1-1-2016

Interactive Security: The Rhetorical Constitution Of Algorithmic Citizenship In War On Terror Discourse

Avery Henry
Wayne State University,

INTERACTIVE SECURITY: THE RHETORICAL CONSTITUTION OF ALGORITHMIC CITIZENSHIP IN WAR ON TERROR DISCOURSE

by

AVERY J. HENRY

DISSERTATION

Submitted to the Graduate School

of Wayne State University,

Detroit, Michigan

in partial fulfillment of the requirements

for the degree of

DOCTOR OF PHILOSOPHY

2016

MAJOR: COMMUNICATION

Approved By:

_____

Advisor Date

_____

Date

_____

Date

_____

Date

ACKNOWLEDGEMENTS

To my wife, Danielle Henry, thank you for supporting me every step of the way on this adventure. You were willing to move across the country and you tirelessly worked to support us while I was in school. Thank you for the constant love and support that made everything possible. I love you.

Thank you to my advisor Kelly Young. I greatly appreciate the countless hours you spent discussing, editing, revising, and working with me on this dissertation (notice I put the list in alphabetical order). On top of all the work spent on the dissertation, I greatly appreciate the additional time and resources you spent teaching me to be an academic, debate director, and educator.

To the other members of my committee, Jeff, Jim, and Ron, thank you all for the work you put into educating me. I greatly enjoyed attending your classes and am trying my best to pass on the knowledge that you so generously gave me. I am also very thankful for the time that you all spent as I pestered you during office hours and even more thankful for your willingness to spend additional time scheduling meetings. Finally, thank you for agreeing to serve on my committee and guiding me throughout my dissertation.

Thank you to all the other graduate students at Wayne State. I could not imagine a more supportive group of scholars to embark on this journey with. I am especially thankful for my office mates Brandon, Craig, John, and Stephen who spent countless hours writing with me, providing advice about classes and the program, and just being great friends. I would also like to thank Bruce and Brad for being so willing to pick up

the debate coaching slack, created by Craig and John of course, and allowing me to spend more time working on this dissertation.

To my parents, John and Cathy Henry, thank you for everything. You gave me life, raised me, and supported my career aspirations of being an academic. You both provided encouragement and love through the entire process. I can only hope to be a fraction of the educators that you both are.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION TO ALGORITHMIC SECURITY

Introduction

American Express released a commercial during Super Bowl XLVIII entitled "Intelligent Security." The commercial begins with a white man walking through a city, protected by the security of police officers' gaze and surveillance cameras. As the man walks past security, Claire Danes, star of Showtime's *Homeland*, provides a voiceover stating, "In the real world security surrounds us, there are cameras, police, guards, but who looks after us online where we spend 200 billion dollars a year?" (ezkl2230, 2013). The message of the commercial indicates that traditional modes of surveillance have made people so secure that they are not aware of the invisible danger that lurks in the virtual realm. Consumers are asked to sign on with American Expresses' virtual security that tracks all of their purchases to learn spending patterns and detect abnormal transactions. By signing up with American Express, consumers are invited to become "members of a more secure world" (ezkl2230, 2013).

The rhetoric of the "Intelligent Security" advertisement invites consumers to join a biopolitical community where subjects willingly subscribe to intense surveillance for the purposes of being secure. In the "real world," consumers become naturalized to the constant surveillance of cameras, closed circuit televisions, and the judicial gaze of police offers. People have naturalized external surveillance to such a degree that they feel so secure that they are unaware of the danger waiting in the digital domain. To counter this false sense of security, American Express enlightens consumers about the dangerous and invisible virtual threat that anonymous hackers, catfishers, and identity thieves represent.

In response to this insidious and invisible threat, American Express conjures the image of a police officer in the circuit board vigilantly tracking daily purchases to keep consumers secure. By invoking the presence of an invisible threat, American Express naturalizes constant surveillance that creates a personalized digital profile, learns consumers' preferences and tracks their behavior. In this new secure community, consumers actively participate in the constitution of a surveillance regime that algorithmically regulates society.

By hiring Claire Danes as a spokesperson, American Express further shows how personalized surveillance is connected to homeland security. In the show *Homeland*, Danes plays a CIA agent who surveils an American citizen suspected of being radicalized after he is found alive in an al Qaeda prison. In taking up the themes of domestic radicalization, drone strikes, and spying on American citizens, *Homeland* glamourizes an intensified security regime. Linking the mass popularity of a show that visually emphasizes the threat of domestic terrorism with a credit card commercial advertising personalized surveillance, American Express articulates algorithmic governance as the future mode of dealing with all security threats, economic or terroristic.

This dissertation maps a similar type of intensification from traditional modes of governmentality and surveillance into algorithmic regulation on a broad scale. By primarily following the presidential rhetoric of George W. Bush and Barack Obama, regarding citizenship, surveillance, and war, it becomes possible to chart the intensification of war from previous approaches to new intelligent security and algorithmic governance methods. The September 11, 2001 attacks against the Pentagon

and World Trade Center radically transformed the cultural terrain of the American way of life. Under the mantra, "never forget," a new cultural logic was forged to combat and ward off future terrorist attacks. The attacks against the United State homeland shattered the exceptionalist belief that America is a fortress free from the violence of the world outside its borders. In response, the government began to implement new security practices to operate in an environment where inside/outside and friend/enemy distinctions are no longer clear. Because modern terrorist threats cannot be easily identified in a diverse and globalized world, new systems of tracking potential target data and disposition were necessary; it necessitated new systems able to monitor both citizens and potential enemies.

In this project, I argue how, in comparison to the previous 1.0 paradigm, a new logic of 2.0 may have intensified post-9/11 cultural, economic, political, and social relations. Prior to 9/11, our culture operated under what I will call a "1.0 paradigm" that interpellates and cultivates passive depoliticized subjectivities. For example, Web 1.0 is thought of as a medium, in which users are docile subjects who passively receive information. In this paradigm, using the internet is conceptualized much like watching television: it is one-way communication where the user consumes information. Similarly, Government 1.0 operates through a representational form of democracy where elites act on behalf of their constituency and citizenship is enacted through consumerism. After 9/11, the cultural milieu of 1.0 shifts away from the passive asymmetrical form of citizenship, government, and web usage into an interactive model that is traditionally categorized through the moniker of 2.0.

Government 2.0 grew out of Web 2.0, in which users interact and connect to one another virtually. In Government 2.0, new channels for direct communication and interaction open between those who govern and those who are governed while Citizenship 2.0 moves from passive consumption to active interactive experiences. Under the 2.0 logic, subjectivity is transformed through the postmodern tenants of celebrating difference, dissolving hierarchical binaries, liberating desire, and promoting flexible and loosely connected networks. As a result, consumerism is less about purchasing this or that product and more about rating products, submitting data about behavior or disposition, and transforming one's subjectivity. Furthermore, this subjectivity links with the circulation of and identification with rhetorical tropes of openness and transparency over-determining everyday life into an informational economy. In doing so, this cultural logic of 2.0 eliminates the concepts of banal activity, as all activity, communication, or information is to be potentially collected and sorted as data and used for a purpose.

In the area of national security, the recording of daily life as data posits citizenship within a suspicion economy. By suspicion, I mean to suggest that after 9/11, the fantasy of fortress America was destroyed and alternative means of security asked for citizens to be vigilant and on the lookout for an ever-present threat. Due to globalization and the impossibility of closing and securing all of America's borders, the government seems to have enlisted its citizens into the war on terror in a number of ways. For instance, the passing of the PATRIOT Act (2001) provides the government with the legal justification needed to begin collecting, monitoring, and sorting daily communications of

its citizens and non-citizens within its borders. This legislation is supplemented with public awareness campaigns such as the New York Metropolitan Transportation Authority's slogan, "See Something, Say Something," encouraging citizens to watch those around them and report anything suspicious to local authorities. Overall, the attacks of 9/11 altered social relations by reconfiguring citizens' (inter)actions with businesses, government, law enforcement, and the military in different and more frequent ways.

In order to explore how this intensification of national security rhetorically operates, I begin by sketching out a theory of algorithmic citizenship and governance demonstrating how there is a shift in the logic and rhetoric of national security that corresponds with the intensification and transformation of the relations between citizens and government. In particular, I note how these alterations occur through the classic Aristotelean modes of persuasion: pathos, logos, and ethos. The section, "Pathetic Security," explores how national security after 9/11 relies on a twofold process of a reactionary measures and a sensory economy to produce and heighten feelings of fear, security, and suspicion. The next section, "Logical Security," traces how citizens' sense of danger works in tandem with statistical risk assessment to calculate the risk of terrorism and weigh it against the burdens of security measures to justify and rationalize heightened surveillance and law-enforcement. Next, in "Ethical Security," I map how the production of feeling and statistical analysis work as technologies of subjectivity cultivating the citizenry as communicative subjects and agents whom provide labor and produce value for national security. After demonstrating how this rhetoric of algorithmic

citizenship operates, I review relevant literature about deliberative democracy, cultural citizenship, citizen-soldiers, and performative citizenship. I finish by outlining the guiding questions for my project and offer an outline of the proceeding chapters of the manuscript.

Pathetic security. Given that the first major attack on American soil involved the hijacking of four commercial airline flights, it is hardly surprising that the reactive logic of the U.S. was to heighten airline security. A major component in securitizing airports was to manage passengers' feelings of security. That is, passengers are encouraged to perform acts of transparency so as to not arouse the suspicion of other passengers or security agents while simultaneously being vigilant for signs of potential danger. Despite networks of security measures, such as increased agents and guards, cameras, and other techniques, flying is always fraught with danger and risk. Moving between various security processes within the network does not foreclose danger; rather, it provides passengers an experience, feeling, or sensation that they are being secured. People arriving at an airport are not guaranteed the ease of travelling that existed before 9/11. Nor are passengers provided assurance that their flights will have safe passage due to any number of factors that could affect personal safety. Instead, the first experience one has when entering an airport is an encounter with law enforcement and surveillance technology. This experience of security occurs through the process of identification and verification, physical screening, public announcements, and the public spectacle of witnessing bodies being screened. This pervasive presence of policing activity and security measures serves the dual role of providing passengers the experience of security

under a canopy of constant legal surveillance while simultaneously summoning self-disciplining subjects who knows that they are being watched and, as a result, conform to the traveling protocols and rules so as not to arouse suspicion.

The move to produce a feeling of security does not guarantee actual security. In fact the process of airport security culminates in a wide range of feelings as people move through the airport. For instance, the performances of transparency are capable of making some people feel safe and secure as they watch the intense screening that people have to undergo. Others might feel anxious, nervous, or uncomfortable that they have to submit to such strict scrutiny or worry that they may have accidently brought a prohibited item with them. There are others who experience the spectacle of security and it magnifies their fear of travel. Yet, others are filled with intense anger at either the inconvenience that security measures produce or at the profiling and stereotyping that results when attempting to detect threats. Regardless the specific feelings that a person has, the suspicion economy of airport security operates through affective production of emotions.

The first process that one must go through in order to fly commercially is to pass through a system of identification and verification. This system is intricately connected to surveillance and citizenship; the ability to produce proper documentation determines who belongs and who does not. The very demand that citizens must show an identification card to prove who they are shows that there is a distrust of the individual, despite the demand's purported value for verification purposes (Lyon, 2009). The burden of proof for one's identity lies within the document that can be produced because, as

Lyon (2009) argues, identification documents are part of a culture of suspicion. In other words, the demand for identification is an order to present oneself as a citizen so that both the citizen and non-citizen can be made intelligible or legible (Lyon, 2009).

In addition to being required to pass through several identification and verification measures, passengers must submit to physical and property searches after standing in a security line as the Transportation Security Administration (TSA) employees regulate the flow of bodies into designated areas. After providing identification to security personnel, passengers are then required to take off all coats or jackets, hats, and shoes, remove all computers and/or other electronic devices from their bags, and put all of their belongings onto a conveyor belt that transports personal items through a screening process. Passengers then wait their turn for the TSA officer to grant them permission to enter the Advanced Imaging Technology (AIT) booth that provides a full body scan in an attempt to detect "metallic and nonmetallic threats, including weapons and explosives, which may be concealed under clothing without physical contact to help TSA keep the traveling public safe" (Transportation Security Administration, 2014, September 3). This scanning system is able to look underneath clothes revealing a generic figure of a body in an attempt to highlight anomalies. While this scanning system no longer renders the naked body apparent to TSA agents, it can reveal health or medical abnormalities that the traveler would not want exposed (ACLU, 2010). According to TSA promotional materials, this screening process is preferred by over 80 percent of Americans because it is an exercise that makes them feel safe (TSA, 2014, September 3).

Of course Americans prefer the AIT screening process because the alternative requires a far more physically invasive method primarily consisting of physical pat-downs. TSA informs all potential travelers that pat-downs will be conducted by an officer of the same sex, which brings with it a potential delay if an officer is not immediately available. The pat-down can be done in a private room rather than in the open space of the airport if a passenger requests it. The officer must offer a private screening when they are conducting a pat-down on "sensitive areas." During the pat-down, the screener,

> will examine your head, shirt collar area, and waistband, and may use either the front or back of his or her hands to feel your body, including buttocks, around breasts, and between the legs, feeling up to the top of the thigh. Women in tight skirts that don't allow an agent to feel the thigh area may be asked to remove the skirt in a private screening area and will be given a gown or towel to put on. (ACLU, 2010, para. 5)

In addition to electing to have this kind of search, individuals are often flagged or randomly selected to undergo a process of a "resolutional pat-down." It is not uncommon to be standing in line and witness or experience the suspicion lottery first hand as TSA agents select people waiting in line and escort them to an alternate area. This mode of screening is authorized when an anomaly is detected by either the AIT, pat-down, or other selection methods. TSA (2014, November 13) inform travelers to remove body piercings as they often register as an anomaly. Additionally, travelers can also be selected if religious headwear "is loose fitting or large enough to hide prohibited items" (TSA, 2014, November 13). These resolutional pat-downs are far more invasive because officers are allowed to use the front of their hand to conduct a more thorough search, including examining the groin area (ACLU, 2010).

The threat of being molested by security officers was not the only terrifying issue that passengers faced. On March 11, 2002, President Bush signed the Homeland Security Presidential Directive 3, which implemented a color-coded Homeland Security Advisory System. The purpose of the advisory system was to create a common context, structure, and vocabulary for discussing threats to the country (Bush, 2002, March 11). The Department of Homeland Security indicated the current threat level and conditions by signifying it through a range of colors: Green meant the threat was low; blue meant guarded; yellow meant there was an elevated threat level; orange indicated high threat levels; and red signaled a severe threat (WH, OPS, 2002, March 12). Passengers were informed through messages throughout the airport indicating what the current threat level color was. The Department of Homeland Security (2015) provides a chronology of the changes to the system. It was introduced March 12, 2002 with a threat level of Yellow. It then fluctuated between Yellow and Orange until August 10, 2006, when it was raised to Red. This means that for nearly ten years, passengers using public transit were told that there was an elevated or high terrorist threat level when they traveled. At no point does DHS indicate that U.S. passengers on public transit were ever told that the threat level was low or even guarded. Instead passengers were confronted with impending danger every time they travelled.

Announcements are constantly delivered over a loudspeaker directing the public to keep their bags on them at all times and to constantly be attentive for suspicious activities such as a person setting down a bag and walking away (Transportation Security Administration, 2014, July 28). In July 2011, the National Terrorism Advisory System

replaced the color-coded Homeland Security Advisory System. It provides information to the public about potential terrorist threats, details about what authorities are doing, and outlines steps that individuals can take to "protect themselves and their families, and help prevent, mitigate, or respond to the threat" (Department of Homeland Security, 2014, September 5). Posters and various images are plastered on walls throughout the airport inscribed with slogans such as "See Something, Say Something," encouraging citizens to be vigilant and communicate any perceived threats or irregularities to the proper authorities (Transportation Security Administration, 2014, July 28). The call to report suspicious behavior requires individuals to experience, feel, or sense danger. For instance, FBI director James Comey stated, "When the hair on the back of your neck stands, listen to that instinct and just tell somebody" (Shamsi & Harwood, 2014). Sensing danger becomes rhetorically significant because it accentuates that technologies and practices do not necessarily bring about actual security as much as they produce an experience of feeling secure or insecure.

The experience of security works through the participation in a suspicion lottery. It begins with the call to produce identification; an act that at the onset deems all individuals as untrustworthy. Because all airline patrons are suspicious, they are required to submit to intense surveillance and security checks to determine who is a normal passenger and who is a threat to be apprehended. In order to make these determinations, individuals must submit and participate in both vertical – authoritative overseer gazes on a population -- and horizontal – peer-to-peer monitoring of suspicious behavior – surveillance. This whole system of monitoring and scrutiny is made public so that people

witness the profiling that is going on all around them. For instance, a person standing at a checkpoint can observe as TSA agents select and pull people out of line for additional screening. This process then works to persuade those passengers who finally make it to their flight that they are secure because they have passed through tedious and intense regulations.

What the current anti-terrorism laws and policies signify is not an actual guarantee of security, but rather the experience or feeling of being in/secure. Regardless if a person feels anger, anxiety, comfort, or fear, the process of security measures and surveillance solicit feelings. It is through the experience of going to an airport, being subjected to intense surveillance and screening processes, and watching others be randomly selected or racially profiled that passengers are able to experience the sensations of security. In other words, going to the airport becomes an affective experience that works to persuade members of the public that they are secure by providing them with a series of activities, commands, intensities, and sensations that conjure a specific mood or attitude of being safe. However, this affective experience of security is not isolated merely to airports; instead, it extends to the entirety of anti-terrorism surveillance and data collection that frames terrorism as an ever-present threat that must be monitored and warded off through the collection of everyday communications and data.

There will be blood: logical security. In addition to providing a feeling of security, post 9/11 national security rhetoric supplements the pathos of security with a calculative logic of utilitarian cost-benefit analysis and risk assessment to rationalize

heightened surveillance of citizens. Take for instance the Public Broadcasting Service (PBS) documentary *United States of Secrets (2014)*, which documents how government officials rely on the rhetorical tactic of blaming those who oppose government surveillance for being culpable in the loss of life. For example, the documentary notes the NSA surveillance operation named, "The Program," gathers data on phone calls and internet traffic of hundreds of millions of Americans in search for suspicious connections. The Program is so excessive and invasive that Jack Goldsmith, the former head of the Department of Justice's Office of Legal Counsel—the esoteric office which interpreted laws in ways that justified a number of excessive post-9/11 policies—informed the government that he was going to pull back his endorsement regarding the Program's legality. In response to this claim, David Addington, attorney of Vice President Dick Cheney, stated, "If you do that, the blood of 100,000 people killed in the next attack will be on your head" (Kirk, Gilmore, & Wiser, 2014). Later, when the *New York Times* was going to publish a story about the Program, President Bush invited a few of its editors and the publisher to the Oval Office to discuss the story. In an attempt to persuade the *Times* to not publish the story, President Bush had Michael Hayden brief the *Times* staff of the Program's importance. Hayden attempted to persuade the *Times* staff not to publish the story by describing a potential worst-case scenario where terrorists attempt to take down the Brooklyn Bridge with a blowtorch. Bill Keller, one of the *Times* editors present at the meeting, describes how Bush followed up with his own slippery slope argument:

> Listen, if you guys publish this article and there's another 9/11, we're going to be called before Congress to explain how we failed to prevent it.

