Conversely, the executive is at its lowest ebb of power when it acts in contravention to the authorities of the Congress and the courts.⁴⁵⁹ Justice Jackson's argument is as prescient for the courtroom as it is the political and practical considerations of social influence.

Regarding working with Congress, both John Yoo and Michael Hayden lament that the Bush Administration did not do more to garner legislative support to bolster the foundations of public support for intelligence programs. Yoo recommends reaching out further to Congress in the future, drawing an analogy to the process in place for keeping Congress apprised of covert actions.⁴⁶⁰ He also recommends more expansive briefings to leaders on the Hill regarding the surveillance programs.⁴⁶¹ In the end, Yoo recognizes the need for greater transparency, providing suggestions for how the executive could engage the NSA surveillance programs more adeptly.⁴⁶² He also offers that an interagency dialogue could enhance the public trust over the program's accountability.⁴⁶³ Yoo suggests that President Bush already created an early model of that decision-making process,⁴⁶⁴ but this case study has demonstrated the constricted nature of such efforts. Hayden also notes the tactical error in keeping the Congressional notifications so narrow, suggesting that it

⁴⁵⁷ *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), 634–55 (Jackson, J., concurring).

⁴⁵⁸ *Youngstown*, 635–37.

⁴⁵⁹ *Youngstown*, 637–38.

⁴⁶⁰ Yoo, *War by Other Means*, 127.

⁴⁶¹ Yoo, 127.

⁴⁶² Yoo, 126–27.

⁴⁶³ Yoo, 126.

⁴⁶⁴ Yoo, 126.

was a major flaw that led to a loss in support for the programs, both in Congress and in the public at large.⁴⁶⁵ At first, very few members of Congress were read into the Stellarwind program, and those who had access could not include staffers or record notes on the subject.⁴⁶⁶ Hayden also recognized the difficult position of the few members of Congress who were notified of the programs; the executive never sought their approval, but merely intended to notify them that the executive was engaged in certain activities.⁴⁶⁷ Hayden later noted that the executive should have briefed the House and Senate Intelligence committees in their entirety, and even some of their staffers.⁴⁶⁸ Beyond the mere notion of briefings on surveillance programs, however, is the tangential idea that the social groups should intend on working together to further policy. In this case that might have meant working with Congress from the beginning to strengthen the foundational authorities for future actions.

Indeed, the Bush Administration also found conflict with the courts. An institutional harm that Jack Goldsmith referenced because of the White House's aggressive actions was the courts' increased involvement in national security.⁴⁶⁹ In prior eras, the courts more commonly demurred on most of the litigation encroaching on foreign affairs or national security law as matters for the executive and Congress to handle. That sharply changed during the Bush Administration through a number of Supreme Court decisions, often notably regarding detention policies.⁴⁷⁰ Yet, the precedent for increased involvement is changing, and a growing number of courts have openly questioned executive national security policy decisions, including on issues of surveillance.⁴⁷¹ Goldsmith argues that, as

⁴⁶⁵ Hayden, *Playing to the Edge*, 79–80.

⁴⁶⁶ Hayden, 77–80.

⁴⁶⁷ Hayden, 79.

⁴⁶⁸ Hayden, 80.

⁴⁶⁹ Goldsmith, 135–37.

⁴⁷⁰ See *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004); see also *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006); *Boumediene v. Bush*, 553 U.S. 723 (2008).

⁴⁷¹ See *ACLU v. Clapper*.

a result of these changing precedents, the executive acutely lost power to the courts.⁴⁷² Similar dangers lurk for other federal, state, and local intelligence leaders; unnecessarily aggressive or controversial initiatives risk increased judicial involvement.

This discussion is ultimately about the threats to intelligence efficacy, which leaders leave vulnerable when they do not adequately take into consideration the reasonable questions of law and citizen privacy interests. As Hayden notes, the government in a liberal, transparent democracy must have the consent of the governed to be truly effective.⁴⁷³ The relevance of each of the stakeholder groups referenced so far—federal agency subgroups, the courts, and Congress—lead back to the most important stakeholder of all: the American people. Like many attorneys and officials who have worked in the IC in recent years, Timothy Edgar believes that the public would be much more comfortable with what the government does in the name of national security if they better understood the internally-created privacy protections and restrictions.⁴⁷⁴ As it stands now, in the wake of numerous disclosures about secret government surveillance efforts, the public is uneasy about what the government does in its name. Public polling in recent years shows that significant swaths of the American citizenry assume the government surveils citizens, often without justification, and that roughly half of the country disapproves of the government’s use of mass surveillance techniques.⁴⁷⁵ The likelihood of universal acceptance of government activities is low, but government actors could do significantly more to produce greater support from the public at large. Yet, to the ingroup of government intelligence officials, the public constitutes another outgroup. Revelations like the Snowden leaks highlight the saliency of that divide, causing more opportunities for conflict. As the social group acting on the other group’s behalf, it is incumbent on intelligence officials to seek

⁴⁷² Goldsmith, *The Terror Presidency*, 139–40, 217.

⁴⁷³ Hayden, 422.

⁴⁷⁴ Edgar, *Beyond Snowden*, 7–11.

⁴⁷⁵ Kenneth Olmstead, “Most Americans Think the Government Could be Monitoring Their Phone Calls and Emails,” Pew Research Center, September 27, 2017, <http://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails/>; “Few See Adequate Limits on NSA Surveillance Program,” Pew Research Center, July 26, 2013, <http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/>.

cooperation from the public as stakeholders and not simply dismiss their concerns as irrelevant. Such dismissive behaviors only fan the flames of conflict.

Timothy Edgar believes that NSA surveillance efforts are generally critical for national security, but they face a tough road in balancing their necessary efforts with the guiding forces in a transparent, liberal society.⁴⁷⁶ He argues that any increased efforts in transparency in recent years would not have happened at all without Snowden.⁴⁷⁷ Yet, it is important to note that Snowden compromised a variety of programs against adversaries and committed significant operational damage to the NSA's surveillance efficacy.⁴⁷⁸ Michael Hayden actually refers to Edward Snowden as "a gift," at least in one respect: Hayden argues that Snowden served as a "canary in a coal mine," in that he is the "visible effect (not the cause) of a broad cultural shift that is redefining legitimate secrecy, necessary transparency, and what constitutes the consent of the governed."⁴⁷⁹ In other words, Snowden serves to demonstrate that a true understanding of "playing to the edge" requires a broader understanding of societal concerns about intelligence collection and consent. Even before the Snowden leaks, Hayden pondered whether intelligence agencies could continue in a post-Cold War world that demanded more transparency and accountability of its intelligence professionals.⁴⁸⁰ Hayden sees the citizenry balking against a long-held reliance on trust in doing what is best for the country.⁴⁸¹ Hayden even believes that a reliance on working with standard oversight bodies may be insufficient today.⁴⁸² He calls for intelligence professionals to reach out to the public and strengthen the ties between them, all while still keeping a healthy respect for the level of secrecy required by intelligence collection and operational security.⁴⁸³

⁴⁷⁶ See Edgar, *Beyond Snowden*, 3–11.

⁴⁷⁷ Edgar, 6.

⁴⁷⁸ Edgar, 6.

⁴⁷⁹ Hayden, *Playing to the Edge*, 422.

⁴⁸⁰ Hayden, 422.

⁴⁸¹ Hayden, 422.

⁴⁸² Hayden, 422.

⁴⁸³ Hayden, 423.

This case demonstrates the difficulties of blending secretive intelligence efforts with increasing demands for public transparency. Abraham Lincoln once said that “public sentiment is everything. With public sentiment, nothing can fail; without it, nothing can succeed.”⁴⁸⁴ The controversies surrounding the post-9/11 surveillance programs evolved Director Hayden’s thoughts on how intelligence organizations should move forward in a nation demanding more accountability and transparency from its officials. Echoing the words of former national security adviser Stephen Hadley and Michael Leiter, who formerly served as the head of the National Counterterrorism Center, Hayden calls for “translucence” with the public, allowing them to generally understand the parameters of what actions the IC takes in the name of the American public.⁴⁸⁵ This could still protect operational security and secrecy enough to ensure efficacy and success.⁴⁸⁶ For all of Hayden’s experience on the growing difficulties facing intelligence officials, he perhaps summarizes the importance of his “before” and “after” most succinctly in a description of Venn diagrams. At one point, Hayden would have aimed for intelligence efforts to find the center within the concentric circles of what was legal, what was effective, and what was relevant to the effort. Now, he says intelligence leaders should also consider what is “politically sustainable.”⁴⁸⁷ To be clear, that does not mean what may be “politically correct,” but it instead means intelligence efforts should work from a foothold of popular support—from stakeholders, from oversight bodies, and from the public writ large. Only then can intelligence agencies succeed in the long run.

Secrecy has its import and value, particularly in the realm of intelligence. Yet, intelligence officials consistently find in modern times that the public expects more transparency.⁴⁸⁸ The Bush Administration—whether from ignorance of the dynamics of the group conflicts they accelerated, a blindness of the controversial nature of their

⁴⁸⁴ Abraham Lincoln, “Lincoln’s Reply,” in *Created Equal?: The Complete Lincoln-Douglas Debates of 1858*, ed. Paul M. Angle (Chicago: University of Chicago Press, 1991), 128.

⁴⁸⁵ Hayden, *Playing to the Edge*, 424.

⁴⁸⁶ Hayden, 424.

⁴⁸⁷ Hayden, 426.

⁴⁸⁸ See Richards, “Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy,” 763.

opinions, or through the elimination of any balancing rigors in their process—set itself up for failure in this regard. From the outskirts of the War Council, Director Hayden told Congressional leaders in a 2002 hearing before a joint Senate and House panel that, “[w]hat I really need you to do is to talk to your constituents and find out where the American people want that line between security and liberty to be.”⁴⁸⁹ To Hayden, the ramifications are startling. Wedging the IC into its own ingroup and shouting down the larger group of the American public will only lead to negative consequences. “If we continue this debate with one side muted, the outcome will not be in doubt: intelligence will be mismanaged or misdirected or crippled, and in the end neither liberty nor security will be served.”⁴⁹⁰ John Yoo similarly criticized the Bush Administration for its lack of public discussion or attempts to build public trust and support for their efforts in many counterterrorism policies, allowing them to instead be painted as malicious.⁴⁹¹ Yoo argued that the administration hid from media reports and public concerns rather than addressing them head on.⁴⁹² The “operational cost” of leakers and institutional harms from outgroup challengers are more significant than intelligence officials tend to consider, and the secretive culture of security at all costs leads to more operational security threats than leaders recognize. Running down the continued path of not recognizing these harms will hamper both operational success and public legitimacy.

It is critical for the modern “Terror Presidency,” according to Jack Goldsmith, to keep the public’s trust while they fight for public safety.⁴⁹³ It is also critical for an administration to persuade its agency members to adapt to new group norms, something else in which the Bush Administration failed. Today, the Snowden leaks (and others) harm operational capabilities, as the amount of terrorist communications lost to the federal

⁴⁸⁹ *Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence*, House Permanent Select Committee on Intelligence, 107th Cong., 2d sess. (statement of Michael V. Hayden, director, National Security Agency/chief, Central Security Service, October 17, 2002), 39, https://fas.org/irp/congress/2002_hr/101702hayden.html.

⁴⁹⁰ Hayden, *Playing to the Edge*, 423.

⁴⁹¹ Yoo, *War by Other Means*, Introduction.

⁴⁹² Yoo, Introduction.

⁴⁹³ “Of course, the main cause of leaks was not the absence of sanctions but rather the perception within the government of illegitimate activity.” (Goldsmith, *The Terror Presidency*, 216).

government via encryption continues to rise; while leaks may be a direct result of excessive secrecy, the “going dark” phenomenon is also a related (though indirect) consequence.⁴⁹⁴

Ethical and thoughtful leadership is imperative for intelligence officials moving forward. While a culture of compliance already exists in federal agencies, leadership must also take into consideration the moral, ethical, societal and political ramifications of intelligence efforts today. The evidence provided in this case study demonstrates that the Bush Administration focused excessively on the prevention narrative fostered by critical social groups, thereby belittling these ramifications as trite. The critical ingroup (the War Council) failed to see the greater picture of how their intelligence efforts needed to generate public support rather than contentiousness. When officials within the War Council began to learn that their efforts brought divided reactions, they clung to their discursive framing, asserting that they were doing what was necessary to protect the country. Perhaps they were, but those officials failed to effectively persuade a large percentage of the population. Members of the War Council even failed to generate effective discourse within the executive branch itself. They failed to effectively address potential concerns from executive branch members who ultimately became leakers and disrupters. Michael Hayden famously said he would play to the edge of what was permissible. Jack Goldsmith’s response is that “even blurry chalk lines delineate areas that are clearly out of bounds.”⁴⁹⁵ Moreover, without a reasoned and balanced perspective on where the chalk lines begin in society, intelligence officials cannot appropriately determine what is truly in bounds.

⁴⁹⁴ Edgar, *Beyond Snowden*, 145.

⁴⁹⁵ Goldsmith, *The Terror Presidency*, 78

IV. NAVIGATING TROUBLED WATERS THROUGH EFFECTIVE LEADERSHIP

Chapters II and III laid out many of the dangers lurking for intelligence officials who choose to embrace the prevention narrative within their social groups and belittle the importance of balancing security and liberty interests, including privacy rights and rule of law concerns. The decision-making process that created the post-9/11 NSA surveillance programs (namely, Stellarwind) provides fodder for many of the potential pitfalls awaiting intelligence officials who ignore these fundamental considerations. These pitfalls include severe institutional harms, loss of public trust, and damaged relationships with critical stakeholders, including their community citizenry, advocacy groups, the media, and groups like legislators who have overlapping responsibilities. As seen in Chapters II and III, those institutional harms may come in the form of weakened workforce morale, threats to institutional efficacy through information leaks, increased assertions of power from other stakeholders like the judiciary, and threatened loss of institutional power through the legislative process. If the Bush Administration worked through the regular legislative process from the beginning of its efforts to overhaul its intelligence capabilities after 9/11, it could have likely obtained all the same authorities seized unilaterally without many of the dangerous harms it created for itself. Instead, the administration suffered threats or actual harms from all the above-noted risks. This chapter begins by analyzing the failures of key Bush Administration officials in not using effective leadership to create change and discusses the ramifications and parallels for all intelligence enterprises. Moving forward, this chapter also discusses the importance of leadership in proactively steering organizations away from such deleterious harms.

For most intelligence organizations, abuse of authorities or capabilities lead to diminished resources or power. However, effective and responsible leadership can mitigate or repair many of the internal harms, like damage to workplace morale.⁴⁹⁶ Regarding

⁴⁹⁶ For an illustrative example, Ed Catmull provides an intriguing discussion of his efforts to retrain Disney Animation employees after years of conflicting bureaucratic pressures and poor leadership (Ed Catmull, “A New Challenge,” in *Creativity, Inc.: Overcoming the Unseen Forces that Stand in the Way of True Inspiration* (New York: Random House, 2014), 243).

external threats, the executive branch of the federal government, and particularly the IC, is too big to fail. Congress is not likely to eliminate the IC's functions related to national security, nor is Congress likely to eliminate the IC's most important tools in the counterterrorism fight.⁴⁹⁷ In this way, the Bush Administration was fortunate. Yet, history demonstrates that executive agencies are not immune to abuses, as the Church Committee revelations exhibit. After that incident, executive agencies found themselves saddled with significant restrictions and oversight, to the point today where several congressional committees oversee IC agencies and legal restrictions significantly limit authorities. As demonstrated in the FISA overview in Chapter II, fallout from civil liberties or rule of law abuses can also lead to significant bureaucratic oversight that was once not a consideration.

Of course, the seventeen agencies that comprise the federal IC are not the only entities involved in intelligence within the United States. State and local law enforcement and homeland security entities increasingly became involved in intelligence collection after September 11, 2001, and with good cause.⁴⁹⁸ As the 9/11 Commission Report notes, a major flaw in the federal intelligence effort prior to 9/11 was the lack of information-sharing and resources devoted to intelligence collection.⁴⁹⁹ State and local intelligence enterprises, if used effectively, can serve to fill in those gaps inherent in a porous United States federal intelligence system. However, few (if any) of those state and local intelligence entities' host agencies created their intelligence enterprises with a sole or primary purpose of counterterrorism or domestic security. Most of the intelligence enterprises in effect today arose from intelligence-led policing efforts from state and local law enforcement agencies. These intelligence enterprises are not too big to fail; under the

⁴⁹⁷ Without much debate, Congress recently reauthorized Section 702 authorities with little (Charlie Savage, "Congress Approves Six-Year Extension of Surveillance Law," *New York Times*, January 18, 2018, <https://www.nytimes.com/2018/01/18/us/politics/surveillance-congress-snowden-privacy.html>).

⁴⁹⁸ For example, state and local agencies now run dozens of fusion centers across the United States, wherein they coordinate with federal, state, and local agencies to share information on criminal activity. Notably, these fusion centers originated in the aftermath of 9/11 as a method to increase the flow of information between federal agencies with state and local partners. ("State and Major Urban Area Fusion Centers," United States Department of Homeland Security, last published June 26, 2017, <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>; "National Network of Fusion Centers Fact Sheet," United States Department of Homeland Security, last published June 21, 2017, <https://www.dhs.gov/national-network-fusion-centers-fact-sheet>).

⁴⁹⁹ See *The 9/11 Commission Report*, 408–10.

right circumstances, any of these agencies could shutter their intelligence enterprises or restrict capabilities so harshly as to render them wholly ineffective. Such agencies may restructure the intelligence effort after perceived abuses, but they will always be involved in criminal investigations. Yet, deleterious effects of the unitary executive model of the presidency, as espoused in this case study by Vice President Cheney and his counsel David Addington, still led to significant harms to the office of the president and the executive agencies that serve the president. Those harms included the loss of judicial deference on matters of national security and increased scrutiny by other stakeholders, including Congress and the media. All of these harms contributed to perhaps the most damaging harm of all: the loss of public trust.

While their components and resources may be different, state and local intelligence enterprises can suffer the same problems outlined in the prior chapters. Primarily comprised of law enforcement agencies, these state and local organizations inherently see themselves as “government protectors” just like the FBI or the NSA, perhaps only different in their mission scope and area of responsibility. These organizations are also susceptible to succumbing to the extremes of the prevention narrative. Even larger state and local intelligence enterprises risk significant costs for observed abuses. The City of New York recently paid out an undisclosed (though surely substantial) cost to settle two high-profile cases regarding the New York City Police Department’s dragnet surveillance of its city’s Muslim population.⁵⁰⁰ Like the case study outlined in Chapters II and III, the NYPD case stemmed from an understandable sentiment after 9/11 that the agency and the city could not tolerate another terrorist event. In its effort to better understand the failures that allowed the 9/11 attacks in New York, the NYPD concluded that the radicalization process is murky, inconsistent, and difficult to trace;⁵⁰¹ thus, the NYPD engaged in a concerted effort to monitor as much as it could of the city’s Muslim population in the hopes of catching and

⁵⁰⁰ Colin Moynihan, “Last Suit Accusing N.Y.P.D. of Spying on Muslims is Settled,” *New York Times*, April 5, 2018, <https://www.nytimes.com/2018/04/05/nyregion/last-suit-accusing-nypd-of-spying-on-muslims-is-settled.html>.

⁵⁰¹ See Mitchel D. Silber and Arvis Bhatt, *Radicalization in the West: The Homegrown Threat* (New York: New York City Police Department, 2007), https://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf.

preventing future events.⁵⁰² The NYPD embraced the prevention narrative so strongly that monitoring based solely on constitutionally-protected characteristics or activities became regular order. Once the program leaked, the NYPD found itself in a firestorm of community outrage, media scrutiny, and litigation.⁵⁰³ The end results of the litigation forced greater external oversight and financial burdens onto the NYPD.⁵⁰⁴ To justify these encumbrances, the NYPD initiated zero official investigations from their Muslim surveillance intelligence efforts before shutting down the program.⁵⁰⁵ This example, along with the case study, demonstrates that the dangers of allowing imbalances in liberty and security can lead to significant institutional harms for intelligence officials at any level of government. All these dangers demonstrate the importance for intelligence enterprise leaders to understand the need to ensure a balance of security and liberty considerations within intelligence organizations. When government actors engage in actions that trigger a loss of stakeholder support, they open themselves up to debilitating harms.

Yet, incumbent in this exercise is the understanding that serious, sometimes aggressive intelligence efforts may be necessary to accomplish effective policing and/or prevention. So, with that realization, this study accepts the value and importance of intelligence efforts generally. Just as this case study demonstrates the dangers of embracing the prevention narrative and engaging in overzealous intelligence efforts to the result of significant harms, leaders should also not heed this examination as justification to become unnecessarily cautious, like some in the IC did after prior abuses. The difficulty for intelligence leaders is to maintain the proper balance of considering security and liberty interests to ensure the greatest level of efficacy and stakeholder support possible given whatever circumstances may present themselves. The navigation of such troubled waters

⁵⁰² See Matt Apuzzo and Adam Goldman, *Enemies Within: Inside the NYPD's Secret Spying Unit and Bin Laden's Final Plot Against America* (New York: Touchstone, 2013).

⁵⁰³ See David Crary, "AP Series about NYPD Surveillance Wins Pulitzer," *Associated Press*, April 16, 2012, <https://www.ap.org/ap-in-the-news/2012/ap-series-about-nypd-surveillance-wins-pulitzer>.

⁵⁰⁴ "Raza v. City of New York— Settlement FAQ," American Civil Liberties Union, accessed July 9, 2018, <https://www.aclu.org/other/raza-v-city-new-york-settlement-faq>.

⁵⁰⁵ Galati Dep. 96: 16-23, June 28, 2012, <https://www.scribd.com/document/103649979/Pages-From-Thomas-Galati-NYPD-Handschu-deposition-EBT-6-28-12-Tcm28-8694> (accessed July 9, 2018).

is difficult because that water is often murky; leaders are unable to predict the future and know what their actions might bring. This applies equally for both the efficacy of preventive measures and for potential stakeholder responses. Leaders cannot insulate themselves from the unknown, but through the recommendations outlined in this chapter and the next, they may better prepare themselves to tackle the unknown and better understand where the edge of appropriateness lies.

This project's analysis through the social identity perspective also highlights the limitations of efficacy in perceptually external oversight. James Madison once highlighted the importance of government oversight, including checks and balances:

If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place, oblige it to control itself.⁵⁰⁶

Madison's words speak to checks and balances on government generally but can easily apply to any activity of government therein. This includes the collection of intelligence, even if executive government intelligence efforts were largely unregulated until the middle of the twentieth century. Indeed, if government entities were able to consistently demonstrate the ability to police themselves, external oversight would not be necessary. This Madisonian quotation is especially pertinent, not only for its message, but also because of its messenger. James Madison and his brethren national founders steeped themselves in the study of Enlightenment thinking. Those studies greatly contribute to the principles inherent in the founding documents of the United States, and the nation's early literary guidance like the *Federalist* and *Anti-Federalist Papers*. Just as Enlightenment principles greatly contributed to this nation's founding principles, they also contribute to the practice of intelligence, which bases its methodological process and findings on hypotheses, research, and objective analysis.⁵⁰⁷ Yet, this project demonstrates the

⁵⁰⁶ James Madison, "Federalist No. 51," in *The Debate on the Constitution*, vol. 2, ed. Bernard Bailyn (New York: Library Classics of the United States, Inc., 1993), 164.

⁵⁰⁷ Hayden, *The Assault on Intelligence*, 221.

limitations of external oversight even in robust systems. The case study demonstrates how actors can easily thwart external overseers by simply refusing them access to information. Moreover, the social identity perspective upon which this paper relies highlights the potential weakness of outgroup external oversight bodies and how easily conflict can arise between social groups, such as when executive agency groups tried to review or challenge Stellarwind. External oversight alone may be insufficient to prepare intelligence enterprises for operating in transparent societies; instead, intelligence leaders should consider internal cultural mechanisms to better balance security and liberty concerns.

The following chapters note several relevant considerations for intelligence leaders, pulling from the case study discussed in Chapters II and III. These recommendations are not one-size-fits-all, and are merely meant to start a dialogue on new potential methods for providing better internal oversight through influencing cultural norms. The intention is not to eliminate the need for external oversight mechanisms such as legislative committees, media watchdogs, inspectors general or general counsels; instead, what follows can effectively supplement their work by placing greater responsibility upon the intelligence culture itself to support a reasonable balance between security and liberty instead of the extremes of the prevention narrative. The chapters that follow provide guidance to intelligence leaders on how to influence the security culture within intelligence enterprises through effective leadership, and on how to better consider and prepare for potential concerns from external stakeholders over what constitutes the appropriate actions of intelligence officials in a transparent, liberal democracy. From there, the discussion extends to how intelligence enterprises should work with those external stakeholders to enhance support and cooperation, ensuring a more solid foundation for intelligence efforts.

A. THE ROLE OF LEADERSHIP IN INFLUENCING THE INGROUP CULTURE

This exercise of organizational culture change begins with leadership. Leadership does not necessarily mean those in hierarchical positions of power, but rather here it means those best suited to influence the norms of an organization's social groups because they most fully represent a group's ideals. Preferably, that would include an organization's policymakers; yet leaders must be sufficiently self-aware and observant to understand the

social dynamics within their organization. In doing so, they can understand whether they are the best direct sources of attempting influential change, whether they should rely on recruiting others as proxies for influential change, and to whom should they look for recruitment. For leaders who hope to better balance security and liberty concerns to avoid the previously-discussed pitfalls, three goals should take precedence: (1) leaders should start small in their efforts; (2) leaders should be aware of the social dynamics as they exist and be willing to adapt proportionally; and (3) leaders should seek to enhance transparency through effective communication within their workforce.⁵⁰⁸

According to the social identity perspective, prototypical leaders need to do more than just embody the group prototype; the prototypical leader must also use the power conveyed through their social placement to influence the group.⁵⁰⁹ This project's case study provides effective examples of some leaders who harnessed these measures to influence ingroup culture, and exposes others who did not. David Addington, as a leader in the prototype position of the War Council, effectively influenced the ingroup culture of that narrow subgroup. Yet, even though this narrow social group possessed the capability to control critical decisions, it was not the only relevant social group. The case study demonstrates the importance of the organization as a whole—and not just the narrower subgroup of policymakers—for establishing organizational influence. Addington severely hindered his own ability (and that of the War Council) to effectively influence group norms for the broader group of government protectors within the executive branch due to his negative barrages on those who questioned his intentions or conclusions. His techniques included shouting down reasonable dissenters, eliminating such people from involvement in future decisions, and punishing those who did not fall in line. These negative actions will not win useful influence from a broader audience uncertain of an individual's justifications for action. Addington's actions presupposed prototypicality and ingroup influence, yet he struggled with those who do not already consider themselves to be part of the narrow ingroup of the War Council.