> And you should be in the chair beside us explaining because you'll be complicit in allowing damage to our country. He was saying, in effect, You, Arthur Sulzberger, will have blood on your hands if there's another attack that could've been prevented by this program. You know, I think anybody would feel goose bumps. (Kirk, Gilmore, & Wiser, 2014, p. 46)

Similarly, Thomas Drake, former senior executive of the NSA who leaked information about the NSA program, was informed by government agents that because of his actions he would have American soldiers' blood on his hands (Kirk, Gilmore, & Wiser, 2014).

The rhetorical tactics of constructing exaggerated apocalyptic scenarios to coerce legal departments, journalists, or whistleblowers from speaking out about government abuses culminates in a culture of secrecy and has chilling effects on free speech in a democratic society. In each of these examples, the government draws upon MacBethian guilt by blaming people who would report government surveillance to the public, implicating them in phantasmal terrorist attacks that are always-already about to occur. However, the rhetorical strategy of exaggerating risk is similarly deployed against the American public at large. Individuals are encouraged to submit and participate in mass surveillance based on manufactured claims about the risks of another terrorist attack. The threat of terrorism operates around a specific rhetorical narrative of "movie-plot threats," where the government or media spin an overly specific scenario in which an extreme apocalyptic disaster will happen (Schneier, 2009). These anxiety-provoking narratives propagated by politicians and popular entertainment all contribute to the creation of "Security Theater," a reactionary countermeasure designed to make people feel secure without providing them actual security. Security theater is rhetorical in nature because terrorist acts of mass destruction are extremely rare statistically and incredibly difficult to

execute (Mueller, 2006). Yet, despite the incredibly low probability of attack, these odds do not assuage the intense fear and passions that are generated by narratives about terrorist destruction.

In order to provide the public with a feeling of safety, the government implements reactive measures to prevent whatever attack was previously tried. For instance, the 9/11 attacks were carried out by terrorists who used box cutters to hijack the flight. In response, airlines prohibited passengers from carrying aboard box cutters. Richard Reid, the "Shoe Bomber", was flying from Madrid to Miami when he was apprehended on the flight after failing to successfully light a bomb in his shoe (Carfano, Bucci,& Zuckerman, 2012). After his failed attempt, airlines required passengers to take off their shoes during the screening process. Furthermore, in 2006, British and Pakistani authorities claimed to foil a terrorist plot that planned to use liquids and an MP3 player to create explosives that would be used to blow up jetliners heading to the U.S. (CNN, 2006). The response was the U.S. raised the threat level to the color Red and MP3 other similar devices that could be used to detonate explosives and all liquids over three ounces were temporarily banned. These reactive policies cannot retroactively prevent the attempts attacks from happening in the first place, nor do they bring consolation to those who experienced an attack. Instead, the whole design of these countermeasures is to provide the public with the feeling that they are secure from events that happened before.

The problem with taking a reactive approach to counter-terrorism is that the security measures put in place do not guarantee passengers complete safety. There have been several studies conducted that conclude that body scanning systems are inaccurate.

For instance, the TSA's Rapiscan full-body X-ray scanner might be tricked in several ways: people could seal weapons under Teflon tape on their spine so that the weapon blends into the background of the X-ray; they could install Malware into the scanning system to trick or deceive the scan; they could mold plastic explosives to be indistinguishable from flesh; or they could sew guns made fully of metal into the side of their clothes so that they blend in against the black backdrop of the X-ray (Greenberg, 2014). Additionally, it is also possible to download an image of a boarding pass from an airline website or scan a copy of an old one, use Photoshop to doctor the date on the boarding pass, print it, and a person could get passed security checkpoints (Mann, 2011). Furthermore, terrorists can also find items not typically considered weapons and use them to dangerous ends. For example, the 9/11 reports stated that the hijackers on American Airlines Flight 77 used box cutters or utility knives; prior to 9/11, these items were commonly used in offices to cut tape or paper (U.S. National Commission on Terrorist Attacks upon the United States, 2004). It is not difficult to conceptualize various makeshift weapons such as a pen or car keys or any number of other items that could be used to physically force someone into submission.

In addition to deploying reactionary countermeasures, U.S. counter-terrorism also found it necessary to identify and predict where potential terrorists might strike next. A former counter-terrorism official described the difficulty of identifying terrorists, arguing that the United States faced "a disposition problem" because they could not determine what behavior was consistent with terrorism (Miller, 2012). President Bush explained the

difficulty of identifying terrorists and justifying the collection of a wide range of information in order to best tend to the disposition problem:

> The terrorists who declared war on America represent no nation. They defend no territory. And they wear no uniform. They do not mass armies on borders or flotillas of warships on the high seas. They operate in the shadows of society. They send small teams of operatives to infiltrate free nations. They live quietly among their victims. They conspire in secret. And then they strike without warning. And in this new war, the most important source of information on where the terrorists are hiding and what they are planning is the terrorists themselves. (WH, OPS, 2006, September 6, para. 6)

As a result, active counterterror operations depict terrorism as a disposition problem and, as such, the only way to provide complete security to the public is to monitor, measure, map, and predict normal and abnormal dispositions to weed out potential terrorists from everyone else.

At least it's an ethos: ethical security. If terrorism is a "disposition problem," a new mode of citizenship and communicative subjectivity is necessary to combat it, according to counterterrorism officials. For example, after 9/11, President Bush was speaking at O'Hare airport in Chicago to airline workers. In his speech, Bush played off a couple well known airline titles to articulate how America was going to be united in bringing justice to the enemy that attacked them (WH, OPS, 2001 September 27). Bush articulated the war on terror as a classic Manichean conflict of good versus evil. Citizens were called to arms and hailed to rally and support the good cause. Yet, citizens were not asked to make the traditional sacrifices that nations ask of their people. For instance, Americans were not asked to ration, scrap, and save. Instead, Americans were asked to

shop, spend, and vacation. To put it even more simply, citizens are asked to do one thing: consume.

It is in this call to consume that this project traces how monitoring consumer activity becomes an active and invaluable part of the warfighting process that suggests the emergence of a system of algorithmic citizenship and governance. When President Bush spoke at O'Hare airport, he informed the citizens that the government was going to deploy every means of intelligence gathering and surveillance at its disposal and he called on citizens to cooperate with law enforcement and intelligence agencies (WH, OPS, 2001, September 27). Additionally, Americans were told that they could help fight the war on terror not just by consuming but also by working. For example, the President's discourse constituted airline employees as citizen-soldiers who fight terror by flying a plane to its destination, loading someone's bag, and servicing passengers; acts that embody the American spirit, freedom of mobility, and an indomitable courage that does not let fear keep employees from doing their jobs (WH, OPS, 2001 September 27). Moreover, the President also called on citizen-soldiers to monitor each other and if they witness a potential terrorist attack unfolding or any suspicious behavior, they should respond like the passengers did on United Airlines Flight 93 and take direct action to thwart the plot. Thus, flying on a plane and taking a vacation are discursively linked to a mode of subjectivity that engages in ideological performances to thwart terrorism. Put another way, if the terrorists were committed to an ideological battle that uses terrorism to disrupt America's way of life, then acts of normalcy such as consuming and working are framed in response as symbolic strikes in the interpellation battle of good versus evil.

This type of discourse is not limited to just government policy or presidential addresses. Immediately following the speech given by President Bush to the airline industry, *CNN* correspondent John King interviewed Disney CEO Paul Pressler about the importance of the President's speech and how Disney was participating in making us all more secure. Early in the interview, King noted that when the U.S. military took action in response to 9/11, it risked provoking more attacks on American soil. For instance, King stated, "terrorists would target populated sites, obviously, Disney, Mickey Mouse, a symbol of America, if you will" (King & Pressler, 2001). If in a world where the enemy engages in symbolic attacks against the World Trade Center, according to the Bush Administration and Disney Corporation, the public fights the war by engaging in a symbolic response of their own. Rather than succumbing to the fear imposed by terrorism, the public is asked to rally behind the war effort by behaving like good Americans and go on vacation. Within this logic, people going to Disney and engaging in other commercial activity in response to 9/11 were directly participating in the global war on terror. In other words, the public, by choosing to fly and go vacation, are able to fight off the economic devastation that the 9/11 attacks caused and symbolically fight the psychological threat posed by terrorists. Taking a vacation was not merely business as usual; instead, this consumerism becomes a weapon in the fight against terrorism.

To help understand how consumerism becomes a major weapon in the war on terror, this dissertation analyzes how this behavior is articulated in relation to security and surveillance. While, the idea of behaving normally works on some level as an ideological performance against terrorism, once it is attached to regimes of surveillance and

algorithmic profiling, it becomes a far more serious warfighting technique. For instance, the consumption involved with purchasing an airline ticket and flying to Disney are accompanied by bodily performances of submitting to enhanced identification systems, tightened security, and tracking systems designed to distinguish good consumer behavior from terrorist dispositions. Good citizens are not only transparent consumers who are open to surveillance, but they also are active and watchful communicative subjects who make themselves and their information visible while reporting on others who they feel are suspicious. Continuing with the Disney example, the public is asked to succumb to new security policies that are being implemented by Disney and other popular tourist locations. As such, Americans are asked to continue their consumerist way of life in the most monitored and regulated way possible. Within this discursive context, the public is taught to associate the increased presence of law enforcement and surveillance as positive experiences that foster a "sense of security" (King & Pressler, 2001). Thus, in typical Disney fashion, the public is offered a manufactured experience; but this time, it includes an artificial sense of security. Much like visiting Epcot does not allow an individual to visit the actual country of Japan but instead offers a simulated experience of travelling around the globe, Disney's rhetoric and security actions did not make the public actually safer; instead, it just gives them the illusion of security. What is noteworthy about the *CNN* interview with Pressler is how it seems to legitimize and normalize the articulation of corporate tourism and military bureaucracy. In the post 9/11 environment, not only would Homeland Security rely on various government agencies to counter terrorism, but it also appears to call on giant consumer corporations such as Disney to aid in the fight

against terrorism. Therefore, in telling the public to go on vacation, President Bush articulates together corporations and the military, labor and consumerism, and transparency and security. These articulations configure a new mode of citizenship and communicating subjects who are encouraged to feel and then communicate their dispositions and report suspicious behaviors and dispositions. The information that is constantly collected through the monitoring of the population is used to later statistically determine normal citizens' dispositions and detect abnormal and potential terrorist behavior.

Corporations and the government attempt to establish an ethos of fun and security. The government attempts to persuade citizens that it is only collecting this data so that it can keep people safe. The maxim of "nothing to hide, nothing to fear" is used to promote the idea that citizens should trust that the government is only spying on potential terrorist suspects and would never abuse its power. Meanwhile, corporations collect mass data using the rhetoric of convenience and entertainment. Citizens can trust that corporations will not abuse the data that they collect, because they are creating algorithmic profiles simply to make life easier and fun. Google only reads your email so it can recommend products that you might like and American Express only monitors spending so it can keep you safe and secure. Thus, consumers are encouraged to join the community of intelligent security and life in a more fun and safe world.

Government 2.0 and algorithmic citizenship. The articulation of consumerism and surveillance in relation to fun and security functions as an altered and intensified mode for citizens actively participating in the war on terror. Following what Tim

O'Reilly terms "government 2.0" and "algorithmic regulation," I argue that citizens are encouraged to identify with the rhetorical tropes of openness and transparency and adhere to a new communicative subjectivity: the collaborative and participatory consumer, or what I term algorithmic citizenship. This new mode of algorithmic citizenship and governance appears to rely on the rhetorical circulation of affective energies regulating an individual's capacity to act based on the appropriate security ratio (Chaput, 2010). Citizens are encouraged to be open and transparent in their daily lives while remaining simultaneously vigilant and willing to communicate through identifying, recording, and reporting all behaviors they deem suspicious.

After the attacks on 9/11, American citizens were forced to confront the fact that they were no longer impervious from being targets of attacks and that the government could not guarantee their complete security. Citizens were left wondering: what went wrong? How could the government fail to identify and prevent the attacks? What could motivate this spectacular violence? This confusion was compounded further by the 9/11 Commission's finding that the suspected hijackers in several instances were flagged for advanced screening prior to their flights but were cleared (U.S. National Commission on Terrorist Attacks upon the United States, 2004). The images of two of the suspected airline hijackers going through security in Portland, Maine circulated around the internet along with the claim that if the airline had a system that utilized biometric identification technology, the two men would have been identified as known terrorists (Gates, 2011). Yet, in this instance, the fact that the government knew that these hijackers likely were terrorists is the exception rather than the norm. Instead, the United States faced a

disposition problem in that it did not know the identity or characteristics of many if not most of the terrorists. As a result, the government needed to update its screening and surveillance processes while relying heavily on the labor of its citizens to watch, report, and circulate any information necessary to help discern normal from abnormal dispositions. The best way for the government to identify, predict, and prevent terrorist attacks would be to promote open access to data, collaboration between citizens and government employees to produce and monitor the data, and information sharing across all agencies. In short, this created the need for a new informational economy based on data collection and sharing, identification, and surveillance.

Within this informational economy, my contention is that the affective production of security is interrelated with the predictive modeling of behavior into algorithms. If this is true, algorithmic regulation works through the mapping and managing of dispositions. It is a loose form of control that does not impose restrictions on daily life. Instead, it operates through the collection of data that is shared: consumer preferences work to formulate normal practices into a statistical model that is then used to predict or detect abnormal or "terrorist" behavior. Put different, within this economy, dispositions, experiences, and feelings are translated and inserted into an algorithmic process to be diagrammed and regulated in order to wage the war on terror.

My argument is that this management of dispositions operates in the monitoring of citizen's communications to detect patterns of normality. First, it works through the advanced data collection of people's daily communications. For example, spying programs like PRISM collect personal data and consumer spending information, which

the government analyzes and sorts in order to differentiate normal practices of citizenship and consumerism from those that have been defined as indicative of terrorism. Second, once the government has collected personal data, it must sort through the information to determine and target those who are classified as potential terrorist or actual terrorist subjects. To this end, the government has established a "Disposition Matrix" that operates as a "single, continually evolving database in which biographies, locations, known associates and affiliated organizations are all catalogued. So are strategies for taking targets down, including extradition requests, capture operations and drone patrols" (Miller, 2012). While the government once worked through a series of inter-related yet independent agencies, such as the Central Intelligence Agency (CIA), the Department of Justice (DOJ), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Immigration and Naturalization Services (INS), that all collected their data on potential security threats and terrorist suspects, this information now can be consolidated into a single database that can be accessed and added to between the different agencies (Miller, 2012).

The development of the disposition matrix has rhetorical significance because it demonstrates how daily communications and consumer behavior are used to determine normal from abnormal dispositions. In other words, the way that people communicate, the terms that they search on-line, and the meanings signified by the goods that people purchase all signify whether a person is a normal or suspicious citizen or terrorist that must be apprehended or eliminated. The ability to link one's communicative subjectivity with a terrorist profile can be the difference that decides whether a person lives or dies.

For once a suspect is flagged as displaying an abnormal or suspicious disposition and put into the database, they are marked as a subject to be captured or killed. The ever growing reliance on aerial drone strikes reveals the co-constitutive nature between surveillance and death; the same technology that is used for intelligence gathering is simultaneously a weapon of carnage and destruction that constantly moves between operating as a tool for data gathering and instrument of death.

Even with an ever-expanding system of government surveillance, it was still impossible for the government to monitor everyone at all times. Thus, the government needed to appeal to citizens to act as the eyes and ears of the national security regime. In this context, it was not enough that citizens merely consumed and conducted their daily lives in a transparent manner; the government also needed citizens to report on other citizens around them that they suspected of being a threat. Therefore, due to this need for type of citizen monitoring, a new mode of citizenship was formed based on the civic obligation that individuals have in rendering themselves transparent through actively participating in a culture of suspicion and surveillance. This new mode of citizenship is based in consumer participation that works as a flexible form of control that monitors consumer attitudes, behavior, and dispositions in order to detect abnormal activity. Citizens as part of their civic duty are asked to participate in monitoring and reporting of any suspicious activity. This civic duty to participate intensifies into an active citizen-detective role that may require investigations in order to help solve terrorist issues on behalf of the state. For example, this level of duty can be witnessed in the FBI's

solicitation of help to identify and apprehend the Boston Marathon bombers as well as the most recent attempts to identify masked Islamic State (ISIS) agents.

The harnessing of citizen's voluntarily efforts to render themselves transparent while actively monitoring, rating, and reporting on one another is a practice O'Reilly (2013) terms as algorithmic regulation. This is the attempt to use algorithms to monitor and preserve a form of homeostasis through the use of information and smart technology to discipline society. Understood in this way, algorithmic regulation functions as an austere and intensified form of biopower, where biopolitics and disciplinary power work together to monitor and preserve a state of homeostasis among the population. Both internal threats such as disease and reproduction rates as well as external threats such as war and terrorism must be monitored in order to ensure and preserve the population (Foucault, 1978). The population is then regulated through various laws and policies such as health and sex education campaigns or military policies concerning war. For example, speed limits are established on roads so as to best regulate the flow of traffic in as efficient and safe manner as possible. Thus, drivers are required to be within the speed limits at all times, else they risk being stopped and ticketed by the police. In this case, the government determines the values it wants to preserve in society and passes legislation and regulations that support the desired goals and outcomes; citizens who violate the laws are subject to penalization.