⁵⁰⁸ Eric Ries, *The Lean Startup* (New York: Crown Business, 2011), 224.

⁵⁰⁹ Hogg, "A Social Identity Theory of Leadership," 194.

Leaders who embody the group prototype have the most influence over the group's vision of the prototype, though the group must still accept the leader's interpretation.⁵¹⁰ In that way, leaders have a disproportionate capability to influence the vision of an ingroup prototype.⁵¹¹ However, that capability is not absolute. Leaders can influence an ingroup's vision through communicative tools, including highlighting ingroup norms or downplaying negative deviants.⁵¹² Addington, or by proxy President Bush or Vice President Cheney, used these techniques to influence the actions of the War Council members who readily subscribed to the ingroup ideology. These members could be considered "high identifiers," or those organizational members who strongly attach their social identity to organizational values; however, any ingroup broader than the narrow subset of the War Council found Addington's influence of social dynamics lacking.

Social groups favor stability and certainty. New initiatives are often the most difficult for leaders to undertake with their group members while maintaining group certainty; new initiatives naturally bring about the unfamiliar.⁵¹³ In contrast to Addington's gruff orders, NSA Director Michael Hayden engaged in attempts to garner organizational support through means of communication and transparency with an awareness of the difficulties inherent in new initiatives. Hayden's efforts are clear examples of attempts at coalition building and transparent communication. After key decision makers at the NSA devised the origins of the Stellarwind program and President Bush approved the program, Hayden took efforts to ensure the members of his agency would support the mission. He recognized the significant culture of compliance his members followed, and he knew that many of them would see the newly-designed mission of Stellarwind as violating rule-of-law cultural norms within the organization since it deviated from the agency's regular norms of surveillance within the United States. When he first suggested the program to President Bush, Vice President Cheney, and Director of Central Intelligence George Tenet, Hayden explained this new initiative would require new

⁵¹⁰ Hogg, 191.

⁵¹¹ Hogg, 188.

⁵¹² Hogg, 191.

⁵¹³ See Havermans, Keegan, and Den Hartog, "Choosing Your Words Carefully," 973–74.

legal authorities. Upon gaining support from his superiors and learning that the president would rely solely on his Article II authorities, Hayden knew this could cause concerns within his organization. He also wanted to ensure that his ingroup legal counsel believed the president's justification to be sufficient. Hayden sought NSA General Counsel Robert Deitz's support prior to acting and though Deitz may not still agree with his decision, he approved the legal justification at the time.⁵¹⁴ Once Deitz was on board, Hayden spoke to his key leadership members in a public address so they could hear directly from him about exactly what he expected the agency to do, and where he drew the line.⁵¹⁵ Hayden made sure that his senior team and legal counsel supported his choices, and that the agency's membership saw those senior personnel standing in support.⁵¹⁶ There were still substantial concerns among NSA personnel about acting in contradiction to FISA-based intelligence norms; yet, Hayden's methods surely positioned his group to be better prepared for what was to come.⁵¹⁷

These examples highlight the need for intelligence leaders to be aware of relevant group dynamics and to communicate effectively to gain ingroup support. Once an organizational leader chooses to balance the equities of security and liberty within an organization, the leader should immediately begin considering how to implement his or her intentions, starting with how he or she intends to influence ingroup members via communication. The use of communication skills is critical for leaders to effectively influence cultural norms. This can even be as simple as considering how a leader speaks. Leaders commonly use several forms of speech to draw group members back to the framings of familiar ideas, including the use of quotations or paraphrasing.⁵¹⁸ Bakhtin calls these tools "speech centers."⁵¹⁹ This method allows leaders to tie new concepts back to

⁵¹⁴ Hayden, *Playing to the Edge*, 70.

⁵¹⁵ Hayden, 73.

⁵¹⁶ Hayden, 73.

⁵¹⁷ See Edgar, *Beyond Snowden*, 41.

⁵¹⁸ Anderson, "What You'll Say Is..." 66–67.

⁵¹⁹ Mikhail Bakhtin, "Discourse in Dostoevsky," in *Problems of Dostoevsky's Poetics*, ed. and trans. Caryl Emerson (Minneapolis: University of Minnesota Press, 1984), 187.

familiar territory, thus increasing the likelihood of effective processing by ingroup members.⁵²⁰

There are also different forms of verbal communication between leadership and group members. Farmer, Slater, and Wright discussed and tested the value of flattening the “communications hierarchy” to achieve greater ingroup support.⁵²¹ Communications between leadership and subordinates necessarily requires some sort of hierarchical nature to push down a message *en masse*, otherwise an organizational leader would never escape an endless cycle of one-on-one or small group conversations to communicate with an entire agency. When an organizational chief decides to push a new vision, there will inherently be some form of one-way communication model to inform the entire organization or subgroup of the initial plan.⁵²² Yet, Farmer, Slater, and Wright’s study demonstrates that significant two-way dialogues must also occur to garner sufficient understanding of the leadership’s vision and support from the organizational mass.⁵²³ The “press agency” or “public information” model of one-way communication via an agency-wide email or group presentation is only the start of a greater dialogue.⁵²⁴

From there, leaders should be prepared to transition to two-way dialogue methods wherein they seek input from ingroup organizational members to understand how their initial plans fit (or do not fit) with ingroup norms and values.⁵²⁵ Leaders seeking to influence relationships with subgroups must recognize the relevant subgroups’ perspectives.⁵²⁶ Only then can they appeal to mutual interests in attempting to align their

⁵²⁰ Anderson, “What You’ll Say Is...,” 66–67, 70.

⁵²¹ Betty A. Farmer, John W. Slater, and Kathleen S. Wright, “The Role of Communication in Achieving Shared Vision Under New Organizational Leadership,” *Journal of Public Relations Research* 10, no. 4 (1998): 233.

⁵²² Farmer, Slater, and Wright, 232.

⁵²³ Farmer, Slater, and Wright, 232.

⁵²⁴ Farmer, Slater, and Wright, 232.

⁵²⁵ See Farmer, Slater, and Wright, 221–22, 232.

⁵²⁶ See Daniel Korschun, “Boundary-Spanning Employees and Relationships with External Stakeholders: A Social Identity Approach,” *Academy of Management Review* 40, no. 4 (October 2015): 619.

goals.⁵²⁷ Fitting action with rhetoric, leaders should also be prepared to alter their plans to most effectively fit their group; in other words, transparency is critical and listening sessions cannot be perfunctory matters. Rhetoric and action are both important for leaders.⁵²⁸ Ultimately, evolving the leadership-to-ingroup member discussion to a two-way symmetrical dialogue where ingroup members feel free to set titles aside and freely discuss ideas leads to the strongest percentages of ingroup vision acceptance.⁵²⁹ Leaders should champion a collaborative relationship to garner the greatest possible ingroup support.⁵³⁰ Additionally, actions must bolster rhetoric.⁵³¹ If a leader suggests that he or she wants to hear from ingroup members, that leader cannot simply dismiss feedback with which the leader disagrees without some level of transparency in providing justifications.

These principles outline how leaders can communicate to garner ingroup buy-in for new ideas, but they omit guidance as to whom and how many members leaders can aim to influence at any given time. Leaders serve as boundary-spanners, meaning they serve as ambassadors of their ingroups to other groups.⁵³² Within an organization, that may mean an agency chief serves as an ambassador of the organizational policymaking ingroup to every other subgroup of the organization, wherein the chief uses her position to communicate the values of the policymaking ingroup to analysts, officers, oversight personnel, and even technical staff. However, leaders should avoid the common mistake of trying to be too much to too many people, particularly when trying to institute significant organizational change.⁵³³ The social identity perspective suggests that ingroup members

⁵²⁷ Korschun, 619.

⁵²⁸ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 241–42.

⁵²⁹ See Farmer, Slater, and Wright, "The Role of Communication in Achieving Shared Vision Under New Organizational Leadership," 221–22, 232.

⁵³⁰ See Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 234.

⁵³¹ Hogg, Van Knippenberg, and Rast, 241–42.

⁵³² See Hogg, Van Knippenberg, and Rast, 241, 243–45.

⁵³³ "If a group becomes less cohesive, more diverse, and less consensual about its prototype, it is less likely that followers will endorse the same person as the leader" (Hogg, "A Social Identity Theory of Leadership," 194).

should perceive leaders as ingroup prototypes to gain the group's consent to lead.⁵³⁴ Otherwise, as also seen in the case study through the president and vice president's use of coercive positional power, the use of positional power limits efficacy to the extent that extrinsic motivations can truly drive adoption.⁵³⁵

To the contrary, a prototypical leader can affect members' intrinsic motivations, and leaders are more likely to garner support and compliance from other ingroup members because of the social attraction hypothesis.⁵³⁶ The social attraction hypothesis provides that prototypical leaders have an easier time persuading fellow ingroup members; studies demonstrate that people agree more with people they like.⁵³⁷ People tend to like a prototype more because the prototype represents an ideal within the ingroup.⁵³⁸ Social attraction hypothesis also argues that strong prototypical leaders typically demonstrate a preference to ingroup members and consistent fairness within the ingroup, meaning that ingroup members show preference for prototypical leaders that they view as being "on their side," or favorable to them rather than to other groups.⁵³⁹ Should a leader maintain consistency with the prototype ideal over time, the leader will continue to gain clout with the ingroup.⁵⁴⁰ Leaders should recognize this and use their capabilities of influence to keep the prototype ideal in a beneficial place for the leader.

These preceding principles are simple to articulate, but sometimes arduous to develop. The process of developing sufficient trust among ingroup members can be slow and takes place over time.⁵⁴¹ As such, leaders should take heed of advice from Eric Ries

⁵³⁴ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 240–41.

⁵³⁵ "In environments where extrinsic rewards are most salient, many people work only to the point that triggers the reward—and no further." (Daniel H. Pink, *Drive: The Surprising Truth About What Motivates Us* (New York: Riverhead Books, 2011), 58).

⁵³⁶ See Hogg, "A Social Identity Theory of Leadership," 187.

⁵³⁷ Hogg, 191.

⁵³⁸ Hogg, 187.

⁵³⁹ Hogg, 189–90.

⁵⁴⁰ Hogg, 186, 190–91.

⁵⁴¹ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 242.

and be sure to start small rather than diving into grandiose, radical changes immediately.⁵⁴² The “build, measure, learn” process of adaptive organizations and lean design fits well within the constructs of the social identity perspective described here.⁵⁴³ The lean management philosophy, which may be more familiar than social psychology to many in managerial positions, also speaks to the need for adaptive learning by policymakers to ensure their vision effectively fits the needs of their organization.⁵⁴⁴

Leadership is critical for influencing organizational norms, but leadership takes place within the context of social dynamics.⁵⁴⁵ There are generally two types of organizations: ideographic and holographic organizations.⁵⁴⁶ The holographic model exists when an organization’s members associate their group values with an entire organization collectively, while the ideographic model exists when group members identify primarily with their subgroup.⁵⁴⁷ Most organizations lean toward the ideographic model.⁵⁴⁸ The social identity of the closer subgroup pulls at members more strongly than the vaguer superordinate group.⁵⁴⁹ This means that intelligence enterprise members may still associate their identity and values with those of the superordinate intelligence enterprise, but are likely to associate more closely with a subgroup (such as a regional office or individual department) should any tension or conflict arise between subgroups. To the issue of leadership, this raises the question of how effective an organizational chief (or any other subgroup leader) can be in influencing a diverse organization of subgroups on his own. This issue is also relevant to the efficacy of a small group of policymakers (like the War Council) in spreading cultural norms across a diverse organization. Groups strive

⁵⁴² Ries, *The Lean Startup*, 238–39.

⁵⁴³ Ries, 228.

⁵⁴⁴ Ries, 224.

⁵⁴⁵ Hogg, “A Social Identity Theory of Leadership,” 193.

⁵⁴⁶ Michael G. Pratt and Peter O. Foreman, “Classifying Managerial Responses to Multiple Organizational Identities,” *Academy of Management Review* 25, no. 1 (January 2000): 20–22.

⁵⁴⁷ Pratt and Foreman, 20–22.

⁵⁴⁸ See Josephine Hennessy and Michael A. West, “Intergroup Behavior in Organizations: A Field Test of Social Identity Theory,” *Small Group Research* 30, no. 3 (June 1999): 376–79.

⁵⁴⁹ See Hennessy and West, 376–79.

for a cohesive and consistent vision of the prototype, which means that they also strive for a cohesive and consistent vision of the ingroup itself; in shaping that vision, leaders must be cognizant to not stretch the vision (or the ingroup) so far as to lose its distinctiveness.⁵⁵⁰ The more diverse an ingroup becomes, the more likely the ingroup will disintegrate, or at the minimum, erupt with uncertainty.⁵⁵¹ In other words, leaders have difficulty effectively influencing members of subgroups to which they do not belong. The moment that the subgroup becomes more salient than the superordinate, the external policymaker is under threat to appear as a foreign entity to the subgroup unless there is a connection that makes the ingroup believe the policymaker is “one of their own.”

This leads to the question of how leaders can change organizational values while still maintaining effective influential leadership and recognizing issues related to intergroup relationships. For the purposes of this project, this question asks how a leader of an intelligence organization can influence group culture so that the group balances liberty considerations with security; yet, the question can also apply to organizational change more generally. The social identity perspective recognizes the difficulties in effectively projecting leadership beyond one’s own ingroup, even if that leader is reaching out to other subgroups still within the same organization. The literature on the social identity perspective suggests several principles to consider initiating this organizational change. Much of that literature focuses on concepts such as cross-categorization, superordinate identities, and social creativity to achieve those ends.

One theory on how to bring disparate groups together is cross-categorization, which is the process of reframing respective ingroup narratives to emphasize an overlapping group identity.⁵⁵² Cross-categorization theory argues that the reframed narratives will cause the relevant group saliency to expand beyond previous group lines.⁵⁵³ For this to

⁵⁵⁰ Hogg, “A Social Identity Theory of Leadership,” 194.

⁵⁵¹ Hogg, 194.

⁵⁵² See Lucy Johnston and Miles Hewstone, “Intergroup Contact: Social Identity and Social Cognition,” in *Social Identity Theory: Constructive and Critical Advances*, ed. Dominic Abrams and Michael A. Hogg (New York: Springer-Verlag, 1990), 192–94.

⁵⁵³ See Johnston and Hewstone, 192–94.

work, the salient characteristics of the cross-categorized group must be as or more salient than the particular subgroups.⁵⁵⁴ Unfortunately for this exercise, Brown and Turner demonstrated some time ago that cross-categorization towards a superordinate identity can have mixed results.⁵⁵⁵

Related to cross-categorization, the theory of the superordinate identity speaks to that overlapping group identity or overarching value system that connects multiple subgroups together. For organizations, the concept primarily focuses on highlighting the organization's value system over the potentially conflicting or competing values and norms of its subgroups. One of the dangers of attempting superordinate identities is in the risk of leaders losing their base by trying to reach out too much to a given outgroup.⁵⁵⁶ In doing so, leaders risk their ingroup members no longer seeing them as "one of us," but rather "one of them."⁵⁵⁷ This risks ingroup members viewing their prototypical leader as being less fair or just to their own members, which can significantly damage prototypicality. Moreover, superordinate narratives can risk ingroup distinctiveness.⁵⁵⁸ Even if superordinate identities worked in the short term, they can easily fray in times of conflict.⁵⁵⁹ For an ingroup and superordinate group to align, each group's values should go toward a superordinate alignment of narratives between groups.⁵⁶⁰

Organizational leaders should find ways to align the values of subgroups (particularly the subgroup of policymakers from which policy decisions may arise) with the organization's various other groups in the superordinate organization, while still

⁵⁵⁴ See Johnston and Hewstone, 192–94.

⁵⁵⁵ See Rupert J. Brown and John C. Turner, "The Criss-Cross Categorization Effect in Intergroup Discrimination," *British Journal of Clinical Psychology* 18, no. 4 (November 1979): 371–383.

⁵⁵⁶ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 240–41.

⁵⁵⁷ Hogg, Van Knippenberg, and Rast, 240.

⁵⁵⁸ Hogg, Van Knippenberg, and Rast, 240.

⁵⁵⁹ Hogg, Van Knippenberg, and Rast, 234.

⁵⁶⁰ Korschun, "Boundary-Spanning Employees and Relationships with External Stakeholders," 618–19, 625.

seeking a way to highlight the saliency of both groups.⁵⁶¹ However, while highlighting saliency is necessary to make an association relevant, it can create conflict and competition. Group associations are most effective at influencing norms and values when that associational relationship is salient in the minds of the organization's members. Organizations can be highly salient for group identification purposes. Many studies demonstrate that people can find high value in associating with an organization, like an employer.⁵⁶² Yet, high saliency in times of threat or uncertainty generally leads to more group-focused motivations, increasing the odds of intergroup conflict.⁵⁶³

Superordinate identities may also struggle when hierarchically distinct groups are involved.⁵⁶⁴ Efforts to influence narratives by leaders from higher or more powerful groups may appear to lower group members to be an attempt by the dominant group to impose their will on the lesser.⁵⁶⁵ It would be ideal for disparate groups to hold positive views but still recognize their mutual distinctions of superiority.⁵⁶⁶ Social creativity can play a role in such an effort in the way leaders attempt to craft narratives. As seen in the case study through the actions and/or rhetoric of President Bush, Vice President Cheney, or David Addington, this analysis again demonstrates that leaders trying to push down changes to cultural norms from the top of an organization are unlikely to be effective unless each of the subgroups across the organization accepts these changes as already fitting in with their preexisting values systems.

While traditional methods in the social identity perspective may highlight the apparent gaps for seeking effective cooperation rather than competition among organizational subgroups, the Intergroup Relational Identity (IRI) theory conceived by

⁵⁶¹ See Hennessy and West, "Intergroup Behavior in Organizations," 376-79; see also Johnston and Hewstone, "Intergroup Contact," 192-94.

⁵⁶² See Korschun, "Boundary-Spanning Employees and Relationships with External Stakeholders," 612.

⁵⁶³ Doosje, Ellemers, and Spears, "Commitment and Intergroup Behaviour," 99.

⁵⁶⁴ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 237.

⁵⁶⁵ Hogg, Van Knippenberg, and Rast, 237.

⁵⁶⁶ Johnston and Hewstone, "Intergroup Contact," 193.

Hogg, Van Knippenberg, and Rast offers a valuable tool for recognizing (and appreciating) distinctions between subgroups in an organization, while still understanding the value in a superordinate identity based on symbiotic relationships between groups. IRI is still a largely conceptual theory that may provide an effective avenue for organizational influence.⁵⁶⁷ Hogg et al. suggest that leaders cannot try to gloss over intergroup biases, but rather should try to acknowledge them and account for their potential.⁵⁶⁸ IRI hinges upon a leader's ability to serve as an entrepreneur of identity, wherein a leader helps establish group identities within respective subgroups and incorporate the nature of the relationships between groups as a defining characteristic.⁵⁶⁹ They argue that effective intergroup leadership requires changing the narrative to heighten intergroup cooperation rather than competition, and they offer a unique method to do so.⁵⁷⁰

The IRI process requires creatively reframing narratives over time to focus on the cooperative relationship between groups while still allowing for distinct compatible ingroup narratives.⁵⁷¹ This model respects distinct ingroup narratives while emphasizing intergroup cooperation.⁵⁷² With a focus on collaboration, IRI does not create a situation wherein a dominant group may threaten subgroup identities. This does not require an intelligence chief to convince all subordinates that she is necessarily "one of them" to gain their trust and influence their norms; such actions have the potential for group members to perceive a blurring of superordinate and subgroup distinctions as a threat that can have negative consequences. Instead, IRI focuses on the superordinate values of the relationship between groups; for instance, IRI might suggest reframing the narrative to argue that the intelligence organization can only be effective when analysts, sworn assets, and leadership use their distinctive values and skills to execute various considerations within the

⁵⁶⁷ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 249.

⁵⁶⁸ Hogg, Van Knippenberg, and Rast, 242.

⁵⁶⁹ Hogg, Van Knippenberg, and Rast, 241–42; see also Hogg & Reid, "Social Identity, Self-Categorization, and the Communication of Group Norms," 20.

⁵⁷⁰ Hogg, Van Knippenberg, and Rast, 243–45.

⁵⁷¹ Hogg, Van Knippenberg, and Rast, 241–43.

⁵⁷² Hogg, Van Knippenberg, and Rast, 241–42.

Intelligence Cycle. From the legal advisor's perspective, IRI suggests that it is more effective to emphasize the need for a collaborative relationship between attorney and clients in an intelligence enterprise to build trust and cooperation rather than convincing analysts and sworn assets that the attorney is "one of them."

The relationship between groups becomes the connecting narrative. IRI embraces collaboration, symbiosis, and distinctions simultaneously. Much like the theory of cross-categorization, IRI calls for leaders to shepherd multiple groups toward a common, overarching goal (or goals) which naturally requires some level of group cooperation.⁵⁷³ However, unlike cross-categorization, IRI does not try to change the salient narratives of subgroups to overlap.⁵⁷⁴ The collaborative relationship between parties defines the groups, but does not define the group's distinctive identities themselves.⁵⁷⁵ IRI can build the trust of multiple groups because it does not threaten the distinct identities of any respective group or group leader.⁵⁷⁶ Instead, IRI allows for construed membership that pushes ingroup identity outward.⁵⁷⁷ Arguably, if used effectively, this method can create a more organic, horizontal method to initiate organizational change.

From the perspective of the intelligence chief who wishes to influence an agency's culture to more fully embrace a balance between security and liberty considerations, the social identity perspective argues that the top-down approach of giving edicts, as President Bush did shortly after 9/11, will produce limited long-term value. Agency members may follow through motions because they are extrinsically compelled to do so, but that does not create any intrinsic motivation to alter group norms and beliefs unless the respective ingroup members adopt the edict as consistent with their preexisting values and view the intelligence chief as sufficiently part of their ingroup to the point they can accept the chief influencing their group norms. Instead of reaching out to other groups directly, IRI calls

⁵⁷³ Hogg, Van Knippenberg, and Rast, 243.

⁵⁷⁴ Hogg, Van Knippenberg, and Rast, 241–42.

⁵⁷⁵ Hogg, Van Knippenberg, and Rast, 241–42.

⁵⁷⁶ Hogg, Van Knippenberg, and Rast, 240, 242.

⁵⁷⁷ Hogg, Van Knippenberg, and Rast, 244.

for prototypical leaders to work together in a boundary-spanning leadership coalition.⁵⁷⁸ Intergroup processes, rather than interpersonal relationships, become critical to the IRI theory.⁵⁷⁹ Next, Chapter V will outline how the IRI process can impose cultural balance between security and liberty in intelligence enterprises through a coalition of leaders.

⁵⁷⁸ Hogg, Van Knippenberg, and Rast, 241–45.

⁵⁷⁹ Hogg, Van Knippenberg, and Rast, 242.

THIS PAGE INTENTIONALLY LEFT BLANK

V. STEERING A TEAM OF TEAMS: RECRUITING PROTOTYPICAL LEADERS TO BALANCE SECURITY AND LIBERTY

This thesis began by asking how intelligence leaders should respond to increasing demands on transparency and privacy. Chapters II and III demonstrated the need for transparency, organizational support, and consent of stakeholders in creating new, aggressive intelligence programs. The case study outlined in those chapters also highlighted the dangers an organization can create for itself in prizing secrecy and downplaying stakeholder support and organizational buy-in when furthering the prevention narrative. Chapter IV emphasized the importance of leadership and the inherent difficulties in social dynamics and initiating social change. Social dynamics limit individual leaders and actors in their scope of influence. Should leaders desire to better prepare their intelligence enterprises for a transparent twenty-first century, then they should attempt to implement some variation of the IRI model within their organizations. By applying the IRI model to intelligence enterprises, particularly with a focus of better balancing security with liberty interests, intelligence officials can better prepare their organizations to consider and plan for societal privacy concerns. The IRI model builds on ideas, based in the social identity perspective, that recognize the limitations of individual subgroup leaders or a leader of a larger, superordinate organization to enact change across entire organizations. Additionally, it advocates for coalition-building partnerships among subgroup prototypical leaders to develop change within each leader's respective subgroup.

Recognizing that organizational needs vary by group and that many of the following elements are malleable, intelligence leaders intent on striking a cultural balance in security organizations should consider the development of a "team of teams" approach, which in many ways mimics efforts by General Stanley McChrystal to create more effective intelligence and operational squads in the military (catalogued in a book by the same name).⁵⁸⁰ Rather than micromanaging organizational culture change themselves,

⁵⁸⁰ See Stanley McChrystal et al., *Team of Teams: New Rules of Engagement for a Complex World* (New York: Portfolio/Penguin, 2015).

intelligence chiefs should recruit subgroup prototypical leaders to the cause of balancing security and liberty interests within their respective subgroups. This, of course, requires sensemaking awareness for an intelligence chief to understand who the appropriate ingroup prototype leaders are to recruit, and to effectively understand what subgroups comprise the organization. The top leader's responsibility in this effort is to use effective communication across the organization to set the stage for the subgroup prototypical leaders to develop support. Through the promotion of this team of teams, intelligence leaders can achieve a balance between security and liberty cultural norms by diffusing responsibilities and promoting ingroup autonomy, by establishing new forms of internal cultural oversight without creating expanding bureaucracies of oversight, by building effective educational programs, and by improved horizontal communication and transparency.