Unlike other guidelines or laws, algorithmic regulations are more concerned with how a system functions and its utility rather than upholding the letter of the law. To do this, algorithmic regulation works through a three-part process: measurement, outcome,

and regulation. According to O'Reilly (2013), the fundamental aspect of algorithmic governance is to "identify key outcomes that we care about as a society—safety, health, fairness, opportunity—encode those outcomes into our laws, and then create a constantly evolving set of regulatory mechanisms that keep us on course towards them" (p. 293). Government is conceptualized as a platform or base operating system that regulates and guides its population towards the telos established through its goal-oriented value process. Before use of algorithmic regulation, the government created rules and provides authority to specific agencies to enforce those rules. Yet, rather than achieving their goals, these rules were circumvented by parties who work to find loopholes or ways to use the letter of the law against itself. In contrast, algorithmic regulation seems to operate like Google, who, when confronted with new techniques by hackers and spammers, re-write the rules to ensure that the system operates smoothly without disturbances (O'Reilly, 2013).

O'Reilly (2013) argues that the general public is persuaded to accept specific types of regulation such as the US Federal Reserve and central banks that regulate the money supply to manage interest rights, inflation, and the overall state of the economy. The public assents to these policies because: "1. the desired outcomes are clear. 2. There is regular measurement and reporting as to whether those outcomes are being achieved, based on data that is made public to everyone 3. Adjustments are made when the desired outcomes are not being achieved" (O'Reilly, 2013, para, 5). In other words, regulation is accepted when it focuses on how something functions rather than if it follows the rules.

Thus, algorithmic regulation then becomes a powerful tool for governmentality. Whereas in a traditional biopolitical extension of governmentality, speed limits rhetorically invite people to accept the rules and regulations of what the government deems safe and those that decline the request are disciplined through tickets if the police catch them. Algorithmic regulation on the other hand uses constant data collection and surveillance to determine the best course of action. For instance, there are red light camera's appearing in cities that constantly monitor the speed of vehicles and determines if they are following proper traffic rules. If the camera system determines that a person has violated the law, then it flags the infraction and the owner of the vehicle is sent a ticket along with photographic evidence of the infraction. The automated response demonstrates how algorithmic regulation augments biopolitical power by coding in criminal infractions and the punishment. Thus, under algorithmic regulation, there is no need for human inspection and regulation, the system can function entirely without the subjective influence of human decision making. That is rather than rely on the whims of a police officer to enforce the rule of law, algorithmic regulation determines legal behavior and automatically takes action against infractions.

Algorithmic regulation is also capable of adapting parameters to ensure that the system is functioning smoothly. In continuing with the example of speed limits, the laws governing speed might be dependent on factors such as road conditions, traffic congestion, or weather (O'Reilly, 2013). Thus, for instance, speed limits might increase if a person is driving on a sunny afternoon on a highway that has very little traffic. The speed limit could also be decreased if it is a congested road and stormy weather. Further,

O'Reilly (2013) even envisions a future where information collected from road sensors, vehicle GPS, and other sources is used to determine and regulate the flow of traffic. If it is a high traffic area at peak time, then sensors can read a vehicles license plate and automatically charge the vehicle a fee for using the road; during light traffic situations, the system can reduce or eliminate the fee to ensure effective regulation.

The government as platform model operates under the values of collaboration, openness and transparency (O'Reilly, 2013). In order to best regulate its population, a government must have access to as much data and information on its citizens as possible. The more data that is collected, the more new statistical overviews and predictive models that can be created to understand the status quo. As a result, the use of data collection can transform how the government works as a platform. Moreover, the government can be viewed as regulating a series of financial investments in society. If viewed as inefficient, government programs should be either defunded or re-routed into a more efficient program. However, in order for government to operate through algorithmic regulation, it requires that information collected for data is freely available to all. For instance, O'Reilly (2013) makes the argument that the financial industry depends upon disclosure of information and therefore open data would make the market more "transparent and self-policing" (para. 4). Hence, an open subjectivity based on surveillance and transparency requires that citizens allow their data to be collected, used, and be openly available. This is necessary so that government data can be given freely to private companies, which then create new services to provide to the citizen-consumer.

In an algorithmic regulation system, crowdsourcing seems to be the method by which the government is able to outsource the work of securitization to the citizenry. Crowdsourcing is when the public is asked to provide ideas, content, or services as opposed to a single individual or a company. What was once work performed by employees of a company or institution is now outsourced to a large number of people who can work collaboratively, harnessing the labor power of large aggregates of people by a select few (Tewksbury, 2012). Therefore, crowdsourcing may mark a new mode of biopolitical control where the relation between the citizens and the state are rearticulated so as to place the burden of safety and security onto the citizens instead of the state (Tewksbury, 2012). For instance, during the Cold War, citizens used to practice sitting under their desk or walking single file to a bomb shelter in preparation for a nuclear war. In comparison, citizens now actively participate in monitoring their surroundings and work to prevent terrorist attacks (Tewksbury, 2012, p. 260).

The rhetoric of collaboration, openness, and transparency work together to constitute a new mode of citizenship designed to harness the affective and immaterial labor of citizens directing their energy towards participation in goal-oriented decentralized networks. The connected and transparent government is one that "harnesses the collective intelligence" of its citizens through the collection of all data and information (O'Reilly 2013). This new mode of citizenship, what I call algorithmic citizenship, is one that works through cultivating a new means of public engagement based on crowdsourcing and participatory collaboration. For example, O'Reilly (2008) argues that citizens are smarter because they have access to smart technologies. The fact

that a citizen can instantly ask a question on Google or Twitter, crowdsource on Facebook, use Wikipedia or an algorithmic recommendation on purchases through Amazon provides citizens with the ability to consume and share information at levels completely unprecedented in history. Therefore, access to information becomes a new civic obligation: one must participate in sharing and making communication public and accessible through social media. The fact that citizens can engage with each other in dialogue or debate on various websites provides participants a platform to voice their opposition or support and connect with others to take action on various issues (O'Reilly, 2013). For instance, O'Reilly envisions a participatory culture where online debates provide the ability to share the data that informs individuals' convictions and personal beliefs. Not only can a person make an argument on social media, but they also have the ability to post a link to an article that serves as evidence to support their claim. O'Reilly (2008, November) contends that algorithmic regulation allows for individuals to share the "code in their head" because hyperlinks are "source code for your thinking: that's a meme that should survive the particulars of this particular debate!" Under this theory, information is important because it fosters a democratic subjectivity based in informed debate and participatory action. These actions of algorithmic regulation require the immaterial labor of reviewing and rating every experience. Put differently, the sharing economy may depend on consumers providing their labor for no compensation other than the possibility of future convenience or improvement in services. Thus, algorithmic citizenship appears to depend on citizens forming connections to take on the civic obligations of the community and state to address various problems. Therefore, the

immaterial labor of appraising everyday actions, products, and services may become a way in which citizens can connect with one another to take on issues otherwise left for government.

Literature review

In order to study the emergence of algorithmic citizenship and government 2.0 in the war on terror era, it is important to contextualize my argument within existing literature. A number of fields have made important scholarly contributions to the study of citizenship, security, and surveillance, particularly since the attacks of 9/11. Most relevant to my inquiry into the development of algorithmic citizensahip and government 2.0 are humanistic studies of the state of democracy and the constitution and function of citizens within our contemporary configuration of American democratic culture. Within this discussion of the relevant literature in the field, I discuss a number of interrelated issues about media effects, security, and more broadly about the conduct and nature of the war on terror.

Deliberative democracy. Rhetorical scholars have done considerable work in exploring the relationship between citizenship, consumerism, surveillance, and war. The vast majority of this scholarship tends to focus on how consumerism and representational democratic practices rhetorical produce a passive and docile citizenry. For example, Jennifer Mercieca (2010) provides a useful heuristic for classifying rhetorical theories based in their relationship to the "decline hypothesis," an argument that citizens' active engagement with government is in decline. Analyzing political fictions, Mercieca (2010) argues that the citizen's relationship to the state is one that has been constructed through

republican values that, over time, came to be understood through the moniker of democracy. For example, before the Revolutionary War, citizens were interpellated under a paradigm of romantic citizenship where heroic and rugged individuals were called upon to revolt against the English monarchy in order to establish a new system of governance. After the Revolutionary War, there was a great deal of political discourse advancing a fear of democracy because it was viewed as chaotic and instable, leading political leaders to cultivate a representational republican system rather than a direct democracy. As a result, citizens were constituted as victims within a tragic scene where the fearful Hobbesian state of anarchy required citizens to submit themselves to the state in order to promote order and stability (Mercieca, 2010). Furthermore, citizenship was deployed through ironic partisans where the heroic citizen patriots submitted to a political party system that would restore order and best represent the people (Mercieca, 2010). These fictions were founded on an exceptionalist trope that posits Americans as the chosen people called upon by God to be a city on a hill; however, Americans were not living up to their covenant or potential and thus needed the order and stability offered by the republic (Mercieca, 2010).

Robert Ivie (2005) interrogates a similar distrust of the people by examining a discourse of "demophobia." According to Ivie (2005), this rhetoric reinforces the idea that citizens are not well-suited to participate in deliberative democracy and, instead, is best engaged in by cultural, economic, and political elites. According to the discourses circulating at the time of the founding of the nation, citizens were easy prey to chaos and demagoguery. As a result, there was tremendous fear of citizen revolts and the idea of

direct democracy. Examining the current war on terror situation, Ivie (2005) explores how the Bush Administration's discourse perpetuated this demophobia by conjuring up the fear of a radically evil Other that could infect Americans with its terrorist ideology. Thus, democratic deliberation was regulated as a rational activity best reserved for the professional elites that were not subject to the irrational passions of the masses. Rather than engage directly in government, citizens were to participate through a representational system of republican governance and acquiesce to the war on terror. Instead of engaging in deliberation and debate, citizens affectively invested in the experience of security and "a politics of quiescence and coercion" to war (Ivie, 2005, p. 6 & 151).

Building on the logic of citizen passivity, Jeremy Engels and William Saas (2013) examine how war rhetoric works through a two-fold typology of assent and acquiescence rhetoric. Assent rhetoric works to gain the public's consent and participation in war. To this end, Engels and Sass (2013) point to the discourse used regarding Iraq having weapons of mass destruction, the demonization of al Qaeda, and other attempts to persuade the public into supporting the war. In comparison, acquiescence rhetoric works by diverting citizen's attention away from war and towards consumption. For instance, Engel's and Saas (2013) draw on the misquoted statement from President Bush telling people to go to Disney World as an indication that the public was encouraged to consume and therefore leave the war planning to the professional elites.

While these rhetorical scholars offer important insight into how rhetoric functions as a tool to disempower citizens, this study aims to supplement and update an

understanding of citizenship, surveillance, and war rhetoric by analyzing the interactive rather than passive approach of government 2.0. The logic of demophobia casts suspicion on citizens, authorizing surveillance as a means to monitor and control the population. While it is important to consider the ways in which rhetoric might operate to control the citizenry, such an exclusive focus might not appreciate the ways that the public actively participates in the production of American exceptionalism and militarism. It seems unlikely that citizens are merely passive dupes who are no longer publicly engaged, particularly in the age of modern social media. Thus, this project joins rhetorical scholars such as Kevin Michael Deluca or Ronald Greene in examining the ways in which digital communications constitute new formations of publics and helps map how these publics communicate and participate in government. Furthermore, scholars should be attentive to the economic logic accompanying governmentality as it may foster a cultural citizenship that collapses the classic binary between the elite who govern and the public who is governed. Analyzing cultural citizenship allows rhetorical scholars to better map how public engagement has been altered while examining the new modes in which it might operate.

Cultural citizenship. Studies of cultural rhetorics of citizenship have identified how two modes of subjectivity have been forged (Miller, 1993). Toby Miller (1993) for instance explains these two types as: "the selfless, active citizen who cares for others and favors a political regime that compensates for losses in the financial domain; and the selfish, active consumer who favors a financial regime that compensates for losses in the political domain" (p. 130). Taking up how mass media technologies such as the

television altered citizens' relationship to the state, Miller (1993) posits that mass media work to situate citizens as consumers in need of democratic training. Prior to this classification, one of the dominant theories of citizenship was understood as having a debt to the state, which in return provided a welfare system that afforded a minimum standard of living. The creation of mass media altered this conception of citizenship and moved it away from a welfare system to one in which citizens were afforded access to the technologies of citizenship such as television. The state provided public broadcasting and public congressional hearings on channels such as *C-Span* that cultivated citizenship with a passive yet receptive engagement with the state. In other words, mass media worked to produce a mode of cultural citizenship through which the state provided the means for citizens to watch, learn, and educate themselves about the political process.

In particular, Stephen Klein (2005) takes up the issue of post-9/11 war films as a market in which consumerism provides the viewing audience the perception of the citizen-soldier and the cultural values that are entailed in that visual experience. For example, according to Klein (2005), the 2001 film *Black Hawk Down*, released following the 9/11 attacks, discourages critical examination of war by excluding the historical context that lead to a U.S. military presence in Somalia in 1993. As a result, the audience views the film in relation to the attacks on 9/11 and can project their current anxieties about the war on terror onto the film. In conclusion, Klein (2005) argues that the narrative, devoid of historical context, constitutes the "reality" of U.S. military involvement in Somalia for many media consumers. The film's lack of historical context invites civilian audiences to rhetorically identify with military soldiers and their

operations rather than question the bureaucrats and politicians who orchestrate the war on terror (Klein, 2005). Besides being strategically released after the attacks of 9/11, *Black Hawk Down*'s production was, by a large part, made possible by the U.S. military. For example, the government provided Black Hawk helicopters, satellite images from actual battles, and troops to act in the film and perform routine stunts. Through this realistic filmmaking, the narrative spun by the film depicts heroic soldiers and embodied characters who the public can see and identity with as patriotic solders while they immerse themselves as a viewing audience. While courageous battles take place on screen, the bureaucratic configuration of military power is disembodied and inarticulate to the public.

Roger Stahl (2010) further tracks this relationship between consumption and war as constituted through a new set of discourse and practices that he terms "militainment." According to Stahl (2010), militainment refers to the assemblage of entertainment, media, and military industries such as movies, sports, and video games that all work together in the production of an interactive virtual-citizen soldier. Rather than provide spectacle where discourses control public opinion by distancing, distracting, and disengaging the citizens from the lived experiences of warfare, these new modes of entertainment allow consumers to actively consume and interactively engage in warfare. This interactive mode of war operates through the combination of active and passive consumption and the production of pleasure accompanying the consumption process. In order to consume a product, citizens passively provide their personal information (e.g., registering online to play video games, purchasing tickets on Stubhub, making purchases on Amazon.com).

Passive consumption becomes active when citizens then directly participate in the entertainment process (e.g., playing interactive first-person shooter video games like *America's Army* or *Call of Duty* or attending a sports event). When players connect online and play *America's Army,* they are not simply watching moving images but are wiring themselves into a fantasy of participating in the routines of war. This is for Stahl (2010) how modern citizenship functions by seducing individuals into expending their energies through prescribed activation of militarized subjectivity through banal acts such as playing video games or attending a sporting event.

Similarly, Stahl (2006) also discusses the production of the virtual citizen-soldier, the hybrid subject formation emerging from the third sphere of cultural production that blurs the line between civilian and soldier in much the same way as a video game. The virtual citizen-soldier participates in a simulated space that is created through the conglomeration of military and consumer entertainment culture that removes citizens from the realm of public deliberation and instead immerses them into the cogs of the machinery of state violence. The traditional divide between the informed civilian who engages the political process and the soldier who follows orders outside the political process is blurred as the citizen becomes an active participant adhering to the logic of Netwar (Stahl, 2006). Within Netwar, citizens are taught that their daily activities are now part of the war on terror. If their daily experiences and performances of subjectivity are essential to fighting the war on terror, then citizens are no longer in a realm of public deliberation; rather, they are interpellated to answer the call of duty and follow the chain of command.

Stahl (2006) isolates several factors that produce the virtual civilian soldier. First, there is the blurring of the traditional binary between civilian and soldier. Second, there are video games that reproduce a social and geographic field that then plunges the citizen into a military role. Third, there is a cultural shift away from the passive interactivity of watching television or movies to an interactive virtual world in which citizens immerses themselves in an active virtual environment. As Stahl (2006) writes, "game time integrates the citizen, however virtually, into the mechanics and pleasures of 'how we fight'" (p. 110). As a result, the citizen participates in a sanitized version of war. For example, Stahl (2006) maintains that we can understand the experience and noise of looking through night vision goggles in a game, but we do not see the material flesh and blood of mangled bodies. Instead, the virtual war is merely an outlet for fantasy projection in a safe and sanitized environment. Therefore, Stahl (2006) argues that the Pentagon's ability to claim that *America's Army* and other similar war video games are authentic provides a newfound rhetorical legitimacy to the virtual citizen-soldier subject position.

It seems rather likely that once constituted into the virtual citizen-soldier subject position, this subjectivity can be extended and intensified into an actual citizen-soldier subject. If that is possible, then the war on ideology may require specific articulations and performances of an active citizen subjectivity designated through a new mode of governmentality. While Klein, Miller, and Stahl analyze how neoliberalism produces a form of cultural citizenship that conditions the public to accept and support war, they all constitute the public as passively participating in the formation of their subjectivity. For

example, Miller assumes that the public is submissively controlled through the use of television, Klein examines how movies promote patriotic subjectivities discouraging dissent, and Stahl examines how video games work to produce disengaged passive virtual citizen-soldiers. In all of these instances, the public is still being manipulated by the rhetorical force of government and media agencies. If citizenship is articulated through active consumerism, then rhetorical scholars should examine how consumerism itself is being reconstituted through a postmodern capitalist logic. Because postmodern capitalism works to dissolve traditional boundaries such as civilian/soldier and inside/outside, it becomes important to understand how consumerism may promote an active form of public engagement that is capable of producing citizen-soldiers who directly participate in maintaining national security.

Citizen-soldier. Moving away from the concept of a virtual to actual citizen-soldiers, Ronald Krebs (2009) analyzes how the citizen-soldier is manifest within neoliberalism. Throughout American history, the citizen-soldier is a rhetorical construction deeply embedded in the formation of American society. For instance, it was the colonial citizens who rose up, formed voluntary militias, and fought against the British. After the Revolutionary War, the citizen-soldier was a familiar rhetorical trope in that the U.S. had a policy of mass conscription where a large standing army comprised of male citizens could be drafted by the government. According to Krebs (2009), American cultural, economic, and military contexts constitute citizens-soldiers who were good citizens willing to sacrifice their lives on the battlefield for national unity and the promotion of political community.

Under the classic citizen-soldier trope, citizenship was conceptualized as the mutual claims of rights and obligations that co-constitute the government and governed. Citizens are afforded the privileges that come from being members of a political community but, in exchange, they must fulfill their civic duties such as paying taxes and voting in elections. This conceptualization of the citizen-soldier would then appear to be completely divorced from the political reality today of the presence of an all-volunteer military force. Thus, Krebs (2009) contends that the citizen-soldier needs to be re-conceptualized as "a set of rhetorical conventions to which social and political actors, both claimants and authorities, give voice" (P. 161-162).