Communication and awareness play significant roles in the early stages of this recruitment process for intelligence leaders. The early stages may be the most important for the superordinate chief to establish the baseline expectations. An intelligence chief may wish to convey rhetoric using the communicative elements discussed earlier in a “public information” manner to broadly communicate an intent to ensure the proper balance between security and liberty in the intelligence enterprise's decision-making processes. However, when implementing rhetoric, leaders should start small. An effective first step—and one that is commonly proscribed as a best practice in intelligence enterprises—is to install a role focused specifically on liberty interests in the enterprise. Ideally, by Department of Justice standards, this role focuses on privacy, civil rights, and civil liberties matters on a full-time basis and has regular access to legal counsel.⁵⁸¹ The liberties-based role is valuable in that, by focusing primarily on privacy, civil rights, rule of law, and civil liberties considerations, the implementation of the role ensures at least one voice to counteract potential extremes of the prevention narrative. However, the installation of a liberties-based role by itself does little if leaders or social groups more generally closet off that position from certain aspects of the enterprise. Just as the White House short-circuited

⁵⁸¹ Global Advisory Committee, *Establishing a Privacy Officer within a Justice or Public Safety Entity: Recommended Responsibilities and Training* (Washington, DC: Department of Justice, June 2014), <https://it.ojp.gov/GIST/165/.../Final-Privacy-Officer-Function-Brochure-6-17-140.pdf>.

internal executive oversight mechanisms by preventing access to information related to Stellarwind, the mere presence of a position does not guarantee appropriate checks, nor does it influence an entire organization's culture. Group members within the intelligence agency are likely to view the liberties-based role as an outsider or external oversight mechanism when their respective ingroups become most salient. If leaders are not careful, intelligence group members may view such a role in a similar derogatory fashion as to how Alberto Gonzales and David Addington viewed the FISC—as nothing more than a roadblock.

Instead, leaders may use the liberties-based role as the initial seed to begin the culture-setting process. The liberties-based role should have open and regular access to various subgroups within the intelligence enterprise, should regularly sit in on their conversations, and should work to develop intergroup relationships with the various subgroups while conveying the message of how groups can balance security and liberty interests. This “fly on the wall” model may lead to acclimation as a starting point.⁵⁸² The liberties-based role could also engage subgroup members in dynamic, critically-thinking based educational training, particularly using scenario-based education as preparation for agency members. Group members are more likely to find relevance and value from scenario-based training rather than rote rule outlines. Ultimately, with sufficient contact and positive intergroup relations, subgroup members would benefit from the liberties-based role member as a “construed” or extended member of the ingroup.⁵⁸³ This also highlights the importance of recruiting people into liberties-based roles who demonstrate an ability to find positive solutions and common ground to garner good will and not have ingroup members view them as roadblocks. Once the organization's subgroups accept that proscriptive privacy role and the collaborative value of its message, intelligence leaders can work to expand and diffuse the sources of the balancing narrative.

⁵⁸² See Johnston and Hewstone, “Intergroup Contact,” 195–198.

⁵⁸³ See Korschun, “Boundary-Spanning Employees and Relationships with External Stakeholders,” 617-19.

The installation of the liberties-based role is not part of the IRI model recommendations—it is a precursor. The social identity perspective and the IRI model highlight the limitations of an individual person or a small group in truly enacting cultural change across a broad intelligence enterprise, as evidenced by the War Council’s failures; instead of enacting true ingroup narrative changes, the liberties-based role serves as an internal oversight mechanism that other groups, when conflict arises, will likely view as part of an outgroup whose message is mitigated by his or her outgroup position. The evidence suggests that any desired cultural change to balance the equities of security and liberty should come from within the collective subgroups of the organization. The IRI model suggests that for an intelligence leader to effectively spread a culture that seeks to balance liberty and security, the leader can recruit subgroup prototypical leaders to the cause by emphasizing the value and importance of the cultural norm. Obtaining the support of these subgroup leaders is critical because they will essentially take on an additional responsibility of part-time liberties-based role members, in that those leaders will need to ensure reasonable analyses of liberty and security interests take place.

This only works if those leaders appreciate and subscribe to the organizational value of the responsibility. Ideally, through the recruitment process, an intelligence leader could develop a coalition of subgroup prototypical leaders who work together to handle and discuss issues related to balancing security and liberty within the organization from various symbiotic perspectives. This does not mean that the leader must convert the subgroup prototypes into staunch privacy advocates. The relevant considerations in balancing security and liberty interests may well change given the context presented. This model expects a diverse variety of perspectives on how to balance security and liberty to best represent society’s diversity of views; in return, the model simply asks its actors to consider how that balancing should occur, along with considerations for the ramifications of the actors’ choices. These leaders may accomplish this balancing through regular discussions about how new initiatives affect that balance, round tabling how external stakeholders, like the media or oversight bodies, might view intelligence efforts, or regularly reviewing the enterprise’s activities in the greater context of societal considerations on privacy. Leaders should recruit members to the prototype coalition from

all of the organization's relevant subgroups. This coalition diffuses the responsibility of promoting new cultural norms from a singular organizational leader to a group of leaders more closely situated to a significantly larger percentage of the organization's members.

As the balancing norms spread, the leaders' goal should be to diffuse responsibility for balancing considerations even further down to line-level assets, eventually reaching a point where every member intrinsically feels a responsibility to consider how their actions play into the balancing of the equities based on their sense that it is an ingroup norm. This should not be a radical notion as personnel regularly engage in similar analytical calculations for matters such as time allocation, resource allocation, and threat priorities. This is not to suggest that spreading responsibility and considerations of balancing the equities will necessarily lead to the elimination of miscalculations by agencies moving forward, but at minimum it would prepare agency personnel at all levels to critically analyze how external stakeholders, like legislative overseers or the public, will perceive their actions. From the social identity perspective, this diffusion of responsibility will better prepare intelligence enterprises to work with external stakeholders and increase members' stability, certainty of purpose, and value within intelligence enterprises, leading to higher morale and efficacy. In effect, this model should mitigate the instability and cycles of risk aversion found in intelligence-based social groups, notably within the IC after major abuses and prior to significant intelligence failures.

Various subgroups within an intelligence enterprise contribute distinctly to the balancing of considerations between security and liberty. Attorneys can provide legal guidance and implications for certain excesses while analysts and sworn assets can detail effective investigative or intelligence techniques. Some groups may be more risk averse while others more aggressive in pressing for security. Ultimately, a two-way symmetrical dialogue among the prototype coalition should develop a balanced framing for intelligence efforts that draws on analysis and evidence-based justifications rather than gut instincts, fear, or raw emotions. The prototype coalition plays a significant role in developing the overarching, superordinate norm throughout the organization of an articulable balancing between security and liberty. The prototypical leaders that intelligence officials recruit will have many roles to play in implementing the necessary change within an organization. One

of them is to serve as a “boundary-spanner,” because their role in the prototype coalition requires cooperation with members of other organizational subgroups.⁵⁸⁴ Boundary-spanners should act consistently with their ingroup values when engaging outgroup members rather than engaging others based on interpersonal relationships.⁵⁸⁵ In the leadership coalitions, leaders represent their groups instead of themselves.⁵⁸⁶ The alternative—cooperation based on interpersonal relationships—will likely result in social groups mitigating the value of those perceived relationships as inconsistent with group norms.⁵⁸⁷ Leadership coalition members should work “to overcome this human propensity and to bridge intergroup differences in order to build cooperation and collaboration among members of two or more groups in the service of a single vision and a sense of purpose.”⁵⁸⁸ If leaders engage the coalition as respective ingroup group members, over time follower ingroup members will come to see the interactions of their group leaders with other group leaders as eliminating preconceived outgroup stereotypes that may denigrate a desired mutual purpose.⁵⁸⁹ Thus, attorneys should represent their ingroup’s legal values while sworn assets should represent their ingroup’s investigative values, and neither the attorney nor the sworn asset should rely solely on interpersonal relationships in engaging the other. The role of the intelligence chief in this process, as well as the role of the prototypical ingroup leaders, is to clearly articulate the mutually beneficial relationship of collaborative efforts to followers.⁵⁹⁰ The best method to articulate these efforts would likely be through the “press agency” or “public information” models.⁵⁹¹

⁵⁸⁴ Korschun, “Boundary-Spanning Employees and Relationships with External Stakeholders,” 612.

⁵⁸⁵ See Johnston and Hewstone, “Intergroup Contact,” 195–96, 198; Hogg, Van Knippenberg, and Rast, “Intergroup Leadership in Organizations,” 241.

⁵⁸⁶ Hogg, Van Knippenberg, and Rast, “Intergroup Leadership in Organizations,” 242.

⁵⁸⁷ See Johnston and Hewstone, “Intergroup Contact,” 195–198

⁵⁸⁸ See Hogg, Van Knippenberg, and Rast, “Intergroup Leadership in Organizations,” 236.

⁵⁸⁹ Hogg, Van Knippenberg, and Rast, 242.

⁵⁹⁰ Hogg, Van Knippenberg, and Rast, 241–42.

⁵⁹¹ See Farmer, Slater, and Wright, “The Role of Communication in Achieving Shared Vision Under New Organizational Leadership,” 232.

One purpose of the leadership coalition is to engage the group's respective leaders in dialogue, particularly for new initiatives. When engaged, these leaders bring their respective positions, perspectives, and arguments as peers, engaging in a dialogue based in some level of evidence and reason. These discussions should be hierarchically flat, meaning no person involved uses any power dynamics or position titles to stifle the discussions. Through such discussions, leaders operate in transparency as they articulate justification for choices and beliefs while subjecting themselves to counterarguments and constructive criticism.⁵⁹² In discussing security-based considerations, each member of the prototype coalition should also interpret and present the liberty-based ramifications from his or her ingroup's perspective. For this thought exercise, consider Mr. Comey and Director Hayden from the case study partaking in this process. They may be two of several in a leadership coalition discussion on a new collection idea. Both men could bring their articulable opinions to the table and engage in a hierarchically-flat dialogue. The ensuing discussion would likely parallel, or at least touch on many stakeholder concerns represented through various leader viewpoints, thereby better preparing leadership for those issues. Noticeably absent from this hypothetical is the presence of an Addington-like character, whose tactics have no place in constructive dialogues.

Beyond the substance that may come from those discussions, the value of prototypical leadership coalitions is in how respective ingroup members view the interactions of their prototypical leaders; if members view norms valuing intergroup relations between leaders based on a mutual interest in furthering a reasonable balance of the equities, then ingroup members are more likely to mirror those values and behaviors. As followers see their own respective prototypical leaders engage in transparent and considerate discussions about organizational activities, those followers will internalize these traits. Through the leadership coalition's use of effective discussions, subgroup members will likely adopt lessons learned from those discussions over time and apply similar tools in their engagement. In effect, the respective leaders take back to their groups

⁵⁹² An excellent example outside of the intelligence context is that of the "Braintrust" meetings created at Pixar Animation to facilitate creative story development of movies (see Catmull, *Creativity, Inc.*, 86–107).

the work of the coalition.⁵⁹³ This is how the superordinate value system spreads. No individual leader or actor is a lynchpin for success; rather, all the included actors are ultimately necessary as they spread the message across the entirety of an organization.

This model also has the added benefits of improving intergroup cooperation, communication skills, and autonomy. If used effectively, the IRI model can lead to a “team of teams” who work more effectively among their respective ingroups and along intergroup relationships. By mirroring the communicative efforts of the leadership coalition’s balancing discussions, leaders can use similar tools to improve critical thinking analysis and situational awareness. This may improve the organization’s resources for intelligence efforts more generally.

The long-term goal of this model is to improve the efficacy of intelligence enterprises to create the necessary resources for cultural change for a singular issue of critical importance: ensuring a reasonable balancing of security and liberty interests. This thesis argues that by using the above-noted tools to influence organizational change, leaders can move their organizations closer to the goal of balance between security and liberty interests while at the same time improving the efficacy of their intelligence resources more generally. One of the ways in which the use of the IRI theory can accomplish these dual missions is through the development of “high identifiers.” If the intelligence leader can establish that one of the organization’s values is to reasonably balance the equities of security and liberty, high identifiers will adopt that value as their own over time. When group saliency is high, people are more likely to act consistently with group norms than when the group is less important.⁵⁹⁴ Those with greater ingroup identification are more likely to show behaviors consistent with group norms and expectations than those with weaker group commitment.⁵⁹⁵ Low identifiers, conversely, are harder to predict, because they tend to focus more on self-serving, personal

⁵⁹³ Hogg, Van Knippenberg, and Rast, “Intergroup Leadership in Organizations,” 244.

⁵⁹⁴ Doosje, Ellemers, and Spears, “Commitment and Intergroup Behaviour,” 99.

⁵⁹⁵ Doosje, Ellemers, and Spears, 84, 89.

motivations.⁵⁹⁶ High identifiers are also more likely to “stick with their team” until the bitter end.⁵⁹⁷ They tend to more overtly and consistently display group prototype characteristics.⁵⁹⁸ The IRI model increases group saliency by highlighting the importance of respective ingroups through their intergroup relationships, thereby making the group’s existence and values critical; thus, in the context of balancing the equities of security and liberty, leaders should highlight how various subgroups are important and must cooperate to effectively achieve that balance. Therefore, the highlighting of ingroup saliency in a positive manner for intergroup collaboration can have the spillover effect of increasing personnel morale and purpose.

Leaders should want more high identifiers among their ranks. Low identifiers are less likely to seek resolutions to group issues if they do not improve the subgroup’s hierarchical social status, while high identifiers are more likely to seek group resolutions regardless of any external competitive considerations.⁵⁹⁹ Low identifiers tend to act more strategically to attain what they perceive as improving their own social status through association; alternatively, high identifiers act more commonly for the sake of the group because they take self-value from the group’s enhancement, since high identifiers more directly tie their self-value to the group’s identity.⁶⁰⁰ The shared group experiences that result from this IRI method can create an effective superordinate social identity, potentially further creating more high identifiers in intelligence enterprises.⁶⁰¹ These efforts better prepare intelligence enterprises for collaboratively working with external stakeholders, which is critical for optimum efficacy, as discussed in Chapters II and III.

⁵⁹⁶ Doosje, Ellemers, and Spears, 95.

⁵⁹⁷ Doosje, Ellemers, and Spears, 95.

⁵⁹⁸ Doosje, Ellemers, and Spears, 85.

⁵⁹⁹ Doosje, Ellemers, and Spears, 94.

⁶⁰⁰ Doosje, Ellemers, and Spears, 95.

⁶⁰¹ See Doosje, Ellemers, and Spears, 85–86.

A. REACHING OUT TO STAKEHOLDERS

The case study in this thesis highlights how government protectors risk alienating external stakeholders when they foster the prevention narrative. Intelligence enterprises need the consent of the people they serve, and this may come in many forms: one may be through the will of legislators; another may be support (even tacitly) from advocates seeking security and those seeking the protection of civil liberties. The intelligence enterprise cannot successfully exist without the consent and support of the public.⁶⁰² The case study also makes clear that intelligence efforts do not operate in a vacuum, and that officials must work collaboratively with external stakeholders to operate at peak strength. Like the subgroup organizational social dynamics outlined above, the social identity perspective and the IRI model provide valuable insights into how intelligence enterprise leaders can move forward in building partnerships with external stakeholders.

It always important to value an organization's relationships with external stakeholders, but this process should begin by focusing on an organization's internal cultural health. The process should ideally begin prior to concerted efforts to initiate new collaborative efforts with external stakeholders, or otherwise intelligence leaders should at least have a sense that their enterprise understands the necessity of working collaboratively with external stakeholders. Priming the organizational culture to prepare for reframing intergroup relationships is likely to improve the efficacy of refocused efforts in establishing deeper collaboration with external partners. At least in the dynamics of organizational subgroup relationships, the superordinate organizational identity can serve as a familiar frame for reference. The intergroup dynamics between an intelligence enterprise and a legislative oversight panel or an external advocacy group are likely to be far more competitive, according to the social identity perspective, than a relationship between a sworn asset and a group of analysts. In the relationship with an advocacy group, extended contact between persons and/or groups is likely to lower hostility on either an interpersonal or intergroup level. In the legislative oversight relationship, there is less opportunity for extended contact on a day-to-day basis, and so competition between groups will increase

⁶⁰² See Lincoln, "Lincoln's Reply," 128.

as conflict arises. Unlike the sworn asset and the analysts, members of an intelligence agency are less likely to feel a sense of shared identity on any level with a perceived hostile media, advocacy organizations like the ACLU, or oversight committees. Yet, these same groups can give intelligence enterprises exponentially more effective authority to operate with consent, so it is the responsibility of intelligence leaders to seek collaborative relationships with these stakeholders when possible.

According to the social identity perspective, when differences between groups are salient, competition between groups will drive conflict.⁶⁰³ However, Korschun argues that ingroup/outgroup relationships can be more productive when ingroup members view the outgroup as extended members of the ingroup.⁶⁰⁴ For example as Korschun notes, the bevy of Apple fan groups, blogs, and supporters who wait in line for weeks before the sale of a new iPhone may not be an ingroup member of the Apple Corporation, but such people may be viewed by Apple employees as part of the extended ingroup who share salient values.⁶⁰⁵ To establish a similar relationship (though surely not as doting as the Apple example), intelligence organizations would need to develop a collectivist nature based on shared values, such as “we are all in this together.”⁶⁰⁶ This is surely easier when the internal culture of an intelligence enterprise already subscribes to a similar ideal.

Using a collectivist orientation, ingroup members who can view external stakeholders as having a “construed” ingroup membership can be valuable for finding a perspective of nominal ingroup association through shared identity.⁶⁰⁷ Collectivist organizational identities are more likely to seek cooperation with stakeholders, as they are more likely to view those stakeholders as valuable assets.⁶⁰⁸ If an intelligence leader were able to establish an internal culture of collaboration and a reasonable balance between

⁶⁰³ Korschun, “Boundary-Spanning Employees and Relationships with External Stakeholders,” 616.

⁶⁰⁴ Korschun, 617–19.

⁶⁰⁵ Korschun, 617.

⁶⁰⁶ Korschun, 625; Frank Mols, “What Makes a Frame Persuasive? Lessons from Social Identity Theory,” *Evidence & Policy* 8, no. 3 (August 2012): 331.

⁶⁰⁷ Korschun, 617–19.

⁶⁰⁸ Korschun, 621.

security and liberty, the extension of this culture to other external stakeholders could be more suggestable. Similar to internal leadership coalitions where respective members may hold different viewpoints on an appropriate balance between security and liberty interests, intelligence agencies and external stakeholders can still agree on a need for balance while viewing the appropriate balance differently. While intelligence agencies may not always like the end results of those debates, those debates will lead to a better understanding of public sentiment and, ultimately, a more solid foundation of public consent from which to operate.

The IRI model also increases the likelihood of effective cultural change among collaborative partners. There is no need for intelligence leaders to suggest members of advocacy groups and the intelligence enterprise are of the same ilk; one supposes members of both groups would scoff at such attempts at narrative framing, even if both groups do want similar goals of balanced liberty and security but may see very different perspectives on how to manifest those goals. Even if the parties were amenable to such a superordinate identity, it would likely falter in times of conflict. The IRI model provides a method for retaining the distinct identities of an intelligence enterprise and external stakeholders like advocacy groups, media outlets, and oversight groups. Using a similar “team of teams” model as outlined earlier in this chapter, organizational prototypical leaders could establish group-based symbiotic relationships with these external partners that highlight the need for intelligence agencies to engage external groups to obtain the consent of the governed. In doing so, leaders could advocate a narrative framing that highlights the need for a shared consensus on what is appropriate activity. Calling back to General Hayden’s notion of “translucence,” such partnerships could allow external groups a better understanding of how intelligence enterprises operate without releasing sensitive information that would debilitate efficacy; the intelligence agency in return would be able to operate from a more stable foundation based on shared consent and understanding.⁶⁰⁹ That stable foundation would improve the sense of certainty that social groups desire, and ultimately improve the

⁶⁰⁹ See Hayden, *Playing to the Edge*, 424.

likelihood that intelligence enterprises will not face sudden external threats like the executive branch saw in the case study examined in this thesis.

Again, the intelligence leader who impresses upon agency membership the importance of working with external stakeholders can only influence the narrative to an extent. Social dynamics of group relationships require more than purely interpersonal relationships to be consistently effective. Based on conflicting evidence, it seems that interpersonal contact alone is insufficient to soften intergroup conflicts.⁶¹⁰ Even with significant personal contacts, the likelihood of intergroup conflict remains high when an outgroup threatens an ingroup's identity, purpose, or distinctiveness.⁶¹¹ The IRI model expects that organizational prototypes who work with external group prototypes do so while projecting group-based values to highlight the intergroup nature of the interactions. Doing so may provide a basis for improved cooperation and, as a result, improved efficacy.

⁶¹⁰ See Johnston and Hewstone, "Intergroup Contact," 195–96, 198.

⁶¹¹ Johnston and Hewstone, 198.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Americans arguably expect more today from their intelligence officials than at any time in recent memory.⁶¹² Not only do citizens expect intelligence organizations to be more transparent than during the Cold War, but intelligence officials must protect the public from a more diverse array of threats than ever before as terrorist organizations continue to splinter and homegrown violent extremists and lone offenders comprise a larger percentage of domestic terrorist activities.⁶¹³ Some might argue that these difficulties are precisely why intelligence leaders must act more aggressively. The purpose of this thesis does not conflict with that notion; instead, this thesis asks the corollary question of how that can be done in a method that maintains a societally-approved balancing of security and liberty interests, thereby maintaining the support of stakeholders and the public writ large while also ensuring efficacy of intelligence efforts.

Stakeholder support is important because intelligence organizations operate most effectively when they have the support of their respective stakeholders, including the legislative bodies who give intelligence organizations their authorities, the courts who often review intelligence activities, the media who frame public narratives about intelligence activities, and, most importantly, the public from whom all authority for intelligence activities derive in a democratic society. The pages of this thesis contain the names of those who came from the ranks of federal executive organizations and who recognized the need to engage in politically sustainable intelligence activities, even if these individuals may have had starkly different interpretations of what was “politically sustainable.”⁶¹⁴ From Michael Hayden to Jack Goldsmith to John Yoo, many people who

⁶¹² See Richards, “Intelligence Dilemma,” 761.

⁶¹³ *Current Terrorist Threat to the United States*, Senate Select Committee on Intelligence, 114th Cong., 1st sess. (statement of Nicholas J. Rasmussen, director, National Counterterrorism Center, February 12, 2015), 2–4, https://www.dni.gov/files/NCTC/documents/news_documents/Current_Terrorist_Threat_to_the_United_States.pdf.

⁶¹⁴ See Hayden, *Playing to the Edge*, 426.

were involved in this case study understand the need to ensure stakeholder support for their activities, or alternatively suffer the consequences.

The social identity perspective makes clear how harmful conflicts between organizational subgroups and among intelligence stakeholders are to organizational health. The case study highlighted in Chapters II and III discussed the apparent dangers for social groups who embrace the “prevention at all costs” narrative. This prevention narrative can come from perceived ingroup inadequacies or through perceived outgroup threats. In the twenty-first century, intelligence officials must be cognizant of the pitfalls awaiting organizations that attempt to unilaterally and aggressively enhance their capabilities in an all-out effort to prevent another terrorist attack. The case study highlighted several of those consequences, which, in their totality, consistently threatened intelligence enterprises with a significant loss of capabilities. Those losses may come from stakeholders who remove an intelligence agency’s authorities to act, from stakeholders who take away intelligence agency resources, from stakeholders who dramatically enhance their own involvement to rebut agency overreach, or from stakeholders who stop cooperating because of a lack of trust. Intelligence abuses may also lead to financial damages, as referenced in Chapter IV.

Internally, social groups who foster the prevention narrative also risk significant organizational harms. Conflict between subgroups weakens the superordinate organization’s cohesion when people retreat into closer subgroups that compete with each other.⁶¹⁵ These competitions ignite a recurring cycle of conflict. As people rely so heavily on their group associations to form their self-identities, the social identity perspective is a useful lens through which to view social dynamics in and around organizations. In the case study, this thesis highlighted the devolving relationships between social groups as the War Council entrenched itself in the framings of the prevention narrative; the thesis also demonstrated the extremes to which members of other social groups went to counteract perceived devolving norms, to include threats to resign *en masse* or leaks of classified information in perceptively dire circumstances.

⁶¹⁵ See Ellemers, De Gilder, and Haslam, “Motivating Individuals and Groups at Work,” 462–64.

By focusing on the social identity perspective to analyze the case study, this thesis makes clear that effective leadership is a critical component to strong organizations.⁶¹⁶ Leadership does not equal raw, coercive positional power.⁶¹⁷ Instead, leadership of a group comes from the group's acceptance and support.⁶¹⁸ According to the social identity perspective, a prototypical leader is an individual who most strongly identifies with a group's perceived vision of the ideal group member, who can then take that correlation and use the group's acceptance to influence group norms.⁶¹⁹ Those in positions of power in organizations must recognize the distinction between power and leadership, and strive to use leadership qualities to positively influence their organization and their surrounding stakeholders.