Following Krebs' (2009) suggestion, I maintain that we should examine the citizen-soldier through a theoretical lens of rhetorical materialism to investigate the public expression of conventions that are observable and challengeable and the silences that the conventions invoke. Krebs (2009) argues that we should understand the citizen-soldier trope not through the decline thesis predicated on the disbanding of the standing army; instead, it should be examined through the economic and political relations that work to govern bodies through citizenship. For instance, drawing on the historical development of the military and military service, Krebs (2009) notes that, despite the claim that good citizen-soldiers are people who repaid their debt of citizenship by joining the armed forces, most economically- and socially-privileged members of a society avoid active military service and this obligation is most often covered by the least privileged members of society.

The move away from conscripted to volunteer military forces can be seen as a neoliberal expression of how citizenship, surveillance, and warfighting were going to be redeployed later. Moving away from the system that forced most citizens into the previous configuration of citizen-soldier trope, neoliberalism has added more nuanced to this trope by reconstituting it through deep cuts to traditional military personnel and the promotion of mobile and floating military bases that exist anywhere and everywhere and increased use of privatized forces such as operated by Blackwater (Krebs, 2009). Blackwater is a private security company that provides security operations and served as a paramilitary group. The company was founded in 2002 and initially operated by providing the CIA with security and the tracking of Osama bin Laden in Afghanistan. The agency was awarded an independent defense contract in Iraq in 2003. The organization came under congressional and media scrutiny after reports that it had been involved in at least 195 "escalation of force" incidents in Iraq, shooting almost one and a half people a week despite the fact that its contract was for defensive purposes only (House of Representatives Committee on Oversight and Government Reform, 2007).

Joan Faber McAlister (2010) argues that, beyond the structural changes noted above, popular culture also works to transform American citizenship into a product of neoliberalism and neo-conservatism. Taking the show *Extreme Makeover* as her point of analysis, McAlister (2010) argues that political practices are being domesticated in a move that relocates social responsibility away from individuals and towards corporate institutions. As a result, citizenship is reduced to consumerism as the viewing public is bombarded with messages to associate the problems of social life as manifesting in one's

home. From this perspective, good citizenship is articulated through a combination of traditional patriotism and neoliberal subjectivities. For instance, the good citizen performs traditional tasks such as volunteering for corporate charity or the military. This subjectivity is also one that works to quash dissent by bracketing out questions about the need to militarize the home. For example, why would we support the rebuilding of a soldier's home instead of questioning why the soldier was sent to war in the first place? James Hay (2007) similarly argues that the war on terror fostered a new take on the idea of the rugged individualist subjectivity embedded in American citizenship. Post 9/11, citizens were told to value active self-defense and to take care of themselves in the event of another terrorist attack. Within this discourse, citizens were told to stock up on duct tape and water and go to private websites so they can best educate and prepare themselves for their future security needs. The message of individual preparation is one that is fostered in the shows that promote the belief that individuality and the civic participation are essential actions in context of the war on terror (Hay, 2007).

In addition to promoting domestic preparedness, war on terror discourse also demanded that citizens remain constantly informed, prepared, and vigilant (Andrejevic, 2007). Citizenship operates around a neoliberal mentality of risk assessment where the threat of terrorism is so expansive and ubiquitous that citizens must constantly participate in the regimes of surveillance while simultaneously monitoring those around them. According to Andrejevic (2007), this operates as two forms of participation in the war on terror: "interpassive [form] where data of every transaction, every purchase, and every movement is aggregated within the government equivalent of the demographic database;

and the interactive form, in which citizens are encouraged to take responsibility for their role in the war on terror even as they go about their daily lives at work, at home, and at school" (p. 173). Thus, by collecting as much information and data as possible, the government is able to use digital data to connect to material bodies in determining normal consumptive patterns from abnormal terrorist activities.

Drawing from Foucault, Jeremy Packer (2007) argues that the technologies of biopower and normalization provide insight as to why war becomes "the binding and organizing mechanism for reconstructing society according to logic of national security under the auspices of the Office of Homeland Security." According to Packer (2007), the futuristic turn towards predictive algorithmic modeling and biopolitical impositions that pathologize criminality combine to constitute the "subject" of Homeland security. As a result, the war on terror becomes a modern day extension of the "race war" described by Foucault. In both examples, the nation-state has to protect the population both within and outside of its territorial boundaries. Because threats can exist both inside and outside of the territorial boundaries, the distinction between friend and enemy is blurred. Thus, the state engages in the risk management strategies of national security in ways that reorient criminality to predictions of dangerousness (Packer, 2007).

Predictive algorithmic modeling appropriates security in order to rhetorically demarcate the population. Under the auspices of preserving and maintaining the security of the population, the state must rely on the information collected and produced through surveillance and apply a "mathematical topoi derived from algorithms that weigh the individual's freedom against the population's safety, transforming all life activities into

calculable risks that function according to economic rationalities" (Chaput, 2010, p. 5). In order to identify an individual's capacity for terrorism, the state relies on predictive algorithms and surveillance technologies to determine the probability that a person being examined is a "terrorist subject." Using a variety of technologies such as biometric facial recognition networked to computer databases, the state creates a futures market for predicting when and where future terrorist attacks might occur. Furthermore, data such as credit scores and other financial information is collected by the state to determine an individual's likeliness of being a terrorist (Packer, 2007). Moreover, once a suspect is determined to be a likely terrorist who is on foreign soil, their data is tracked and becomes an identifier used to target and kill. The collection of big data and mass surveillance dragnets formulate statistical models of citizen ab/normality. Even seemingly normal acts of consumption still provide statistical indicators as to what constitutes a standard of normality. For example, this is precisely the advertisement made by American Express: it will monitor and tack your spending so that it can learn your habits. Of course, the monitoring of daily transactions provides a level of financial security if someone steals your information and attempts to make an illegal purchase. However, the flip side of this policy is that the banks and credit card companies monitor your spending to create an algorithmic profile that they use to determine a person's normal spending habits. Because an individual engaging in acts of consumption is always simultaneously producing information and data about him or her selves, this data is collected and used by national security agencies to determine who is or is not a likely terrorist suspect. Therefore, when citizens are not directly fighting terrorists, they are

working to identify terrorists through the production of information that works to form normalized consumption patterns (Packer, 2007).

In later work, Packer (2014) maintains that surveillance technologies and practices are transforming social power through the automation of immaterial labor. The immaterial labor of seeing, sensing, and feeling are frequently being redirected from activities that humans engage in to ones that are performed by machines. This alters the field of surveillance substantially as human bodies themselves are diminishingly targeted for surveillance (Packer, 2014). Rather, machines are automating surveillance against other machines in that what they are really monitoring is data and images. For instance, a computer will analyze the financial data of various users to determine the likelihood that the individual attempting to complete a financial transaction is a terrorist. The actual human body itself is no longer the site for objectification as it is digital data that is being placed under surveillance. While displacing the body in some sense, the synecdoche of data for physical bodies still has significant consequences for the material body in that if one's data is flagged as belonging to a terrorist subject, the body is then targeted for detainment or execution. According to classified documents released by Edward Snowden, a former drone operator for the military's Joint Special Operations Command and intelligence officer of the NSA, and the testimony of Brandon Bryant, a former drone sensor operator with the Air Force, the U.S. uses geolocation of SIM cards and metadata to target and kill suspected terrorists (Scahill & Greenwald, 2014). Indeed, the use of metadata to determine the enemy led to one particular NSA unit adopting the slogan, "We Track'Em, You Whack 'Em" (Priest, 2013). Moreover, intelligence agencies such

as the NSA monitor cellphone metadata to determine who a suspected al Qaeda operative was and where they were located. Once identified, drone strikes were then authorized based not on the physical surveillance of bodies but through the collection of data and surveillance. This produced the tragic consequences where civilians would be killed in a drone strike because a terrorist suspect happened to use their cellphone or because a civilian used a cellphone whose geolocation was associated with a potential terrorist (Scahill & Greenwald, 2014).

While Andrejevic, Hay, Krebs, McAlister, and Packer all theorize how neoliberal rhetorics work to constitute citizen-soldier subjects, this project seeks to supplement their work by assessing how consumerism is an active process by which citizens participate in the production of valuable information in the identification, targeting and elimination of terrorist. For instance, Hay and McAlister both replicate a passive demophobic view of citizenship where neoliberal rhetorics work to persuade citizens to incorporate security matters into their domestic activities and practices while ignoring the active role that consumerism plays in the formation of citizenship and public engagement. In comparison, Andrejevic and Packer provide great insight into how cost-benefit analysis and algorithmic modelling have become a way in which citizenship is articulated with national security and the war on terror. Packer (2014), for instance, wants to reclaim a sense of human agency which can then be used to formulate a more traditionalist Marxist alternative to the war on terror. In his reasoning, if surveillance is automating warfighting, then soldiers can become a unified group of people who are capable of rallying together to struggle against the automation of labor. Yet, this strategy seems to

advance a technophobic model of citizenship rather than theorizing how citizenship can be accessed through several modalities that are not a result of passive automation through technology. It also diverts attention away from the way in which humans themselves actively contribute and participate in the practices of national security such as drone strikes or the ways that privatized paramilitary groups form. Therefore, while these scholars have valuable insight into the ways in which surveillance and warfighting are conducted under our contemporary neoliberal order, this project works to supplement this research by also examining the ways in which people actively enact their citizenship to better understand how the current techniques of governing and national security operate and the possibility of resistance with them.

Citizenship as performance/discourse. So far, I have focused on the ways that rhetorical scholars have directed their energy towards understanding how people identify with particular tropes of citizenship such as the citizen-soldier. Changing trajectories slightly, this I now examine how scholars offer a different conceptualization of citizenship that is less concerned with identifying with specific subject positions and is more interested with the ways that citizens actively use language and subjectivity to enact agency. Robert Asen (2004), for instance, argues for a discursive theory of citizenship that reorients our examination of citizenship away from what legally counts as citizenship towards investigating various enactments or performances of citizenship. According to Asen, the citizenship-as-legal status/legal possession perspectives are so entrenched that they represent the only definition of the word "citizenship" in the dictionary. For example, the *Oxford English Dictionary* defines citizenship as "the position or status of

being a citizen, with its rights and privileges" (as cited in Asen, 2004). Yet, this understanding of citizenship is rather exclusive and fails to attend to a wide range of practices that makes one count as a citizen (Asen, 2004).

Yet, citizenship, even when conceptualized as a legal category that one occupies, requires citizens to perform a particular way in order to be intelligible as good citizens. For example, David Lyon (2009) provides an example of Slovenia's independence in 1991 in which bodies that did not render themselves intelligible were therefore moved to the periphery and outside of consideration as legitimate actors. When Slovenia became a country, residents who lived there had six months to apply for citizenship and those who did not were purged from the registry, thus denied the privileges and rights of citizenship and were forced into a life of exile as stateless refugees. More recently, in 2006, the United Kingdom passed the Immigration, Asylum and Nationality Act allowing dual nationals to be deprived of their British citizenship if the Secretary of State is "satisfied that deprivation is conducive to the public good" (Corbin, 2013, p. 31). As a result, the British government is able to denationalize dual citizens by claiming that citizenship is a privilege one earns and not an inherent right. Likewise, the U.S. is not immune from consideration of legislation designed to revoke citizenship. For instance, the current popularity of Republican presidential candidate Donald Trump or Rep. Steven King's (R-Iowa) idea to revoking automatic birthright citizenship. King's legislation would call for at least one parent to already be a citizen in order for a child to be provided with citizenship (Marcos, 2015). These efforts rely on the racist construction of anxiety about "anchor babies," children who are granted automatic birthright citizenship born by

noncitizen parents in hope that the child will help the parents' application for citizenship or legal residency (Marcos, 2015). Regarding national security, the Department of Justice filed to have Enaam Arnaout's citizenship status revoked because he provided material support for bin Laden and the Mujahideen when they were fighting the Soviets in the early 1990s (Janssen, 2014). Additionally, Sen. Ted Cruz (R-Texas) has submitted the Expatriate Terrorist Act, which would provide the government with the legal justification for revoking citizenship of any American who joins or aids a foreign terrorist group (Chapman, 2014). While citizenship is constitutionally protected as a right of birth in the U.S., there is public discussion about attaching contingent stipulations based on the performances that citizens enact.

The audience, content, and manner with which an individual communicates materially implicate that person as a good citizen or a criminal who is to be denied due process. Take for example 2012's Statute 18 U.S.C. 2339B, "Providing Material Support or Resources to Designated Foreign Terrorist Organizations", which defines certain speech acts as constituting material support for terrorist organizations:

> The term ''material support or resources'' means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials; (2) the term ''training'' means instruction or teaching designed to impart a specific skill, as opposed to general knowledge; and (3) the term ''expert advice or assistance'' means advice or assistance derived from scientific, technical or other specialized knowledge. (p.542)

Furthermore, the Supreme Court ruled 6-3 to uphold the criminalization of speech in *Holder v Humanitarian Law Project* (2010). This decision legally solidified prohibitions against material support for terrorists, even if the support is in the form of peaceful counsel directed towards conflict resolution, human rights advocacy, or international law instruction (Kaminer, 2010). Justice Roberts, writing the majority opinion, argued that even training in non-violence or international law to resolve disputes would provide terrorists with information and techniques that could then be used in a broader strategy to promote terrorism (*Holder v. Humanitarian Law Project*, 2010). For instance, teaching terrorist organizations to petition international bodies for relief might help them to obtain funding which could then be used to further terrorist activity. Moreover, Justice Roberts stated, "that Congress chose knowledge about the organization's connection to terrorism, not specific intent to further its terrorist activities, as the necessary mental state for a violation" and, as such, a reasonably intelligent person would know that the organization they were communicating with was a terrorist organization and thus the speech would be criminalized as providing material support (*Holder v. Humanitarian Law Project*, 2010, p. 6). Consequently, citizens' communication with a terrorist organization manifests materially as a form of criminal engagement that can be used to apprehend citizens without due process and, if on foreign soil, execute them via drone strikes. Thus, this legal precedent exposes a move away from a traditional legal and liberal model towards a public engagement and performance as citizenship model of citizenship.

In contrast to the state's focus on specific performances, Asen (2004) conceptualizes citizenship as a mode of public engagement. From his perspective,

citizenship is a performance rather than a possession of the citizen (Asen, 2004). Similarly, Greene (2001) describes the rhetorical citizen as one with the attributes necessary for making and critiquing good reasons. As a result, public engagement is always a process of risk and vulnerability. Butler (1996) further argues that a form of power that constitutes subjects as citizens is a process of subjection where we depend on the discourse that we did not choose but nonetheless "initiates and sustains our agency" (p. 2). When one makes an argument and tests it publicly, they run the risk of being changed, vulnerable, or wrong through the process of engagement (Asen, 2004). Thus, public undertakings are rhetorical in that they position people as rhetorical agents hoping to persuade or seek recognition of their views from others, even as they recognize that others hope to do the same. The process of public engagement is fraught with risk and vulnerability because it requires that one open oneself up to encounter and be encountered by difference; it is to interact with others of different beliefs, experiences, perceptions, and worldviews. Hence, engagement encourages people to step away from familiar territory and into uncomfortable situations, encountering difference where one's own beliefs, perceptions, and worldviews are questioned. This fosters an appreciation of the social in that the legitimacy of one's worldview is depending on the recognition of others (Asen, 2004).

As a result, citizenship as a performance is not confined to the privilege of membership or a set of rights granted by an external authority. Rather, citizenship is enacting agency and is something that can be performed even by those who are classified as "non-citizens" (Asen, 2004). Additionally, citizenship is multimodal in that it can be

enacted in different ways by different people. Connecting citizenship to public engagement has the rhetorical dimensions of focusing on subjectivity and publicity. Rather than bodies articulated together through assemblages of globalization, membership, nationality, and neoliberalism, a discursive theory of citizenship is one that allows for examining subjectivity as a multiplicity outside of a fixed and essentialized subject, one who is always- already interpellated and positioned into a binary of citizen/non-citizen. Instead, subjectivity becomes a process that disrupts fixed characterizations and memberships based on identities and belonging, thus allowing alternative articulations to form.

This project works to supplement a discursive theory of citizenship, adapting it in relation to postmodern capitalism. According to Frederick Jameson (1991) and Jeffery Nealon (2012), the "work on oneself" and self-help form of subjectivity is transcoded and cannot be disassociated from neoliberal capitalist subjectivity. When considering how citizenship is multimodal and can be enacted differently by different people, rhetorical scholars should take into consideration how big data allows for the corporate and governmental mapping of these performances under the mantra of personalization. Greene's (2004) focus on rhetoric as immaterial labor can be used to theorize big data and personalization. If we direct our focus to how rhetoric is a form of life-affirming labor, we can see that communication is part of the biopolitical production of life. The role of communication in this process means rhetorical agency can be abstracted and captured to perform work such as rating products or providing personal information to access websites. However, Greene (2004) claims that not all of labor's value can be

abstracted and captured. Instead, focusing on the constitutive power of rhetoric suggests that a different politics is possible, one where: "a common creativity and invention, a productive excess and joy, the material immanence of democracy" (Greene, 2004, p. 204). It is in this alternative conceptualization of rhetorical agency that I find the theoretical tools to analyze the relation between immaterial labor and the algorithmic regulation of government 2.0.

Guiding questions

In order to follow how algorithmic citizenship is constituted and enacted, this study maps the various modes of public engagement that are called forth through corporations, government, and publics. Following the rhetorical circulation of this construction through these venues allows me to examine the complex forms of subjection that occur around citizenship. In theorizing algorithmic citizenship, this project explores the grid of intelligibility that may be produced through corporate and state governmentality while simultaneously examining how citizens may actively constitute their own subjectivity. Rather than conceptualizing citizens as merely passive consumers who are subject to the whims of corporations and government, it is likely that this new mode of citizenship is produced through a government 2.0 logic that calls forth an active citizen subject who participates in its relations of subjection and governance. To explore the ways that citizenship may be enacted through government 2.0, this project addresses several research questions.

What form of citizenship is promoted under government 2.0? This theorization of algorithmic citizenship outlined follows the work of Tim O'Reilly who

coined the terminology "government 2.0" and "algorithmic regulation." The rhetoric of government 2.0 and algorithmic regulation may work to provide insight into the identification of citizens as communicative subjects. Chapter 3 examines IBM as a case study that maps how IBM may implement government 2.0 and algorithmic regulation into a specific form of governance based on the gathering and analyzing communications and then formulating predictive strategies for dealing with both national security and the policing of communities.