The case study discussed in Chapters II and III suggests that those with the most power in the White House after 9/11—namely, President Bush, Vice President Cheney, and Counsel to the Vice President David Addington—failed to recognize the distinction between power and leadership when they sought to implement aggressive, norm-changing intelligence programs. Their reliance on unilateral decisions and purely coercive power led to a failure of organizational acceptance. This resulted in significant conflict when their orders deviated from previously-held group norms. The case study also suggests that those policymakers unnecessarily created strife through their tactics; they could have just as easily obtained similar authorizations and resources through a persuasive campaign to garner support from stakeholders within the IC and from external stakeholders. Instead, those policymakers risked the institutional efficacy of the executive branch and the IC's intelligence capabilities with harms that have had continuing ramifications beyond their supposed resolutions.⁶²⁰

⁶¹⁶ See Hogg, "A Social Identity Theory of Leadership," 193.

⁶¹⁷ Hogg, 194.

⁶¹⁸ See Terry, Hogg, and Duck, "Group Membership, Social Identity, and Attitudes," 301.

⁶¹⁹ Hogg, "A Social Identity Theory of Leadership," 194.

⁶²⁰ See Edgar, *Beyond Snowden*, 41.

Looking forward, this thesis lays a foundation upon which future researchers and policy-makers may build. The central theme of this foundation is determining how to influence the cultures of security-based intelligence enterprises to effectively balance security and liberty interests, including privacy rights, civil rights, civil liberties, and rule of law considerations. Within these pages are broad strokes meant to provide a generalized outline that leaders can apply based on individualized organizational needs. Through the IRI theory, this thesis provides one potential method for improving the ability of intelligence enterprises to balance the equities between security and liberty. The IRI theory is only one possible tool to enact this goal, but IRI is thoroughly steeped in the social identity perspective discussed in this thesis. IRI is distinct in the field of social identity in that it focuses on the necessity of intergroup relations as a defining characteristic of groups' identities.⁶²¹ This method recognizes the need to grasp social dynamics when seeking to institute cultural change and uses those forces to the leader's advantage. Specifically, this application of the IRI Theory compels an organizational chief to combine a "press agency" or "public information" model communication technique while recruiting and fostering a leadership coalition of organizational subgroup prototypical leaders, or a leadership coalition.⁶²² Those leaders set the stage for social influence among themselves and among their respective ingroups.⁶²³

The job of the leadership coalition is to work among its members to determine an appropriate balancing of security and liberty interests in intelligence efforts. That balancing should be the result of candid, engaging discussions involving a variety of perspectives based in articulable concerns. Through that dialogue, the leadership coalition can mirror stakeholder concerns over intelligence and better prepare the organization for those stakeholder interests. Moreover, when members of the leadership coalition engage each other as members of their respective ingroups, those leaders set the stage for their ingroup

⁶²¹ Hogg, Van Knippenberg, and Rast, "Intergroup Leadership in Organizations," 241–42.

⁶²² See Hogg, Van Knippenberg, and Rast, 243–45.

⁶²³ See Hogg, Van Knippenberg, and Rast, 244; see also Hogg, "A Social Identity Theory of Leadership," 187.

followers to act in kind.⁶²⁴ Thus, IRI has the additional benefit of potentially lessening intergroup conflict.

Use of the IRI model can also improve relationships with external stakeholders. By using a similar model to the internal leadership coalition concept, intelligence agencies can improve “translucence” with public stakeholders and better understand their concerns over government surveillance while maintaining necessary levels of secrecy.⁶²⁵ Improved relationships with external stakeholders enable intelligence leaders to better understand where the consent of the governed may lie. Using the IRI model, intelligence officials can focus on framing collective values of an intelligence enterprise and its stakeholders while still respecting different perspectives.⁶²⁶ Conversely, an ingroup that fosters the prevention narrative can lead to flippant mitigation of outgroup stakeholder concerns as evidenced in the case study.⁶²⁷ These actions tend to only inflame group distinctions, continuing cycles of conflict. As a result, intelligence officials have less understanding about what external stakeholders may support.

Moving forward, application of the IRI theory to an intelligence enterprise to better balance security and liberty interests requires real-world testing. It is, at this point, a theoretical concept of change, though it is a concept many intelligence officials who read this work will likely recognize as having merit. While the IRI model is purely abstract today, interested persons can take this model (or a relevant variant) and apply it in a real-time scenario. Through effective testing of this social psychological model, researchers and practitioners can improve upon this foundational basis to determine the most effective steps for limiting the threats of the prevention narrative.

By working with external stakeholders and fostering an internal organizational culture that seeks to reasonably balance security and liberty interests, officials lessen the

⁶²⁴ Hogg, Van Knippenberg, and Rast, 244.

⁶²⁵ See Hayden, *Playing to the Edge*, 424.

⁶²⁶ Hogg, Van Knippenberg, and Rast, 240.

⁶²⁷ For examples, see John Yoo’s dismissals of outgroup concerns (Yoo, *War by Other Means*, 21, 76).

likelihood that stakeholders will one day question and scrutinize their actions for potential abuses of authority or violations of stakeholder expectations. Officials can also use these concepts to prevent many of the dire scenes of social conflict outlined in the case study.⁶²⁸ Ultimately, using social identity-based models like the IRI theory, intelligence officials can better prepare their organizations to understand what might be out of bounds for their organizations, what the organization's stakeholders might allow in times of necessity, and what exactly constitutes "playing to the edge" in their areas of responsibility.

⁶²⁸ For examples, see Comey, *A Higher Loyalty*, 87–90; see also Edgar, *Beyond Snowden*, 46.

APPENDIX. TABLE SOURCES

The information listed in “Table 1: Timeline of Major Events In the Case Study” is found in the following sources: The National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: Norton, 2004); Timothy Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (Washington, DC: Brookings Institution Press, 2017); Michael V. Hayden, *Playing to the Edge: Intelligence in the Age of Terror* (New York: Penguin Books, 2016); James Comey, *A Higher Loyalty: Truth, Lies, and Leadership* (New York: Flatiron Books, 2018); Charlie Savage, *Power Wars: Inside Obama’s Post-9/11 Presidency* (New York: Little, Brown and Company, 2015); Department of Justice, *A Review of the Department of Justice’s Involvement with the President’s Surveillance Program* (Washington, DC: Department of Justice, 2009), <https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf>; James Risén and Eric Lichtblau, “Bush Lets U.S. Spy on Callers Without Courts,” *New York Times*, December 16, 2005, <https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>; David Sanger, “Bush Says He Ordered Domestic Spying,” *New York Times*, December 18, 2005; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107–56, 107th Cong., 1st sess. (October 21, 2001); Protect America Act of 2007, Public Law 110–55, 110th Cong., 1st sess. (August 5, 2007): 552–57; Foreign Intelligence Surveillance Act of 1978 Amendments Act (FISA Amendments Act) of 2008, Public Law 110–261, U.S. *Statutes at Large* 122 (2008): 2436–478, codified at U.S. *Code* 50 (2015), §§ 1801 et seq.

The information listed in “Table 2: Recurring Individuals from the Case Study” is found in the following sources: Michael V. Hayden, *Playing to the Edge: Intelligence in the Age of Terror* (New York: Penguin Books, 2016); Jack Goldsmith, *The Terror Presidency: Law and Judgment Inside the Bush Administration* (New York: W.W. Norton & Company, 2007); James Comey, *A Higher Loyalty: Truth, Lies, and Leadership* (New York: Flatiron Books, 2018); Charlie Savage, *Power Wars: Inside Obama’s Post-9/11 Presidency* (New York: Little, Brown and Company, 2015); Department of Justice, *A Review of the Department of Justice’s Involvement with the President’s Surveillance Program* (Washington, DC: Department of Justice, 2009), <https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf>.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- American Civil Liberties Union. “Raza v. City of New York—Settlement FAQ.” Accessed July 9, 2018. <https://www.aclu.org/other/raza-v-city-new-york-settlement-faq>.
- Anderson, Donald L. “What You’ll Say Is...: Represented Voice in Organizational Change Discourse.” *Journal of Organizational Change Management* 18, no. 1 (2005): 63–77.
- Anderson, Scott R., and Benjamin Wittes. “Climate Change is Real at the FBI—and Here is the Data to Prove It.” *Lawfare* (blog). July 15, 2018, <https://www.lawfareblog.com/climate-change-real-fbi-and-here-data-prove-it>.
- Apuzzo, Matt, and Adam Goldman. *Enemies Within: Inside the NYPD’s Secret Spying Unit and Bin Laden’s Final Plot Against America*. New York: Touchstone, 2013.
- Ashcroft, John. *Never Again: Securing America and Restoring Justice*. New York: Center Street, 2006.
- Bakhtin, Mikhail. “Discourse in Dostoevsky.” In *Problems of Dostoevsky’s Poetics*, edited and translated by Caryl Emerson, 181–269. Minneapolis, MN: University of Minnesota Press, 1984.
- . “Toward a Methodology for the Human Sciences.” In *Speech Genres and Other Late Essays*, edited by Caryl Emerson and Michael Holquist, translated by Vern W. McGee, 159–72. Austin, TX: University of Texas Press, 1986.
- Bazan, Elizabeth B., *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*. CRS Report No. RL30465. Washington, DC: Congressional Research Service, 2004. <https://fas.org/irp/crs/RL30465.pdf>.
- Best, Samuel J., Brian S. Kreuger, and Shanna Pearson-Merkowitz. “Al Qaeda Versus Big Brother: Anxiety About Government Monitoring and Support for Domestic Counterterrorism Policies.” *Political Behavior* 34, no. 4 (December 2012): 607–25.
- Brannan, David, Kristin Darken, and Anders Strindberg. *A Practitioner’s Way Forward: Terrorism Analysis*. Salinas, CA: Agile Press, 2014.
- Brown, Rupert J., and John C. Turner. “The Criss-Cross Categorization Effect in Intergroup Discrimination.” *British Journal of Clinical Psychology* 18, no. 4 (November 1979): 371–383.

- C-SPAN. “Less Safe, Less Free: The ‘Preventive Paradigm’ and the War on Terror.” Video, 1:55, September 25, 2007, <https://www.c-span.org/video/?201188-1/less-safe-free>.
- Catmull, Ed. *Creativity, Inc.: Overcoming the Unseen Forces that Stand in the Way of True Inspiration*. New York: Random House, 2014.
- Comey, James. *A Higher Loyalty: Truth, Lies, and Leadership*. New York: Flatiron Books, 2018.
- . “Intelligence Under the Law.” 10 *Green Bag* 2D 439 (May 2005).
- Czarniawska, Barbara, and Bernward Joerges. “Travel of Idea.” In *Translating Organizational Change*, edited by Barbara Czarniawska and Guje Sevón, 13–48. Berlin: Walter de Gruyter & Co., 1996.
- Department of Justice. *A Review of the Department of Justice’s Involvement with the President’s Surveillance Program*. Washington, DC: Department of Justice, 2009. <https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf>.
- Donohue, Laura K. *The Future of Foreign Intelligence*. New York: Oxford University Press, 2016.
- Doosje, Bertjan, Naomi Ellemers, and Russell Spears. “Commitment and Intergroup Behaviour.” In *Social Identity*, edited by Naomi Ellemers, Russell Spears, and Bertjan Doosje, 84–106. Oxford: Blackwell, 1999.
- Dragu, Tiberiu. “Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention.” *The American Political Science Review* 105, no. 1 (February 2011): 64–78.
- Dutton, Jane E., and Susan E. Jackson. “Categorizing Strategic Issues: Links to Organizational Action.” *Academy of Management Review* 12, no. 1 (January 1987): 76–90.
- Dycus, Stephen, William C. Banks, Peter Raven-Hansen, and Stephen I. Vladeck, eds. *Counterterrorism Law*. 3rd ed. New York: Wolters Kluwer, 2016.
- Edgar, Timothy. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, D.C.: Brookings Institution Press, 2017.
- Ellemers, Naomi, Dick De Gilder, and S. Alexander Haslam. “Motivating Individuals and Groups at Work: A Social Identity Perspective on Leadership and Group Performance.” *Academy of Management Review* 29, no. 3 (July 2004): 459–78.
- Etzioni, Amitai. “NSA: National Security vs. Individual Rights.” *Intelligence and National Security* 30, no. 1 (2015): 100–36.