How does government 2.0 regulate citizens through the rhetoric of national security? The attacks on 9/11 may have caused a shift in how government officials and agencies implement policy initiatives based on the collection of communications and participation of the citizenry. Chapters 2 and 4 follow the speeches of Presidents Bush and Obama to map the shift in increased surveillance, predictive warfare, and the emergence of terrorist-citizens—citizens who are radicalized or persuaded to identify with a terrorist ideology or disposition. In analyzing these speeches, these chapters explore the ways in which terrorism has moved from an external threat into a domestic internal ideological struggle waged through the communications, dispositions, and performances of citizens.

How does the public enact algorithmic citizenship and participate in government 2.0? In order to respond to this question, the dissertation scrutinizes the ways in which the public enacts citizenship through contributing immaterial labor in the name of national security. This study maps the ways that citizens may participate in government 2.0 through crowdsourcing of the war on terror. Specifically, I follow the

digital communication practices of the members of the public who participated in IBM's interactive THINK exhibit, as well as the FBI crowdsourcing directed to capture and apprehend of the Boston Bomber. Finally, this study examines how the act of whistleblowing on government surveillance constitutes a way that citizens enact algorithmic citizenship through the rhetorical tropes of transparency and openness.

Addressing these question can make a number of potential contributions to various fields interested in citizenship, security, surveillance, and digital culture. For those interested in citizenship studies, examining algorithmic citizenship allows scholars to map the changing terrain of public engagement. This is pertinent for scholars in the fields of communication, sociology, and political science in that digital communication is capable of calling forth new forms of speaking subjects whose everyday mundane communications are capable of reaching large audiences and can be monitored to determine one's disposition. Moreover, algorithmic citizenship has implications for those interested in the workings of government. For example, the development of smart technologies now posits new modes of relations between those that govern and their publics. The ability to connect and communicate with those who govern and the development of government 2.0 may constitute a new configuration in how citizenship and governance function. Finally, this study might be of interest to citizenship scholars as it traces how citizenship may be rhetorically redefined away from a right of birth into a privilege based upon a new patriotic duty of speaking and performing in a manner that might be deemed as acceptable by those who govern.

Reading an algorithmic citizen subject

The articulation of biopolitics, consumerism, citizenship, neoliberalism, surveillance, and war rhetoric constitutes and transforms individuals into communicating rhetorical subjects. The rhetorical subject is one that "speaks and is spoken to" (Greene, 2009, p. 49). Rhetorical materialism seeks to describe how the, as Greene (2009) states, "persuasive, deliberative, educational, technological, and/or aesthetic dimensions of communication are integral to the articulation of regimes of value" (p. 49). The value produced through communication is inextricably tied to the fashioning of specific forms of communicating subjects. For instance, rhetorical subjectivity operates through specific regimes of production and is valued for the labor it both can and cannot accomplish. This is particularly important for this study because the rhetorical subject traverses the citizenship apparatus (Greene, 2009). Algorithmic citizenship relies upon the circulation of affect to regulate persuasive capacity through the production of experiences of security, technological advancement, entertainment, and civic duty. The circulation of these discourses and techniques produce value through the transhistorical and transsituational exchanges, the whole of which govern individual and collective decisions (Chaput, 2010).

Using rhetorical materialism as a lens, rhetoric can be understood to produces value in everyday practices the same way that general consumer practices generate political economic value. O'Reilly (2010) argues that algorithmic regulation and concepts such as government 2.0 model the policies and institutional set-up of companies such as Amazon, Craiglist, eBay, Facebook, Google, Twitter, and Wikipedia because they are all successful in harnessing the immaterial labor of its users to add value and co-create its

products. To bring this back to rhetorical materialism, these companies appropriate the immaterial labor of their users, such as their data and information, in order to improve commercial or governmental success. Individuals are interpellated into specific rhetorical subjects who communicate their personal information to be used by corporations and government agencies. Then the information that is collected for the purposes of consumer advertising also can be shared with or collected by governmental agencies for the purpose of national security. Thus, the mundane act of everyday communications produces value for companies or governmental organizations. O'Reilly (2010) argues that information produced by and on behalf of the citizens is the lifeblood of the economy; the government has a responsibility to treat that information as a national asset. Therefore, the informational economy of government 2.0 becomes a biopolitical concern to be managed in the production of the population.

Greene's (1998) perspective on rhetorical materialism maintains that rhetorical practices function as a technology of deliberation by distributing discourses, institutions, and populations into a field of action. A critic can map a governing institution's discursive effectivity in terms of its contribution to governmentality. In other words, "a materialist rhetoric marks how governing institutions represent, mobilize and regulate a population in order to judge their way of life (Greene, 1998, p. 27). In this light, rhetoric becomes a technique of government no longer attaching its materiality to the politics of representation but instead directs its focus on the articulation of concepts linked through affect or ideology. Additionally, rhetorical materialism does not engage in a hermeneutics of suspicion that seeks to uncover the hidden expression of a more

primordial reality; instead, it examines how rhetorical practices exist as a human technology that serves in the governing of bodies by making visible populations in need of welfare. From this perspective, the rhetorical scholar explores how rhetorical fragments are attached to a structure of signification for the purpose of governing a population.

The articulation of disparate individualized elements into a population is part of Foucault's theory of biopolitics and governmentality. According to Foucault (2000), governmentality is the articulation of "institutions, procedures, analysis and reflections, the calculations and tactics that allow the exercise of this very specific albeit complex form of power which has as its target population, as its principal form of knowledge political economy, and as its essential technical means apparatuses of security" (p.219-220). The constitution of disparate individual elements into a population works through the exclusion of some form of other: criminals, external enemies, and others (Foucault, 1998). In the case of this project, governmentality works to constitute a population through the exclusion of radical dispositions, Islamic extremism, and terrorism. Under a traditional understanding of the infusion of anatamo/biopolitics, the state attempts to preserve a state of homeostasis through efforts to control internal enemies with the rule of law while utilizing the army to deal with the external enemies. Yet, neoliberalism and the war on terror may have dissolved these traditional boundaries; thus, the state has developed new techniques to preserve a state of homeostasis. We are now witnessing situations where it seems difficult to delineate between internal and external enemies and, as such, legal and military responses are also adapting. While Presidents Bush and

Obama claim that they employ surveillance against non-citizens, Snowden's disclosures expose how surveillance has become a global phenomenon that bypasses simple delineations of national sovereignty. Instead, the public is learning more about the global nature of digital communication and how it is used both inside and outside of the territorial U.S. to locate the ideological dispositions of terrorists both domestic and foreign.

Rhetorical materialism provides a method for rhetorical scholars to examine how the political rationality of the war on terror is linked to the political technology of the production of individual subjects articulated into a population. The population is then monitored and regulated in order to create a state of equilibrium or homeostasis. The biopolitical rationality of homeostatic control rhetoric is embodied by institutions and strategies; these ideas that are naturalized so much so that they become taken for granted (Foucault, 1998). This project uses rhetorical materialism to map the ways in which governmentality and institutional embodiment of political rationality has been transformed into a system of algorithmic regulation that operates to capitalize on the immaterial labor of citizens through the biopolitical and economic rationalities of government 2.0 rhetoric. To perform this analysis, I tend to the rhetorical circulation and fluidity of everyday affect, practices, and uncertainties (Chaput, 2010). More specifically, this study follows the constitution of algorithmic citizenship as it circulates in the production of an open and transparent subjectivity in algorithmic, corporate, governmental, and social media discourses. This allows for a mapping of how the new algorithmic citizen is produced, made public, and produces value.

To trace the articulation of the algorithmic citizen, I explore what Chaput (2010) describes as the, "truth-effects of a multifaceted discursive structure through a neoliberal focus on affects and connectivities" (p. 6). Rhetoric is located through an indeterminate sociality, "the coming-together or belonging-together of the processually unique and divergent forms of life" (Chaput, 2010 p. 19). Similarly, Greene (1998), drawing from Foucault, contends that the materiality of rhetoric functions as a "technology of deliberation" that informs governmental judgments to remake reality. For instance, algorithmic regulation and government 2.0 likely require active consumer citizens who are open and transparent with their data. In this scenario, rhetoric operates as a technique and technology to cultivate the digital algorithmic subject who can communicate through various means of social media (e.g., Facebook, Gmail, Google Hangout, Twitter, and Skype); smartphones (e.g., GPS, phone calls, and text messaging); monitored algorithmic consumerism (e.g., Amazon and eBay); and participatory consumerism (e.g., providing feedback and reviews for Air BnB, Lyft, and Uber). In all of these examples, rhetoric works as a technology of production capable of manipulating relations. By applying articulation theory alongside with rhetorical materialism, this study aims to map how the algorithmic citizenship is imposed with national security as a strategy to conduct the war on terror.

While I read for a rhetoric of transparency as a cultural technology, it remains important to examine governmental discourse to understand the form of material rhetoric that I am tracing. Governmental rhetoric is significant to the material history of rhetoric because it highlights the relationship between technologies and institutional histories

(Greene, 2009). For instance, there have been many scholars who theorize how rhetoric operates through specific media such as Facebook; however, intellectuals should also analyze the whole cultural terrain associated with institutions in general and how it contributes to particular modes of subjectivity. This project explores the ways that institutions attempt to persuade through the circulation of "technologies of public persuasion" or the ways institutional forms produce and reproduce their technologies.

With this understanding of the role of governmentality, I examine the rhetoric of algorithmic citizenship and government 2.0 to understand how it operates by calling for government to be treated as a platform that manages the population through the collection and regulation of big data and users' communications. O'Reilly (2010) contends that government is at its core merely a mechanism for collective action. For example, people come together into social groups and organize bodies through the creation of laws. Additionally, the organization of bodies is funded through taxation polices and the building of institutions which are relegated to manage the problems that are too large to be handled individually but which are deemed to be in the best interest of the population as a whole. Thus, government 2.0 is likely unique in that it works to harness technology, specifically collaborative technologies, in order to best monitor, manage, and regulate collective problems at every level of government (O'Reilly, 2010).

Bringing together these understandings of rhetorical materialism and governmentality, at a broad level, this study explores the ways in which institutions attempt to frame problems and the policies implemented to solve them becomes technique of rhetorical materialism (Greene, 2009). In order to do this, I examine the

educational, media, military, and state assemblages that work to deal with the problems associated with terrorism and citizenship. To map the rhetorical circulation of algorithmic citizenship and government 2.0, this study follows the corporate discourse, public campaigns, and policy implementation of IBM programs such as Blue Crush and THINK. In addition, this project maps how government 2.0 and algorithmic citizenship is constituted through presidential discourse and policy implementation by following the speeches of Presidents George W. Bush and Barack Obama. Finally, the study follows how publics produce value through participating in the war on terror through crowdsourcing and the contribution to transparency and openness in the act of whistleblowing.

Texts are selected for analysis by operating as an exercise in critical algorithmic analysis. As such, the entire study is interacting with algorithms that defined the parameters of my research and study into a personalized project from the moment I first typed in "rhetoric, surveillance, and war" into a web search engine. While the personalized research allows for me to receive numerous news articles or book recommendations based on pre-selected search terms, for numerous reasons I cannot bring in all the information collected. Therefore, this study, much like the data collection by both government and corporations, must be collected and sorted in order to identify the works that are most useful. As such, each of my case studies is a product of exploring and following an algorithmic trail. For instance, I began with analyzing IBM's museum exhibit and, in doing so, that it led me to predictive policing, which led me to Blue Crush. Following this trail and searching within IBM's website and Google search results, I

produced algorithms that I am going to study. This also holds true to the selection of books I ordered on Amazon and the presidential speeches I located; they were located based on search terms and algorithms that connect together these terms.

Chapter previews

In order to follow the rhetorical circulation of algorithmic citizenship, the ensuing chapters explore the ways that citizenship, consumerism, surveillance, and war are articulated together. Chapter 2 follows President George W. Bush administration's rhetoric of counter-terrorism, national security, and surveillance from 9/11 through the end of his presidency. The purpose of following Bush's rhetoric is to map how he utilized presidential definition as a rhetorical technique to define an enemy and persuade citizens to accept strict security measures and government surveillance. Specifically, Chapter 2 tracks Bush's speeches directly after 9/11 when he defined the war on terror, outlined the counter-terrorism policy, and framed the role of citizens in relation to this new type of war. Then, the chapter takes up the relationship between defining a terrorist enemy and citizen by following three case studies. The first case is the "Lackawanna 6" and the first U.S. drone strike that killed an American citizen. Second, the chapter follows John Walker Lindh and the official government discourse surrounding his capture and arrest. Third, the chapter explores the classification of enemy combatants and the implications it has on citizenship. Last, the study follows the rhetoric surrounding Bush's surveillance legislation, in particular, the passage of the USA Patriot Act of 2001 and the implementation of the Terrorist Surveillance Program. These

programs provide both the legal justification and the policy protocols for mass government surveillance.

Chapter 3 examines the production of the algorithmic communicative subject to see how the rhetoric of openness and transparency likely circulates and aids in the production of active citizens who shares its data. In particular, this chapter analyzes economic discourse and campaigns to see how algorithmic citizenship and government 2.0 is articulated, implemented, and marketed. Using IBM as a case study, this chapter begins by analyzing the economic logic that manifests in the corporate response of transparency in relation to government data collection. Next, the chapter examines how algorithmic citizenship may be constituted through the THINK exhibit and campaign. This campaign attempts to reduce citizenship to a network of data-subjects that produce value through their signifying potential. A critical examination of IBM's THINK campaign can expose how corporations attempt to capture and appropriate citizens' immaterial labor that is then implemented into policies of predictive policing and matters of national security. To explore these concepts, Chapter 3 analyzes IBM's Social Intelligence Fusion Toolkit program, Blue CRUSH campaign, and the Human Terrain System Project. These IBM programs are directly linked to the THINK exhibit in that they promote advanced data analytics for predictive security purposes. The Social Intelligence Fusion Toolkit allows for intelligence and law enforcement to monitor citizens social media such as Twitter. Blue CRUSH was implemented in Memphis and relies upon the collection of big data to determine and predict sites and bodies that are linked with criminality. The Human Terrain System Projects provide resources to the

military to create predictive cultural maps in Afghanistan and Iraq in order to give forces real-time information and aid the process of targeted killings.

Chapter 4 analyzes President Obama's rhetoric of transparency and open data. This chapter begins by exploring the way that Obama ran his political campaign utilizing advanced statistical research and championing the slogans of transparency and open data. Next, the chapter follows Obama's speeches and policies while he was in office to provide insight into how the campaigning concepts materialized into policy. In analyzing Obama's speeches, this chapter explores how citizenship, surveillance, and war are articulated through the Department of Justice White Papers that outline the legal precedent for killing an American citizen who is a high ranking al Qaeda official located on foreign soil with drone strikes. Later, Chapter 4 moves to Obama's May 23, 2013 and his January 17, 2014 speeches on drones and surveillance. These speeches are selected because they indicate a shift in the war on terror from an external threat into more of a domestic problem, possibly justifying mass surveillance in the name of national security. Finally, this chapter concludes with Obama's White House Summit on Radical Ideology, which was a high level meeting to "highlight efforts to stop extremists from radicalizing, recruiting, or inspiring individuals" (Tau, 2015, para. 2).

Chapter 5 addresses the initial questions that guide my inquiry. The chapter provides conclusions regarding how algorithmic citizenship is interpolated and enacted by citizens. Drawing from the previous chapters, Chapter 5 brings together a theory of algorithmic citizenship and government 2.0 and how these concepts are articulated and transcoded into a logic of national security. While the previous chapters explore the way

that algorithmic citizenship is constituted through the discourse of economic and policy-making elites, Chapter 5 argues that the interactive nature of government 2.0 provides citizens with new modes to enact political agency. Drawing from examples ranging from Jean-Francois Lyotard, the sousveillance movement, Wiki-Leaks, and surveillance whistleblowers, Chapter five demonstrates various ways that algorithmic citizens are able to collaborate, engage in open debate, and constitute themselves as political agents that play an interactive part in the governing process. The chapter then discusses the limitations of this project and suggests ideas for future research. While this dissertation sketches out an idea of algorithmic citizenship and how rhetorical tropes of transparency and openness are essential for governmentality, there is much work to be done regarding how citizens enact their own agency.

CHAPTER 2: BUSH 2.0?

On January 29, 2002, President Bush, in the annual State of the Union Address, succinctly outlined his strategy for conducting the war on terror. A major component of his strategy was to persuade the public to accept the cultural shift regarding the responsibility of national security away from the government and onto citizens. Bush explains:

> For too long our culture has said, "If it feels good, do it." Now America is embracing a new ethic and a new creed: "Let's roll." In the sacrifice of soldiers, the fierce brotherhood of firefighters, and the bravery and generosity of ordinary citizens, we have glimpsed what a new culture of responsibility could look like. (WH, OPS, 2002, January 29, para. 51)

In soliciting citizens to adopt the new culture of responsibility, Bush begins the rhetorical constitution of algorithmic citizenship. The culture of responsibility requires that citizens become more than mere consumers living their daily lives while the government fights a global war on terror on their behalf. According to Bush, because the U.S. is exceptional, it is the nation's responsibility to confront global enemies such as the "axis of evil" that produces geopolitical chaos and danger. Yet, citizens are responsible for assenting to war by volunteering their services and helping carry out the war in their daily activities. The president outsources the responsibility of the war onto citizen-soldiers who are hailed to serve their country in the fight against terrorism and evil in all of their manifestations.

One of the many things that makes this speech particularly interesting in reformulating the discourse of modern warfare is that Bush began his constitution of algorithmic citizenship by first redefining the global disposition of various nations. This begins with Bush declaring that terrorists view the entire world as a battlefield and thus

the American response will require the U.S. to scour the globe (WH, OPS, 2002, January 29). Even though most of the visible military action occurred in Afghanistan, the U.S. was taking action and gathering intelligence all over the world. This invisible action occurs by training other countries' armed forces to participate in the fight against terror. It also occurred by imposing more military presence in countries that the U.S. has not declared war against. For instance, Bush provided the example of naval patrols off the coast of Africa to prevent terrorist activity in Somalia (WH, OPS, 2002, January 29). Moreover, if a country was unwilling to join the U.S. in its demand to take action to eliminate terrorism, Bush vowed that America would act on their behalf.