- Farmer, Betty A., John W. Slater, and Kathleen S. Wright. "The Role of Communication in Achieving Shared Vision Under New Organizational Leadership." *Journal of Public Relations Research* 10, no. 4 (1998): 219–35.
- Fiol, C. Marlene, Michael G. Pratt, and Edward J. O'Connor. "Managing Intractable Identity Conflicts." *Academy of Management Review* 34, no. 1 (January 2009): 32–55.
- Global Advisory Committee. *Establishing a Privacy Officer within a Justice or Public Safety Entity: Recommended Responsibilities and Training*. Washington, DC: Department of Justice, June 2014, <https://it.ojp.gov/GIST/165/.../Final-Privacy-Officer-Function-Brochure-6-17-140.pdf>.
- Goldsmith, Jack. "Interview Jack Goldsmith." PBS Frontline. August 22, 2007. <https://www.pbs.org/wgbh/pages/frontline/cheney/interviews/goldsmith.html>.
- . *The Terror Presidency: Law and Judgment Inside the Bush Administration*. New York: W.W. Norton & Company, 2007.
- Gonzales, Alberto. "Correspondence Regarding Foreign Intelligence Surveillance Court Order." Letter to the Honorable Patrick Leahy and the Honorable Arlen Specter, January 17, 2007, <https://www.documentcloud.org/documents/1018118-alberto-gonzales-ppsp-letter.html>.
- . "Remarks to the American Bar Association Standing Committee on Law and National Security." Presentation in Washington, DC, February 24, 2004. <https://fas.org/irp/news/2004/02/gonzales.pdf>.
- Gould, Jon B. "Playing with Fire: The Civil Liberties Implications of September 11th." *Public Administration Review* 62, no. s1 (September 2002): 74–79.
- Greenaway, Katharine H., Ruth G. Wright, Joanne Willingham, Katherine J. Reynolds, and S. Alexander Haslam. "Shared Identity is Key to Effective Communication." *Personality and Social Psychology Bulletin* 41, no. 2 (February 2015): 171–82.
- Harris, Shane. *The Watchers: The Rise of America's Surveillance State*. New York: Penguin Press, 2010.
- Havermans, Liselore A., Anne Keegan, and Deanne N. Den Hartog. "Choosing Your Words Carefully: Leaders' Narratives of Complex Emergent Problem Resolution." *International Journal of Project Management* 33, no. 5 (July 2015): 973–84.
- Hayden, Michael V. *The Assault on Intelligence: American National Security in an Age of Lies*. New York: Penguin Press, 2018.

- . *Playing to the Edge: Intelligence in the Age of Terror*. New York: Penguin Books, 2016.
- . “What American Intelligence & Especially the NSA Have Been Doing to Defend the Nation.” Address to the National Press Club, Washington, DC, January 23, 2006. <https://fas.org/irp/news/2006/01/hayden012306.html>.
- Hennessy, Josephine, and Michael A. West. “Intergroup Behavior in Organizations: A Field Test of Social Identity Theory.” *Small Group Research* 30, no. 3 (June 1999): 361–82.
- Hobbes, Thomas. *Leviathan*. Baltimore: Penguin Books, 1968.
- Hogg, Michael A. “A Social Identity Theory of Leadership.” *Personality and Social Psychology Review* 1, no. 3 (August 2001): 184–200.
- Hogg, Michael A., and Craig McGarty. “Self-Categorization and Social Identity.” In *Social Identity Theory: Constructive and Critical Advances*, edited by Dominic Abrams and Michael A. Hogg, 10–27. New York: Springer-Verlag, 1990.
- Hogg, Michael A., and Barbara A. Mullin. “Joining Groups to Reduce Uncertainty: Subjective Uncertainty Reduction and Group Identification.” In *Social Identity and Social Cognition*, edited by Dominic Abrams and Michael A. Hogg, 249–79. Oxford: Blackwell, 1999.
- Hogg, Michael A., and Scott A. Reid. “Social Identity, Self-Categorization, and the Communication of Group Norms.” *Communication Theory* 16, no. 1 (February 2006): 7–30.
- Hogg, Michael A., and Deborah J. Terry. “Social Identity and Self-Categorization Processes in Organizational Contexts.” *Academy of Management Review* 25, no. 1 (January 2000): 121–140.
- Hogg, Michael A., Deborah J. Terry, and Katherine M. White. “A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory.” *Social Psychology Quarterly* 58, no.4 (December 1995): 255–69.
- Hogg, Michael A., Daan Van Knippenberg, David E. Rast, III. “Intergroup Leadership in Organizations: Leading Across Group and Organizational Boundaries.” *Academy of Management Review* 37, no. 2 (April 2012): 232–55.
- Huddy, Leonie, Stanley Feldman, Charles Taber, & Gallya Lahav. “Threat, Anxiety, and Support of Antiterrorism Policies.” *American Journal of Political Science* 49, no. 3 (July 2005): 593–608.

- Johnston, Lucy, and Miles Hewstone. "Intergroup Contact: Social Identity and Social Cognition." In *Social Identity Theory: Constructive and Critical Advances*, edited by Dominic Abrams and Michael A. Hogg, 185–210. New York: Springer-Verlag, 1990.
- Korschun, Daniel. "Boundary-Spanning Employees and Relationships with External Stakeholders: A Social Identity Approach." *Academy of Management Review* 40, no. 4 (October 2015): 611–29.
- Kris, David. "Carpenter's Implications for Foreign Intelligence Surveillance." *Lawfare* (blog). June 24, 2018, <https://www.lawfareblog.com/carpenters-implications-foreign-intelligence-surveillance>.
- Lichtblau, Eric. *Bush's Law: The Remaking of American Justice*. New York: Pantheon Books, 2008.
- Lincoln, Abraham. "Lincoln's Reply." In *Created Equal?: The Complete Lincoln-Douglas Debates of 1858*, edited by Paul M. Angle, 114–30. Chicago: University of Chicago Press, 1991.
- Lopach, James J., and Jean A. Luckowski. "National Security and Civil Liberty, Striking the Balance." *The Social Studies* 97, no. 6 (November/December 2006): 245–48.
- Madison, James. "Federalist No. 51." In *The Debate on the Constitution*, vol. 2, edited by Bernard Bailyn, 163–77. New York: Library Classics of the United States, Inc., 1993.
- McChrystal, Stanley, with Tantum Collins, David Silverman, and Chris Fussell. *Team of Teams: New Rules of Engagement for a Complex World*. New York: Portfolio/Penguin, 2015.
- Medine, David, Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. Washington, DC: Privacy and Civil Liberties Oversight Board, July 2, 2014.
- . *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*. Washington, DC: Privacy and Civil Liberties Oversight Board, January 3, 2014.
- Mols, Frank. "What Makes a Frame Persuasive? Lesson from Social Identity Theory." *Evidence & Policy* 8, no. 3 (August 2012): 329–45.
- The National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. New York: Norton, 2004.

- Nelson, Lisa. "Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era." *Public Administration Review* 64, no. 3 (May/June 2004): 259–69.
- Oakes, Penelope, J. S. Alexander Haslam, and Katherine J. Reynolds. "Social Categorization and Social Context: Is Stereotype Change a Matter of Information or of Meaning?" In *Social Identity and Social Cognition*, edited by Dominic Abrams and Michael A. Hogg, 55–79. Oxford: Blackwell, 1999.
- Olmstead, Kenneth. "Most Americans think the government could be monitoring their phone calls and emails." Pew Research Center. September 27, 2017. <http://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails/>.
- Operario, Don, and Susan T. Fiske. "Integrating Social Identity and Social Cognition: A Framework for Bridging Diverse Perspectives." In *Social Identity and Social Cognition*, edited by Dominic Abrams and Michael A. Hogg, 26–53. Oxford: Blackwell, 1999.
- Pew Research Center. "Few See Adequate Limits on NSA Surveillance Program." July 26, 2013. <http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/>.
- Pink, Daniel H. *Drive: The Surprising Truth About What Motivates Us*. New York: Riverhead Books, 2011.
- Posner, Richard A. "Privacy, Surveillance, and Law." *University of Chicago Law Review* 75, no. 1 (Winter 2008): 245–60.
- Pozen, David E. "Privacy-Privacy Tradeoffs." *University of Chicago Law Review* 83, no. 1 (Winter 2016): 221–47.
- Pratt, Michael G., and Peter O. Foreman. "Classifying Managerial Responses to Multiple Organizational Identities." *Academy of Management Review* 25, no. 1 (January 2000): 18–42.
- Rast, III, David E., Amber M. Gaffney, Michael A. Hogg, and Richard J. Crisp. "Leadership Under Uncertainty: When Leaders Who Are Non-Prototypical Group Members Can Gain Support." *Journal of Experimental Social Psychology* 48, no. 3 (May 2012): 646–53.
- Rehnquist, William H. *All the Laws but One: Civil Liberties in Wartime*. New York: Knopf, 1998.
- Richards, Julian. "Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (October 2012): 761–80.

- Richards, Neil M. “The Dangers of Surveillance.” *Harvard Law Review* 126, no. 7 (May 2013): 1934–65.
- Ries, Eric. *The Lean Startup*. New York: Crown Business, 2011.
- Savage, Charlie. *Power Wars: Inside Obama’s Post-9/11 Presidency*. New York: Little, Brown and Company, 2015.
- Schlesinger, Jr., Arthur M. *The Imperial Presidency*. Boston: Houghton Mifflin, 1973.
- Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee). *Final Report*, S. Rep. No. 94–755. Washington, DC: Senate, April 29, 1976. <https://www.intelligence.senate.gov/resources/intelligence-related-commissions>.
- Silber, Mitchell D., and Arvis Bhatt. *Radicalization in the West: The Homegrown Threat*. New York: New York City Police Department, 2007, https://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf.
- Sims, Jennifer. “Intelligence to Counter Terror: The Importance of All-Source Fusion.” *Intelligence and National Security* 22, no. 1 (February 2007): 38–56.
- Solove, Daniel J. “Data Mining and the Security-Liberty Debate.” *University of Chicago Law Review* 75, no. 1 (Winter 2008): 343–62.
- . “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *San Diego Law Review* 44 (2007): 745–72.
- Stuntz, William J. “Secret Service: Against Privacy and Transparency.” *New Republic*, April 17, 2006.
- Sunstein, Cass R. “Beyond Cheneyism and Snowdenism.” *University of Chicago Law Review* 83, no. 1 (Winter 2016): 271–93.
- Suskind, Ron. *The One Percent Doctrine: Deep Inside America’s Pursuit of Its Enemies Since 9/11*. New York: Simon & Schuster, 2006.
- Sutherland, Daniel W. “Homeland Security and Civil Liberties: Preserving America’s Way of Life.” *Notre Dame Journal of Law, Ethics and Public Policy* 19, no. 1 (February 2014): 289–308.
- Tajfel, Henri. English Manuscript of “La Catégorisation Sociale.” In *Introduction à la Psychologie Sociale*, edited by Serge Moscovici, 272–302. Paris: Larousse, 1972.
- , ed. *Social Identity and Intergroup Relations*. Cambridge: Cambridge University Press, 1982.

- Tajfel, Henri, and John Turner. "An Integrative Theory of Intergroup Conflict." in *The Social Psychology of Intergroup Relations*, edited by William G. Austin and Stephen Worchel, 33–47. Monterey, CA: Brooks/Cole, 1979.
- Terry, Deborah J., Michael A. Hogg, and Julie M. Duck. "Group Membership, Social Identity, and Attitudes." In *Social Identity and Social Cognition*, edited by Dominic Abrams and Michael A. Hogg, 280–314. Oxford: Blackwell, 1999.
- Turner, John C. "Social Categorization and the Self Concept: A Social Cognitive Theory of Group Behaviour." In *Advances in Group Processes*, vol. 2, edited by Edward Lawler, 77–122. Greenwich, CT: JAI Press, 1985.
- . "Social Comparison and Social Identity: Some Prospects for Intergroup Behaviour." *European Journal of Social Psychology* 5, no. 1 (January/March 1975): 5–34.
- Turner, John C., Michael A. Hogg, Penelope J. Oakes, Stephen D. Reicher, and Margaret S. Wetherell, eds. *Rediscovering the Social Group: A Self-Categorization Theory*. New York: Basil Blackwell, 1987.
- U.S. Congress. Senate. *Hearing on Oversight of the Department of Justice*. 110th Cong., 1st sess., July 24, 2007, http://www.washingtonpost.com/wp-srv/politics/documents/gonzalez_transcript_072407.html.
- U.S. Congress. Senate. *Hearing on the U.S. Attorney Firings before the Senate Judiciary Committee*, 110th Cong., 1st sess., May 15, 2007, http://gulcfac.typepad.com/georgetown_university_law/files/comey.transcript.pdf.
- United States Department of Homeland Security. "National Network of Fusion Centers Fact Sheet." Last published June 21, 2017. <https://www.dhs.gov/national-network-fusion-centers-fact-sheet>.
- . "State and Major Urban Area Fusion Centers." Last published June 26, 2017. <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>.
- Vagle, Jeffrey L. "Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance." *Indiana Law Journal* 90, no. 1 (Winter 2015): 101–50.
- Van Knippenberg, Daan. "Social Identity and Persuasion: Reconsidering the Role of Group Membership." In *Social Identity and Social Cognition*, edited by Dominic Abrams and Michael A. Hogg, 315–31. Oxford: Blackwell, 1999.
- Wittes, Benjamin, and Jodie C. Liu. "The Privacy Paradox: The Privacy Benefits of Privacy Threats." Center for Technology Innovation at Brookings, Brookings Institution. May 21, 2015. https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf.

- Yoo, John. "Authority for Warrantless National Security Searches." Letter to Judge Colleen Kollar-Kotelly, May 17, 2002, <https://www.justice.gov/olc/page/file/936196/download>.
- . "Memorandum for the Attorney General." Washington, DC: Department of Justice, 2001. <https://www.justice.gov/sites/default/files/olc/legacy/2011/03/25/johnyoo-memo-for-ag.pdf>.
- . "The Terrorist Surveillance Program and the Constitution." *George Mason Law Review* 14, no. 3 (Spring 2007): 565–604.
- . *War by Other Means: An Insider's Account of the War on Terror*. New York: Atlantic Monthly Press, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California