Bush distinguished between timid countries unwilling to act and hostile nation-states that he articulated as being terrorist allies. Specifically, Iraq, Iran, and North Korea were defined as hostile nations, which as Bush stated, "constitute an axis of evil, arming to threaten the peace of the world" (WH, OPS, 2002, January 29, para. 21). These countries were articulated as being especially evil because they all possessed or were attempting to possess weapons of mass destruction. By positing that these countries were capable of having weapons of mass destruction and allied with terrorist organizations, Bush aimed to persuade the public that it is America's responsibility to subject these countries to strict surveillance, sanctions, and, as was the case with Iraq, in need of regime change through war or other means.

In addition to refining the world outside the U.S., Bush's State of the Union Address also reconstituted the citizen's duties. Even though the U.S. was acting globally against both terrorist organizations and their alleged nation-state allies and sponsors,

Bush maintained that security was only possible when citizens were vigilant at home (WH, OPS, 2002, January 29). Citizen's awareness required a dual process of submitting to intense surveillance and actively monitoring activity around them. Bush explained this process when claiming that, "we will improve intelligence collection and sharing, expand patrols at our borders, strengthen the security of air travel, and use technology to track the arrivals and departures of visitors to the United States" (WH, OPS, 2002, January 29, para. 31). Citizens were encouraged to submit to this surveillance based on the traditional biopolitical defense of improving public health. For instance, increased border control and police surveillance were defended on the basis that it will help put a stop to illegal drugs and make neighborhoods safer. Furthermore, Bush articulated the culture of responsibility with national security, asking citizens to keep their eyes and ears open, commit themselves to service such as the USA Freedom Corps, whose purpose will be homeland security, and when confronted with acts of terrorism to take action like the passengers did in response to the Umar Farouk Abdulmutallab's attempt to detonate a bomb located in his underwear (WH, OPS, 2002, January 29). The 2002 State of the Union address provides valuable insight into how President Bush uses the war on terror as a rhetorical strategy designed to persuade citizens to accept security measures such as intense surveillance while simultaneously directing their energy to directly participate in the war efforts through everyday activity.

Exploring similar rhetorical acts found in this State of the Union, this chapter widens the frame to tracks how citizenship and governance have intensified since September 11, 2001 into modes that are consistent with the logic of 2.0. Examining

Bush's presidential rhetoric is quite fitting given how W. in many is a 2.0 president. There is the easy and obvious connection that George W. Bush is the son of President George H.W. Bush; where even the name is a more efficient version that eliminates an entire name. However, if one is to draw a distinction between 1.0 and 2.0 in regards to how the latter builds on and intensifies the former, then it is not difficult to connect Bush 43's rhetoric on citizenship, surveillance, and war operates as a 2.0 version of his father. There is Gulf War I and Gulf War II. Bush 41 had the War on Drugs that increases police power and mass surveillance. Bush 43 continues the War on Drugs, and then upgrades to 2.0 version, the War on Terror, which streamlines and bolsters War on Drugs military and police collaboration, information gathering, and targeted killings, and intensified the original Gulf War by removing Saddam Hussain.

Given Bush 43's proclivity for expanding domestic surveillance and war, this chapter analyzes his presidential speeches to highlight how citizenship is transformed into a 2.0 version of algorithmic citizenship. More broadly, this chapter explores how the logic of government 2.0 and algorithmic citizenship becomes ingrained as essential characteristics in conducting the war on terror. The remainder of the chapter is categorized into three sections. The first section provides a theoretical context to understand the rhetorical strategies used in presidential address during the war on terror. The second section analyzes how Bush used public address to define the war on terror, interpellate citizens to participate in an ideological battle, and implement policies of mass surveillance. The third section examines how Bush implemented mass surveillance as an essential tool for identifying potential terrorists, predicting future attacks, and taking pre-

emptive action to prevent them. Next, the chapter addresses how information becomes a vital national resource by analyzing Bush's surveillance programs and information gathering policies. Finally, the chapter explores how citizenship is constituted through performances of transparency that allow the government to identify normal citizens from those who were infected by the contagion of terrorism.

The rhetorical effects and functions of presidential address

Interpellating citizenship. The process of interpellating citizens, shaping public memory, and utilizing presidential definition operate as a series of interrelated rhetorical strategies that demarcates national identity and the political possibilities which can be pursued. Vanessa Beasley (2001) contends that presidential address articulates abstract ideological commitments into the social identity of the public. In other words, presidential speeches play a fundamental role in the interpellative process involved in constructing and managing citizenship. The president is able to circumscribe the social identity of citizens and position the audience to identify with an offered subject position. While the interpellative process is not always successful, the attacks on 9/11 provided a unique opportunity for citizens became more likely to accept the ideological calling of the president, as the affect generated by the attacks could be routed into support for presidential policies. In this rhetorical situation, President Bush responded with public address that sought to shape public memory and citizens' role by defining the enemy and the threat. The same rhetorical force that defined an enemy as an external threat also operates to define the ideological investments of good citizenship. For instance, Americans were able to unify as a nation that was at war against the threat of Islamic

fundamentalism and terrorism. Framing the war on terror as an ideological battle against competing ideological values, Bush is able to redefine American values, encourage citizens to adopt them, and then identify those who do not adhere to those values as a threat to national security.

Public memory and nostalgia. The ability to shape public memory is another public address technique that is used liberally by politicians, especially the president. Shawn and Trevor Perry-Giles (2000) explain that collective memory has material consequences as it ideologically constitutes the way that citizens interacts with one another and institutions and their public involvements. By drawing on historical narratives, the president defines the collective identity of the nation based on an interpretation of a shared past. Furthermore, presidents call forth and interpret public memory, expressing history through narratives inviting the public to identify and embody particular subject positions. The ability to articulate specific modes of subjectivity as well as a collective national subjectivity provides President Bush with powerful rhetorical tools to wage the war on terror.

According to President Bush, part of being the chief decision-maker is the ability to engage in a form of reactive security that includes worst case scenario planning and a readiness to respond if and when this scenario occurs (WH, OPS, 2006, January 23). While the president's job requires constantly attention on national security, Bush argued that the public's focus should be directed towards maintain normalcy (WH, OPS, 2006, January 23). To achieve this goal after the attacks, Bush asked the public to get on with their lives. In other words, the public could return to their normal consumer lifestyles, fly

on planes, take trips to tourist destinations, return to work at a major financial center, or take in a sporting event with a large crowd. In utilizing the rhetorical technique of framing public memory, Bush was able to direct citizens focus towards consuming and normalcy while framing the role of the president as the ever-vigilant protector that should collecting information to best protect the population. This is what Jeremy Engles and William Sass (2013) label as acquiescence rhetoric; the call for acceptance of presidential war decisions due to the differential in both expertise and focus.

Integral to Bush's call for a return to a state of normalcy was the rhetorical strategy of political nostalgia. Parry-Gilles (2000) contend that political nostalgia magnifies appeals based in a selective recollection of the past because of the emotional resonance it creates between political leaders and audiences and the identification it creates with an idealized yet partisan view of the past. For example, after 9/11, citizens were asked to overlook the disparate problems in their daily lives and to unite together as a nation resolved to undefeated by terrorism. However, the calls to return to daily life glossed over the particular material struggles and differences faced by individuals in the wake of the tragedy in order to appeal to unify with a mythologized version of the past that never existed. Moreover, this articulated collective memory seeped in political nostalgia demanded that citizens sacrifice many of their civil liberties in order to preserve a way of life that never really existed.

Presidential definition. The last function or technique of presidential public address that I examine in this chapter is the use of definition. President Bush's attempts to shape public memory highlights the fluidity of social reality. In a postmodern sense,

social reality is fluid, pliable, and full of potential. It is not a given, natural, or pre-determined state of affairs. Instead, it is chosen from a multiplicity of possibilities. Zarefsky (2004) contends that political actors contribute to the production of social reality and that people actively participate in shaping and giving meaning to the world around them. The primary way that people constitute their social reality is through naming the world around them. By naming a situation, people shape the context for understanding social reality and determine the parameters for engagement. Therefore, the ability to define and name is rhetorically very powerful. Defining is the power to identify, name, and bring forth or allow something new to emerge into a field of signification. In addition to allowing new meanings and signs to be constituted and emerge, definitions also frame how something should be understood. It dictates what something is, what value it has, and the meaning that it signifies.

Zarefsky (2004) argues that the office of the president has a sustainable ability to define political reality. The president has unique access and authority to communicate with a wide range of audiences. For instance, the president can address the nation through an electronic broadcast, communicate with the press and shape the context in which the public encounter specific events, and speak directly with policy-makers in Congress. By choosing to define political situations in specific ways with these audiences, the president is able to frame reality as if it were natural and uncontestable rather than selected and open to critique or discussion. Furthermore, through framing, the president can dictate what constitutes credible and worthy arguments, data, and proof (Zarefsky, 2004). Take for example, the evidence offered by the Bush administration to

prove that Iraq had weapons of mass destruction. The Administration provided satellite images of what it considered to be proof that Iraq possessed WMDs. However, the satellite data could only be analyzed and understood by technical experts. Consequently, Bush was able to define Iraq as a threat to U.S. national security by controlling what counted as sufficient evidence. This control of what constituted data prevented the public from challenging the presidential definition of WMD threat because it was incapable of analyzing the evidence that was being presented to them and contesting was it was ample proof. Therefore, the way that the American public understood the situation in Iraq was framed in terms of threat construction that foreclosed or discredited any discussion about whether or not Iraq posed an actual threat to national security.

Additionally, by defining Iraq as a terrorist and WMD threat, Bush was able to control the discussion about appropriate courses of actions in response to the risk. If Iraq has WMDs, then the U.S. was justified in taking pre-emptive action to eliminate WMD use. Furthermore, presidential definition invited moral judgments that concluded that Saddam Hussain and his regime was evil and oppressive and warranted elimination. This was done in two parts: first, Iraq was included in the "Axis of Evil" that was defined as the primary enemy facing the U.S.; second, Hussain's regime was bad enough to justify one war against it and now there are claims of WMD possession. Such an evil and oppression regime necessarily had to be invaded through the definitional logic of the Bush administration.

Zarefsky (2004) also contends that presidents use definitional arguments by creating associations between various terms. For example, Bush's decision to classify the

9/11 terrorist attacks as an act of war. Zarefsky (2004) notes that the terrorist attacks did not necessarily meet the characteristics of war because the attacks were not carried out by a military, did not involve at least another nation-state, and there was no declaration of war by either side. Yet, in defining the attacks as an act of war, Bush was able to justify that a swift military response was necessary that was to be conducted under the wars power of the president rather than as a crime that warranted a public trial and deliberation about the best response to the attack (Zarefksy, 2004).

Interestingly, even though this reality is offered to the public as an accurate reflection of reality, presidential definitions are flexible enough to allow for strategic shifts in definition. For instance, once more information came out that called into question the Administration's evidence that defined Iraq as a WMD threat, President Bush's discourse shifted the threat frame away from WMD possession to the liberation of oppressed people, particularly women, and the spread of democracy (Zarefsky, 2004). This ability to shift frames shows the fluid power of presidential definition. On one hand, presidential definition naturalizes social reality as an uncontestable given, yet, on the other, it is also malleable enough to shift when necessary.

Now that I have reviewed the broad rhetorical effects, functions, and techniques of presidential public address, I now use this understanding of presidential address to analyze how President Bush specifically frames the war on terror. The first section examines how Bush used arguments of definition about the war on terror. Mapping the ways Bush defined the war provides insight into the ideology and logic that rationalized mass surveillance and preemptive warfare. The second section maps Bush's rhetoric of

enemyship and how it was articulated in relation to citizenship. In order to find the enemy and bring them to justice, Bush first had to identify what constituted a terrorist. To determine this, Bush relied on presidential definition to classify good citizens from enemies. This system of classification transformed typical understandings of citizenship and initiated the president's ability to classify bodies to be detained or eliminated. The third section follows how Bush rhetorically framed his justifications for domestic surveillance and intelligence gathering as consistent with American values. The ability to classify surveillance programs as top secret while publicly claiming that they are legal, restrained, and true to American values allowed the president to control public discourse regarding classification of enemies and threat construction. This then displaced constitutional protections of citizenship and justified a secret program of domestic spying.

Defining the war on terror

Enemies and terrain. On the evening of 9/11/2001, President Bush addressed the nation about the attacks from the Oval Office. While Bush did not announce who was behind the attacks, he did use his speech to declare that the attacks were an act of terrorism and that the U.S. would launch a successful war on terrorism (WH, OPS, 2001, September 11). With the simply expression "war on terror", the choice to define the events of 9/11 as an act of war became the framework from which the American people would conceptualize what occurred and how America would respond. Throughout the remainder of his presidency, Bush framed the attacks and America's response as a global war on terror being waged through a Manichean battle of "good" versus "evil,"

"civilized" versus "barbarians," and "us" versus "them." This framing operates through a biopolitical and realist logic of protecting the American people from an external threat. On the evening of 9/11, Bush began to ontologically structure the war on terror as an ideological conflict between those who defended freedom and those who threaten freedom. While the specific identify of the enemy was unknown, Bush defined the enemy as terror. While this becomes operationalized to mean global terrorist networks, it is important to note how the frame defines a psychological state as the enemy rather than a class of traditional enemies; this explains how the war on terror can be expanded even when enemies are defeated or early justifications are no longer valid.

Once a vague enemy has been identified, Bush next deploys the classic American exceptionalist metaphor, which alluded to Jesus's Sermon on the Mount, of America as "God's country" and the "shining city upon the hill." According to Bush, "America was targeted for attack because we're the brightest beacon for freedom and opportunity in the world. And no one will keep that light from shining" (WH, OPS, 2001, September 11, para. 4). That shining beacon could then be used to identify and apprehend the enemy that was lurking in the shadows. Bush argued that the U.S. and its allies would rise up to win the war against terrorism and in doing so "will make no distinction between the terrorists who committed these acts and those who harbor them" (WH, OPS, 2001, September 11, para. 9). In this war on terror, there are no innocent bystanders, as Bush dramatically frames the war through biblical and exceptionalist allusions to clearly demarcate groups and nations as absolute evil or good. As Bush states, the choice is

absolute: "Either you are with us, or you are with the terrorists" (WH, OPS, 2001 September 20, para. 31).

Four days later, on September 15, the Bush administration began to use a colonialist "clash of civilizations" frame the war on terror as a war between the civilized world and its barbaric other. First posited by Harvard political scientist Samuel Huntington (1993), the Clash of Civilizations hypothesis maintains that cultural and religious differences between cultures will generate conflict and war in the post-Cold war era. For the Bush administration, this thesis operates as a perfect theory for the new realignment of global power in the rise of global terrorism. For example, Secretary of State Colin Powell announced that the attacks on 9/11 were not just against the United States, but against all Western civilization (WH, OPS, 2001, September 15, Pres urges readiness and patience). President Bush reaffirmed this statement, explaining that Americans were a kind people who could not imagine the barbaric acts of the uncivilized terrorists who hide in holes and caves. Then Bush explained that the America would win a war against "barbaric behavior, people that hate freedom and what we stand for" (WH, OPS, 2001, September 15, Pres urges readiness and patience, para. 23). However, Bush later stated that this is not just America's fight; "This is the world's fight. This is civilization's fight" (WH, OPS, 2001 September 20, para. 35).

By defining the war on terror through the tropes of a global struggle between good civilizations and evil barbarism, Bush was able to implement a military strategy that was equally as totalizing. In a speech for prayer and remembrance, Bush explained the role America has in conducting this war stating: "Just three days removed from these

events, Americans do not yet have the distance of history. But our responsibility to history is already clear: to answer these attacks and rid the world of evil" (WH, OPS, 2001, September 14, para. 7). The problem with this framing of the world in the wake of the 9/11 attacks, according to noted intellectual Edward Said, is that it is grounded in Islamophobia and oversimplifies important differences and similarities between different cultures, which results in extreme violent responses.

Yet, despite its flaws, the Administration continued to use this rhetorical lens to understand the world and to establish a military response. For instance, on September 15, President Bush introduced the American public to a new type of war: "This is a conflict without battlefields or beachheads, a conflict with opponents who believe they are invisible" (WH, OPS, 2001, September 15, Radio Address, para. 2). In this speech, Bush was preparing the public for what has turned out to be a very long war. The American people were asked to be patient, maintain their resolve, and be strong because "victory against terrorism will not take place in a single battle, but in a series of decisive actions against terrorist organizations and those who harbor and support them" (WH, OPS, 2001, September 15, Radio Address, para. 2). On September 20, Bush further clarified, stating:

> Americans should not expect one battle, but a lengthy campaign, unlike any other we have ever seen. It may include dramatic strikes, visible on TV, and covert operations, secret even in success. We will starve terrorists of funding, turn them one against another, drive them from place to place, until there is no refuge or no rest. And we will pursue nations that provide aid or safe haven to terrorism. Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists. (WH, OPS, 2001, September 20, para. 30)

The public had to be patient and unwavering in their support for the war on terror because it was unclear exactly who the enemies of freedom were, let alone how the government

could effectively engage such an enemy other than massive military invasion. Yet, later in the day on September 15, Bush provided an answer to how the government was going to deal with an enemy that was illusive and operated through a veil of invisibility; he drew on an old western allusion and gusto, stating, "we will smoke them out of their holes" (WH, OPS, 2001, September 15, Pres urges readiness, para. 3).

In order to "smoke out" the enemy, the Bush administration had to wage a war of information. In the name of protecting the American people and their way of life, the President began implement policies of collaboration between intelligence agencies, law enforcement, and warfighting organizations to find the terrorists and bring them to justice. The American people were informed that "our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated" (WH, OPS, 2001 September 20, para. 23). Even though the war on terror was to be conducted as a global response to eradicate the evil in the world, Bush still discussed the war through the traditional imperialist Clash of Civilization trope of the "civilized inside" fighting against the "barbarous outside."

While the terrorists operated in a postmodern fashion of communicating through flexible networks, molecularization, and fluidly transgressing borders, the threat was never thought of as being internal. For instance, during a national radio address, Bush claimed: "We are now waging a global war on terror -- from the mountains of Afghanistan to the border regions of Pakistan, to the Horn of Africa, to the islands of the Philippines, to the plains of Iraq. We will stay on the offense, fighting the terrorists abroad so we do not have to face them at home" (WH, OPS, 2005, July 9, para. 6). Then,

a few months later, President Bush echoed this viewpoint, stating: "Our troops know that they're fighting in Iraq, Afghanistan, and elsewhere to protect their fellow Americans from a savage enemy. They know that if we do not confront these evil men abroad, we will have to face them one day in our own cities and streets, and they know that the safety and security of every American is at stake in this war, and they know we will prevail" (WH, OPS, 2005, August 20, para. 4).

In order to prevail, President Bush wanted to collect as much information on the enemy as possible. In his State of the Union speech on September 20, 2001, the President explained his strategy for conducting the war on terror, stating: "We will direct every resource at our command—every means of diplomacy, every tool of intelligence, every necessary weapon of war—to the disruption and to the defeat of the global terror network" (WH, OPS, 2001 September 20, para. 28). By December, the Bush administration realized how it could direct all the resources at its command: through the use of mass surveillance, preemptive strikes, and a revolutionary military technology.

When strategizing about how to win the war on terror, the Bush administration often used rhetoric that framed the entire world as a global battlefield. For example, Vice President Dick Cheney stated, "The terrorist enemies are hidden and dispersed, and they view the entire world as a battlefield. They are determined to commit indiscriminate murder against innocent, unsuspecting men, women, and children" (WH, OPS, 2007, January 21, para. 10). Waging a global war required the United States to go on the offensive, preemptively striking enemies abroad in order to prevent fighting the war on a domestic front. In framing a global battlefield, the Bush administration posited its

enemies as being so dangerous that they were ubiquitous. Thus, in order to protect the American people from this insidious threat, the government would have to be able to gather information against an enemy on a global scale and in real time. In particular, President Bush went to great lengths to emphasize that although the threat is global, it was brought about by an external enemy who has the ability to infiltrate national borders. Therefore, to best prevent another attack, the United States needed the legal tools to surveil globally. This allowed the government to collect information on terrorist suspects, statistically predict where future attacks are most likely to occur, and take effective measures to prevent an attack from ever taking place.

The framing of the global network of terror constituted the entire world as a battlefield that the government must monitor to identify and follow the movements of a dispersed and fluid enemy. For instance, President Bush used this definition of the battlefield to justify the importance of Predator drones, stating, "When all of our military can continuously locate and track moving targets — with surveillance from air and space — warfare will be truly revolutionized" (WH, OPS, 2001, December 11, para. 28). To actualize this revolution in military strategy, Bush began to implement numerous surveillance programs designed to monitor and strike enemy targets all across the world. This revolution in military intelligence required innovation in public values. Bush explained this paradigm shift in surveillance, going so far as to explain that before the attacks, government surveillance was, "held in suspicion, and even contempt. Now, when we face this new war, we know how much we need them" (WH, OPS, 2001, December 11, para. 49).

Definition of the president's role. A major component of Bush's rhetorical strategy for promoting and rationalizing the war on terror was the use of Presidential definition. This chapter traces how President Bush utilized presidential definition to determine both the role of the President in regards to the war on terror as well as that of the public. In this regard, the following sections outline the broad rhetorical techniques deployed by Bush. In order to map the broad techniques, the sections examine how Bush frames the role of the presidency, the role of the public, and the role the law plays in authorizing, conducting, and legitimating mass surveillance and the war on terror. After outlining the broad techniques, the chapter explores the specifics of Bush's public address to highlight the role that rhetoric played in the implementation of the public policies of surveillance and war-fighting.

While speaking at Kansas State University in 2006, President Bush highlighted the role of presidency as being responsible for managing the social relations and values of citizens. Bush admits that part of the job of the president is to be well-informed and to listen to numerous perspectives; however, when it comes to waging the war on terror, he stated, "I'm the decider" (WH, OPS, 2006, January 23). Bush further elaborated:

> If I had to give you a job description, it would be a decision-maker. I make a lot of decisions. I make some that you see that obviously affect people's lives, not only here, but around the world. I make a lot of small ones you never see, but have got consequence. Decision-maker is the job description. (WH, OPS, 2006, January 23, para. 11)

According to President Bush, the responsibility of the president is to make decisions. While many of the choices are about the policies that the nation should implement, numerous other decisions are made regarding issues such as how to manage social

relations. For instance, after 9/11, President Bush had to choose a rhetorical strategy to unite the people. He did this by constituting the American people as a unified exceptionalist subject that adheres to a specific set of cultural values and beliefs. To accomplish this task, Bush relies heavily on the rhetorical techniques of framing public memory and defining social reality.

The war on terror and the Iraq War that followed were politically rationalized on the basis that the President has access to more information than the public and as such it is his job to make decisions for the public. For instance, February 2003 was a time of unprecedented global anti-war protests on the eve of an impending invasion of Iraq. On February 18th, after swearing in the new chairman of the Securities and Exchange Commission, Bush fielded questions from the media. Reporters seized the opportunity to inquire about how the global protests affected Bush's thoughts on the upcoming war with Iraq. Bush provided two responses. First, Bush cited the protests as examples of democracy in action. Because the world was able to voice its disapproval, it was a sign that democracy was valuable and worked (Gonyea & Bush, 2003). Thus, the dissent against the Iraq War was celebrated as a victory for American values and good democratic citizenship. Second, Bush argued that the protests exposed the ignorance of the public because it did not understand that Saddam Hussain was a threat to global peace (Gonyea & Bush, 2003). In other words, Bush did not have to listen to the millions of people voicing their dissent because they were ill-informed and thus could not properly represent the interests of the American people. Perhaps more surprisingly, President Bush was dismissive of the size of global dissent. The opinions of the substantial number

of protesters—close to 30 million people—were belittled by the President when he noted that deciding policy based on the wishes of popular opinion would be similar to making decisions based on "focus group[s]" (Gonyea & Bush, 2003). Rather than act in response to this public outcry, Bush maintained that his job was to take on the role of the sovereign and protect the American population from their own misguided desires.

Definition of the public's role. According to President Bush, when it came to the war on terror, the public's framing of its collective memory should remember the tragedy of the attack and mourn for what was lost, but then to quickly move on with life in a customary way. In order to invite citizens to return to their regular daily lives, Bush had to circulate a narrative of normalcy and connect it to the publics' memory. To accomplish this task, Bush suggested that the public to travel, take vacations to Disneyland, or return to work. Instead of focusing on life's difficulties, President Bush reminded the public of how great life is in America and how the good life is made possible by hardworking citizens carrying out their daily activities. As was evidenced by his "Axis of Evil" speech, Bush set up the narrative that national heroes are everyday Americans who work hard and take responsibility for one another. Therefore, by identifying with Bush's interpellation of an ordinal yet heroic subjectivity, the public could accept the rhetorical hailing of the President.

Legality as a definition of appropriateness. In the name of national security, the President implemented numerous surveillance policies and directing intelligence agencies to gather information for the war on terror. Congress also provided the President with a two notable pieces of legislation: The Authorized Use of Military Force

(AUMF); and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act). Although these laws were passed by Congress, they provided the President with the legal tools necessary to implement a mass surveillance program conducted by intelligence agencies such as the NSA. The implementation of the AUMF and the 2001 USA Patriot Act provide President Bush with a rhetoric of legality, with which he invites the public to accept enhanced interrogation techniques, government secrecy, and surveillance because they were made legally permissible by representatives acting on behalf of the people. By explaining his intelligence and surveillance policies as legal, Bush can rhetorically posit the war on terror as being constitutional and important in the ideological conflict to promote American values.

The President's uses of the rhetoric of legality to rationalize surveillance as a vital tool in the ontological positioning of algorithmic citizenship. Citizens are to submit to mass surveillance and to engage in performances of transparency because information is vital to winning the war on terror. President Bush highlighted this at a press conference where he explained that the Terrorist Surveillance Program and the 2001 USA Patriot Act are valuable tools in helping intelligence gaps that occurred prior to September 11(WH, OPS, 2005, December 17). These surveillance programs privilege data as a national asset, using it to biopolitically map and monitor the population. By collecting as much data as possible, communication patterns can be calculated statistically and used to algorithmically sort the population based upon the threat that a communication profile posed. In the name of preserving American values such as freedom and democracy, the

government implemented an asymmetrical surveillance program that inverted its common principles. In order to win the war on terror, the American public was rendered transparent and participate in the algorithmic regulation and data mining. Meanwhile, the government, which casts itself as open and transparent, was secretive in the name of preserving national security.

Definitions as justifications for the AUMF and PATRIOT Act. On September 18, 2001, President Bush signed the Authorization for Use of Military Force (WH, OPS, Pres signs AUMF). This legislation was signed to help bolster national security. The President claimed that he needed increased war powers to better defend the civilized American people at home and abroad from the uncivilized terrorists (WH, OPS, 2001, September 18). Using biopolitical protection of the American people as its justification, the AUMF codified into law:

> That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons. (AUMF, 2001, p. 1)

The extremely broad phrase "all necessary and appropriate force" has been liberally applied to justify the President conducting warrantless surveillance in the name of counter-terrorism. As the Department of Justice explains:

> Of vital importance to the use of force against the enemy is locating the enemy and identifying its plans of attack. And of vital importance to identifying the enemy and detecting possible future plots was the authority to intercept communications to or from the United States of persons with links to al Qaeda or related terrorist organizations. Given that the agents who carried out the initial attacks resided in the United States and had successfully blended into American society and disguised their identities

> and intentions until they were ready to strike, the necessity of using the most effective intelligence gathering tools against such an enemy, including electronic surveillance, was patent. Indeed, Congress recognized that the enemy in this conflict poses an "unusual and extraordinary threat." (p.12)

The fact that the terrorists who carried out the 9/11 attacks were able to blend into American society and disguise their identities and intentions explains why everybody must be regarded in suspicion. If a terrorist is capable of going unnoticed, then the government must surveil everyone in order to detect and identify the imposter.

The AUMF has been used by the President as well as the Department of Justice for legally intercepting communications of citizens by the NSA (DOJ, 2006, Jan 19). Bush publicly acknowledging that he was using the AUMF, and his constitutional authority vested in him as Commander-in-Chief to authorize the NSA to intercept communications of people linked to al Qaeda and related terrorist organizations (WH, OPS, 2005, December 17). The DOJ argued that the AUMF authorizes the president to secretly conduct surveillance against the enemy in order to protect the nation (DOJ, 2006, Jan 19). Moreover, as long as the president is conducting foreign intelligence, then she/he does not need a warrant to conduct electronic or wireless surveillance. The DOJ (2006, Jan 19) goes as far to state, "the history of the President's use of warrantless surveillance during armed conflicts demonstrates that the NSA surveillance described by the President is a fundamental incident of the use of military force that is necessarily included in the AUMF" (p.10).

On October 26, 2001, President Bush signed into law the USA Patriot Act. This Act provided Bush with additional tools to authorize intelligence agencies' mass

surveillance of American citizens. This was accompanied by the Department of Justice's webpage dedicated to explaining the USA Patriot Act, which described the counter-terrorism strategy as advancing the principles of collaboration, collecting, and sharing of information, and personalized surveillance and targeting, in order to predict, prevent, and punish all those who were implicated in terrorism (DOJ, n.d.). As Bush claimed several years later, "the Patriot Act tore down the legal and bureaucratic wall that kept law enforcement and intelligence authorities from sharing vital information about terrorist threats. And the Patriot Act allowed federal investigators to pursue terrorists with tools they already used against other criminals" (WH, OPS, 2005, December 17, para. 2). The application of surveillance tools used to detain drug dealers and domestic criminals becomes a common theme used when justifying the USA Patriot Act. While the statement seemingly makes sense, a closer examination about the historical connections between the war on terror and the war on drugs reveals that Bush was attempting to justify the use of domestic surveillance for the war on terror.

Bush 41 used the Drug Enforcement Agency (DEA) to justify a massive surveillance dragnet of citizen's phone records to map associations of the drug cartels and dealers (Heath, 2015). Robert Mueller, the chief criminal prosecutor for the Attorney General at that time, gave the DEA permission to collect large sets of phone metadata for intelligence operations (Heath, 2015). In 2001, Mueller was the Director of the FBI and was very important in the establishment of the President's surveillance program. Indeed, Mueller was so important that President Bush 43 thanked him personally in a speech delivered to the FBI in 2003. This praise of Mueller makes sense given that he legally

oversaw a surveillance program that became a template used by the NSA when it launched its massive phone surveillance programs for the war on terror.

The DOJ justified increased mass surveillance as merely extending investigative tools that were already available in the investigations of organized crime or drug trafficking (DOJ, n.d.). The USA Patriot Act extended the ability to conduct electronic surveillance to "terrorism-related crimes, including: chemical-weapons offenses, the use of weapons of mass destruction, killing Americans abroad, and terrorism financing" (DOJ, n.d., What is the Pat Act). This broadening of surveillance resulted in legalizing "roving wiretaps", which target a particular suspect rather than a particular device. Thus, rather than having a warrant to tap a particular phone, the government granted the ability to track any device that is reasonably believed to be associated with a terrorist suspect. This tactic ran the risk capturing information of innocent people or exacerbating stereotypes. For instance, once a terrorist suspect goes to a specific bank, mosque, or store, all of those places can be subjected to strict surveillance. The result is that numerous other people become caught in this surveillance dragnet because they were associated by being in the same area or having the same religion. The USA Patriot Act also extended the ability to delay notification to a subject when a judicially-approved search warrant has been executed (DOJ, ND). This is rationalized as allowing law enforcement to conduct investigations without tipping off terrorists; an excuse frequently used by George Bush when refusing to provide any information to the public so as to prevent the enemy from finding out.

The mantra of national security and the legal permissibility of the Patriot Act further gave federal agencies the authority to collect consumer records from private businesses. The DOJ explained this need, in arguing, "investigators might seek select records from hardware stores or chemical plants, for example, to find out who bought materials to make a bomb, or bank records to see who's sending money to terrorists" (DOJ, What is the Pat Act?, para. 9). In order to preserve national security, the federal government can collect people's credit records to see what they bought, where they bought it, and then use this information to construct terrorist profiles and statistical predictions of future attacks. These legal justifications rely on the claim of national security to institutionalize the principles of algorithmic citizenship by promoting a transparent citizenry and emphasizing the importance of collaboration and the need for information sharing. President Bush explained this shift in stating:

> As of today, we're changing the laws governing information-sharing. And as importantly, we're changing the culture of our various agencies that fight terrorism. Countering and investigating terrorist activity is the number one priority for both law enforcement and intelligence agencies. (WH, OPS, 2001, October 26, para. 13)

The move to information sharing is also a transition towards algorithmic citizenship and is articulated through the rhetorical phrase of "connecting the dots." For example, the President highlighted the previous failure when the government could not make the connection between terrorists abroad and within the country on 9/11, when two of the hijackers communicated to known members of al Qaeda that were overseas (WH, OPS, 2005, December 19). Furthermore, the Department of Justice (n.d.) described the Patriot Act as cooperation among agencies and facilitating information sharing so they can better

"connect the dots." Bush also stated that the USA Patriot Act was essential for connecting the dots that were missed in regards to 9/11 (WH, OPS, 2005, December 19). Additionally, White House Press Secretary Scott McClellan defended the NSA terrorist surveillance program as necessary to connect the dots and "stay a step ahead of a deadly enemy that is determined to strike America again" (WH, OPS, 2006, January 22, para. 1). Therefore, President Bush invited citizens to accept the secret surveillance because it is a policy that could have theoretically identified the 9/11 attackers and prevented the attack. As a corrective, he authorized the NSA to monitor American citizens' communications in search for links between terrorists.

Threat construction and surveillance. Shortly after 9/11, the President authorized the NSA to conduct a classified surveillance program to detect and prevent further attacks against the United States (Fine et al, 2009). This program was later named the Presidential Surveillance Program (PSP) and it authorized numerous classified surveillance polices. Despite the secretive nature of government surveillance programs, the public learned about some of the surveillance programs implemented by President Bush. For instance, the President publicly acknowledged the existence of the Terrorist Surveillance Program. After several other parts of the surveillance program were leaked to the media, an unclassified report documenting the historical operation of the PSP was released. According to the information made publicly available, the PSP was largely designed by the NSA, which disseminated intelligence reports to other agencies such as the CIA, FBI, National Counterterrorism Center (NCTC), and the Office of the Director of National Intelligence (ODNI) for analysis and investigation (Fine et al, 2009). The

CIA would use the information to prepare threat assessment memoranda that were used to support the periodic Presidential Authorizations that occurred every 45 days.

The use of threat assessment memos demonstrates the rhetorical strategies that the government used to implement mass surveillance. First, surveillance relies on the creation of fantastic futuristic scenarios of death and destruction. In order to prevent these scenarios, the government must collect as much information as possible to determine where an attack is most likely to occur and take pre-emptive action so that the threat never materializes. For national security purposes, the surveillance programs are classified and implemented in secret. If someone finds out about the surveillance program, or if someone involved dissents, then they are to be blamed and deemed personally culpable for the loss of life because they were complacent in not doing everything possible in preventing a future attack.

For example, in 2005, ODNI assumed responsibility for preparing the threat assessment memos. The content of the memos contained such terrifying scenarios that the ODNI personnel referred to them as "scary memos" (Fine et al, 2009). The writers of the threat assessments were aware that their findings would determine the likelihood for extending the PSP. Assessments that predicted scenarios of terrorism and mass destruction became persuasive tools that were used to gain reauthorization. For instance, Deputy Attorney General James Comey questioned the legality of the PSP and was considering not supporting re-authorization of the program. Comey was then invited to a meeting where Dick Cheney stressed how the PSP was of "critical importance" (Fine, et

al, 2009). Cheney also claimed that, if the program was not recertified, Comey would be personally responsible for thousands of people's lives (Fine et al., 2009).

The PSP authorized the NSA to spy on citizens in and outside of the United States for evidence of terrorist activity without a court-approved warrant (Risen & Lichtblau, 2005). The PSP's surveillance intensified once the CIA began to capture top al Qaeda members such as Abu Zubaydah, the man President Bush uses as a poster child for the success of enhanced interrogation techniques. However, the CIA apprehended more than just people associated with 9/11; they also took possession of terrorists' cell phones, computers, and personal phone directories. The NSA began to monitor all calls, e-mails, and electronic communications that came from the confiscated devices. Then the NSA mapped the connections that were associated with terrorist communications. Those subjects linked with suspected terrorists became suspects themselves and were also put under surveillance (Risen & Lichtblau, 2005). This allowed for the government to collect a chain of information regarding what people were linked to terrorism. The Department of Justice (2006, January 19) touted surveillance as an indispensable aspect of national security because it provides an early warning system that monitored the communications coming in and out of the United States of persons reasonably believed to be linked to al Qaeda.

Given the increasing amount of information being collected on suspected terrorists, the government desired to have an efficient way to collect, sort, and store information so that it could be used to most effectively prevent future attacks. In the 2003 State of the Union, President Bush announced that the leaders of intelligence

agencies such as the CIA, FBI, Homeland Security, and Department of Defense developed a Terrorist Threat Integration Center (TTIC), to "merge and analyze all threat information in a single location" (WH, OPS, 2003, January 28, para. 49). By establishing a comprehensive picture of terrorist activity from a single database, information could no longer be divided into the traditional binary of domestic and foreign. The TTIC institutionalized that all information relating to terrorism, "from raw reports to finished analytic assessments," be shared amongst all levels of government (WH, OPS, 2003, February 14). To make this possible the government created a central location that stores all information and institutionalized a Joint Task Force that required federal, state, and local law enforcement to share information in order to best identify and apprehend terrorists. This shift to information sharing was legally rationalized through the adoption of the USA Patriot Act which transformed the bureaucratic process of information gathering with the ethos of collaboration (WH, OPS, 2003, February 14). Again, the President implemented algorithmic governance by mandating that government agencies share information so that law enforcement can respond in real-time to apprehend suspected terrorists. In an attempt to foster collaboration, President Bush argued that the war on terror's success depended on intelligence and law enforcement agencies' abilities to cooperate (WH, OPS, 2003, February 14).

The President further dissolves the bureaucratic boundaries between intelligence agencies and military operations by linking Saddam Hussain with terrorism and weapons of mass destruction. With the looming war with Iraq, President Bush emphasized this linkage in the State of the Union by stating:

> Before September the 11th, many in the world believed that Saddam Hussein could be contained. But chemical agents, lethal viruses and shadowy terrorist networks are not easily contained. Imagine those 19 hijackers with other weapons and other plans -- this time armed by Saddam Hussein. It would take one vial, one canister, one crate slipped into this country to bring a day of horror like none we have ever known. We will do everything in our power to make sure that that day never comes. (WH, OPS, 2003, January 28, para. 77)

By positing Hussain as a WMD terrorist, President Bush was able to justify the need for global surveillance that works to establish and preventative use of force. This form of threat construction is a powerful rhetorical strategy because it plays on fears of weapons of mass destruction use. By invoking an unimaginable horror, the President asked the public to support both the government surveillance that identifies the threat and then the response of force that preemptively strikes against the threat before it can materialize.

Bush's articulation of Hussain as a WMD threat also provided an indication of way that algorithmic governance would work to regulate the population. For example, President Bush was able to define the leader of a sovereign country as an evil terrorist who must be stopped before he unleashes potential nuclear annihilation. The reliance on presidential definition through threat construction works to produce a political culture where citizens' affect and anxiety is routed in ways to make it that they will submit to the systems of surveillance that are intended to biopolitically regulate society. For instance, in his February 14, 2003 speech to the FBI in support of the establishment of the TTIC, the President informed the American people that the government had authorized intelligence agencies to work together to engage in mass surveillance. In addition, he articulated together the public's fear and the need for military action and mass surveillance. As President Bush remarked:

> The American people need to know that we're collecting a lot of information and we're going to share it in a way that enables us to do our jobs that you expect us to do. That we're going to use the best information technologies available to not only make sure information flows freely at the federal level, but flows from this databank of information to local law enforcement officials. It will enable us to make sure that we do everything we can to win the war on terror at home, just like we're going to do everything we can by unleashing one of the greatest militaries -- the greatest military ever assembled abroad. We've got fabulous men and women in uniform who are on the hunt. The finest, bravest, soldiers ever known to mankind are helping us track them down one by one. (WH, OPS, 2003, February 14, para. 22-23)

By articulating the upcoming war with public anxiety about WMD global terrorism, the President was able to justify mass surveillance in the name of protecting the American people from "cold-blooded killers" that were constantly plotting horrific attacks (WH, OPS, 2003, February 14)

By framing surveillance as being vital to the war in Iraq and the larger war on terror, President Bush was able to implement a central database for the purpose of data-mining in order to diagnose terrorist dispositions and pathologize populations. In establishing the TTIC, the President institutionalized an "up-to-date database of known and suspected terrorists accessible to appropriate officials at all levels of government" (WH, OPS, 2003, February 14, para. 19). This allowed for the institutionalization of so-called capture/kill lists, which lists names the government uses to gather information so as to determine which people need to be detained or exterminated as enemy combatants and militants. The TTIC was directed by John Brennan, who later becomes the Director of the CIA and is credited for developing Obama's disposition matrix. Brennan referred to TTIC as a "revolutionary concept," stating that the program:

> represents a new way of optimizing the U.S. Government's knowledge and formidable capabilities in the fight against terrorism...that allows us to gain a comprehensive understanding of terrorist threats to U.S. interests at home and abroad and, most importantly, to provide this information and related analysis to those responsible for detecting, disrupting, deterring, and defending against terrorist attacks. (FBI, 2004, April 30, para. 6)

Although the Bush administration implemented the capture/kill lists, the preferred option was to capture because more information can be gained from the living than from the dead.

On September 17, 2001, President Bush was asked directly if he wanted Osama Bin Laden dead. He responded: "I want justice. There's an old poster out west, as I recall, that said, 'Wanted: Dead or Alive'" (WH, OPS, 2001, September 17, para. 31). While Bush refused to extrapolate on the statement, saying that he was only remembering a poster from when he was a kid, history would later expose the serious nature of that response. Six days after the 9/11 attacks, he signed off on a secret memorandum authorizing the CIA to establish secret terrorist detention facilities (de Vogue, 2008). These prisons, also referred to as "black sites," were established outside of the United States territory and its laws and were used to detain high value terrorist suspects. The terrorist suspects were subjected to enhanced interrogation techniques such as being kept awake by music blaring at extremely high volumes, stripped and held in an icy room, and suffered waterboarding (Mayer, 2007). The purpose of subjecting high-value terrorists to these interrogation methods was to gain information that could be used to seek revenge on these people and to prevent future attacks.

President Bush publicly justified his policies of secrecy, surveillance, and torture on the fact that the attacks of 9/11 ushered in a new era of warfare. Bush explained in a

speech in 2006, that the attacks on 9/11 made it "instantly clear that we'd entered a new world, and a dangerous new war (WH, OPS, 2006, September 6, para. 2). Bush justifies his enhanced interrogation methods on a nationalist and utilitarian calculus that was premised on the judgment that saving American lives outweighing the discomfort and rights of terrorists who could provide valuable information. Bush went so far as to explain that enhanced interrogation methods "has been and remains, one of our most vital tools in our war against the terrorists" (WH, OPS, 2006, September 6, para. 26). He further justifies his information gathering strategies by stating:

> Captured terrorists have unique knowledge about how terrorist networks operate. They have knowledge of where their operatives are deployed, and knowledge about what plots are underway. This intelligence -- this is intelligence that cannot be found any other place. And our security depends on getting this kind of information. To win the war on terror, we must be able to detain, question, and, when appropriate, prosecute terrorists captured here in America, and on the battlefields around the world. (WH, OPS, 2006, September 6, para. 7)

Thus, the ability to rationalize mass surveillance follows a set rhetorical protocol. First, President Bush defines the enemy as evil and operating globally. Second, this threat is magnified through rhetoric of apocalyptic scenarios describing WMD attacks triggered by small cells of terrorists or an evil nation-state such as Iraq. Third, by labelling the enemy as evil, the President creates the perfect image of a monstrous enemy that is malicious to its core. Fourth, because the enemy is evil and slaughters innocent life, it is possible to rationalize the dehumanization and scapegoating of the enemy and rationalizing acts such as torture and lethal operations against suspected enemies.

However, the power of presidential definition goes far beyond the ability to simply declare the enemy as evil, it also provides the ability to define and identify who

constitutes the good. While President Bush rationalized the war on terror against an absolutely evil enemy, he rationalized his policies further by articulating his counter-terrorism policies as legal and consistent with American values. This definition of the war on terror provided President Bush the ability to route the public's affect in ways to generate public support for the war on terror while actively implementing surveillance policies and warfighting strategies that directly targeted citizens. Moreover, as Gilles Deleuze and Félix Guattari (1984) note in their study of why people passionate fight for their own domination, the public desires their own repression as clichés and other discourses define and order their world. Yet, unlike the phrase Deleuze and Guattari (2009) coined to characterize this theory, "more taxes, less bread," the post 9/11 American public chanted, "more surveillance, less liberty and nothing to hide, nothing to fear" (29).

In order to analyze how the masses came to desire their own repression regarding government surveillance, the next section will take up how the Bush administration hailed citizens to participate in the war on terror. In the name of national security, the President interpellated a series of performances that good citizens should engage in. Those who failed to adhere to the performances were articulated as potential citizen-terrorists. Once a citizen was suspected of being a citizen-terrorist, they could be legally redefined as an enemy who, based on government discretion, may be denied constitutionally-protected privileges.

Citizenship, drones, and presidential classification. In order to legally apprehend, detain, and obtain information through potentially torturous means, President

Bush had to label those detained as unlawful enemy combatants. Unlawful enemy combatant is defined in the Military Commissions Act of 2006 as:

> (i) a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces); or ‘‘(ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense. (p. S. 3930—2)

This law provided the Bush administration with the means to classify citizens as unlawful enemy combatants who could then be detained or eliminated through lethal operations. While these policies were known to exist, the details regarding government classifications of citizens as enemy combatants were kept secret. The reasons, according to former White House Council and later US Attorney General Alberto Gonzales (2004), were that the determination required sensitive intelligence that, if revealed, could jeopardize future capture and prevention of terrorist attacks. Therefore, while the government created legal categories that suspended the rights of citizenship, the details about it were classified as a matter of national security.

The ability to classify people as “enemy combatants” had profound implications for citizenship. Gonzales (2004, February 24), argued that the war on terrorism faced a unique threat where a globalized enemy had the potential to infiltrate neighborhoods. Although the enemy was untraditional, it had engaged in acts of war; those who fight with the enemy are combatants even if they are American citizens. Accordingly, a person who was associated with al Qaeda and labelled an enemy combatant could be denied the

rights and privileges provided by citizenship. Once classified as enemy combatant, suspects can be detained because they are the enemy, not because they are "guilty" of any crime. Gonzales (2004) furthered explained that it is inaccurate to claim that these people were being held without charges, because that suggests that there is a need to even charge suspects with a crime. Instead, enemy combatants can be held without right to avoid self-incrimination or have a public trial. Because they are affiliated with an enemy force during war time, these combatants can be held and subjected to interrogation in order to acquire information. The ability to detain and hold enemy combatants without charges means that the government can gain intelligence while keeping them off the battlefield. For example, President Bush explained the importance of this policy by stating, "we have an obligation to the American people, to detain these enemies and stop them from rejoining the battle" (WH, OPS, 2006, September 6, para. 8). Unlawful enemy combatants are held indefinitely until the government has determined that they do not "pose a continuing threat and no longer have significant intelligence value" (WH, OPS, 2006, September 6, para. 9).

In order to justify enhanced interrogation techniques and infinite detention, President Bush posited unlawful enemy combatants as monsters who have valuable information. He went to great lengths to explain that enemy combats are not common criminals or innocent bystanders; rather, they are evil murders who want to kill all American people. Moreover, the President argued that these detained unlawful enemy combatants held valuable information that could be used to save innocent American lives. Worse yet, according to President Bush, the terrorists had received training on how to

resist the typical U.S. interrogation techniques. Because the enemy had developed a strategy to resist interrogation, the CIA resorted to what the President referred to as "an alternative set of procedures," also known as advanced interrogation techniques (WH, OPS, 2006, September 6). President Bush did not want to disclose the new interrogation methods publicly, claiming that if terrorists knew what they were, they could devise a strategy to resist the techniques (WH, OPS, 2006, September 6). However, it is possible that the secrecy surrounding these interrogation methods was also based on the need to prevent the public from discovering that, to use the words of President Obama, "we tortured some folks" (WH, OPS, 2014, August 1, para. 94).

Before the Supreme Court ruled that the Geneva Convention's Common Article 3, which calls for the humane treatment of combatants and non-combatants, applied to al Qaeda and Taliban members, President Bush issued a memo declaring the inapplicability of the Article to the war on terror. The primary justification for not applying the Convention was that the war on terror is a different type of war. According to the President, the Geneva Convention only applied to citizens and troops of nation-states that were engaged in conflict with one another; it did not apply to the war on terror, which "usher[ed] in a new paradigm" where groups with international reach commit horrific acts against innocent civilians (Bush, 2002). Thus, according to the President, the attacks on 9/11 require the United States to rethink how it conducts warfare. In rethinking its warfighting paradigm, President Bush claimed the legal authority to suspend the Geneva Convention between the United States and Afghanistan, although he could have followed the principles if he had desired. Furthermore, the President argued that the Geneva

Convention does not apply because the people were detained for issues related to terrorism, which classifies them as enemy combatants and, therefore, they do not qualify as prisoners of war (Bush, 2002).

The Supreme Court ruled in the 2004 *Hamdi v.Rumsfeld* Supreme Court decision that the President had the authority to detain American citizens as enemy combatants; however, the decision also ruled that citizens had a right to challenge their detention (Elsea, 2005). Once a citizen is labeled an enemy combatant, the government has several options that its disposal: criminal prosecution, detention as a material witness, or detention as an enemy combatant. This gives the government flexibility on how it chooses to prosecute those it believes are associated with terrorism. If the government is concerned that a criminal trial would either alert al Qaeda or risk national security, the government could instead try the suspect through a military tribunal. This means that the government does not have to publicly reveal the methods and information gained from its intelligence investigation.

The government also can use enemy combatant status as a negotiating tool when dealing with American citizens who are affiliated with al Qaeda. Shortly after the 9/11 attacks, the U.S. military captured John Walker Lindh, an American citizen living in Afghanistan. Lindh maintained that he was in Pakistan and Yemen learning about his Islamic faith when he migrated to Afghanistan to help Taliban forces fight against the Northern Alliance. While in Afghanistan, Lindh was captured by American forces and was held as an enemy combatant. On his capture and arrest, the Bush administration labeled him an "American Taliban" and "al-Qaeda fighter, a terrorist, and a traitor"

(Ashcroft, 2001; Bush, 2001; and Lindh, 2011). President Bush announced on December 21, 2001, that the Administration was going to set a legal precedent for how to deal with American citizens who were suspected of terrorism, going as far to describe the Lindh's case as a unique circumstance because he was the first war on terror-era American citizen-terrorist (Bush, 2001). However, despite being labeled an American terrorist prior to trial, Lindh was always considered a citizen who retained his due process rights. For example, when asked by the media why the government was not going to try Lindh in a military tribunal, Attorney General John Ashcroft replied that tribunals were reserved for non-citizens and thus Lindh would be given his day in court. Rather than risk trial, Lindh agreed to a deal in which he pleaded guilty to a charge of supplying services to the Taliban and carrying an explosive during the commission of a felony for his part in a military prison uprising. In exchange for the plea bargain, the U.S. government agreed to forego its right to treat Lindh as an unlawful enemy combatant. However, if Lindh is ever found to be associating with anyone from al Qaeda or its affiliates, then the agreement is made void and the government can invoke its ability to capture and detain him as an unlawful enemy combatant (Elsea, 2005).

Despite the shifting context of war and terrorism, in which Americans were joining the conflict against the U.S., citizenship was still based on the biopolitical and Realpolitik logic of inclusion/exclusion that assumes that the U.S. at war with an external identifiable enemy. For instance, Ashcroft demonstrated this in his announcement of the charges filed against Lindh, claiming that the U.S. has external enemies and if a citizen decides to join forces with those enemies, then s/he must have been tricked or deceived.

Even President Bush expressed pity for Lindh, calling him, "a poor misguided Marin County hot-tubber," in reference to his progressive or hippie upbringing (BBC, 2002). Therefore, for the Bush Administration, while terrorism was a contamination threat to the U.S., the threat was not an internally produced but rather an external threat that corrupts otherwise good citizens. This was emphasized further by the President in a speech in 2006 where he discussed the threat of homegrown terrorists, by stating:

> More and more, we're facing threats from locally established terrorist cells that are inspired by al Qaeda's ideology and goals, but do not necessarily have direct links to al Qaeda, such as training and funding. Some of these groups are made up of "homegrown" terrorists, militant extremists who were born and educated in Western nations, were indoctrinated by radical Islamists or attracted to their ideology, and joined the violent extremist cause. (WH, OPS, 2006, September 5, para. 29)

In the examples given by President Bush, domestic terrorists are rhetorically framed as normally good Western people that have been brainwashed or seduced by radical Islamic extremism. In many ways, the President and Administration could not conceive of a world where Western people could ever commit acts of terrorism unless they were corrupted in an ideological battle.

While the United States has numerous options for dealing with unlawful enemy combatants captured on U.S. soil, those apprehended outside the U.S. faced far more perilous options. Declaring people unlawful enemy combatants allowed for the government to implement targeted killing policies without having to remove the ban on assassinations. The *New York Times* reported that the "Wanted: Dead or Alive" slogan was much more than rhetorical flourish; it was also national policy. By October 21, 2001, legendary *Washington Post* reporter Bob Woodward noted that the "smoke them

out" rhetoric was supported by a secret directive that authorized the CIA to use lethal force against bin Laden. However, the directive to use legal force was then expanded to allow the CIA to kill high-value members of al Qaeda without having to gain specific approval by either the president or congress (Risen & Johnston, 2002). The secretive nature of targeted killings meant that the American public could only be informed of the covert operations if they were reported after the fact by the media, foreclosing the potential for public deliberation and debate.

While the Bush administration introduced many new types of military technologies and warfighting techniques, one of the primary developments in the war on terror was the use of unmanned aerial drone vehicles. For example, President Bush applauded Predator drones as a "revolution" in military technology, stating:

> Before the war, the Predator had skeptics, because it did not fit the old ways. Now it is clear the military does not have enough unmanned vehicles. We're entering an era in which unmanned vehicles of all kinds will take on greater importance — in space, on land, in the air, and at sea. (WH, OPS, 2001, December 11, para. 25)

Prior to 9/11, the Clinton administration and the CIA had internal debates about whether the government was legally authorized to kill Osama bin Laden (Coll, 2004). President Clinton had authorized the CIA to pursue bin Laden but the orders were ambiguous on the CIA's ability to use lethal force. While in retrospect it is possible to look back and trace the legal precedent to justify the killing of bin Laden to a time between the years 1998-2000, President Clinton primarily directed the CIA to pursue capture rather than killing.

While still favoring capture publicly, President Bush, in contrast to Clinton, was far less ambiguous in his orders to the CIA. According to Jon Yoo (2001), the legal advisor for the President's Surveillance Program, the President authorized targeted killing by drone strikes in a secret order just days after 9/11. The first CIA drone strike to be publicly acknowledged occurred in 2002 and killed six suspected al Qaeda members. One of the people killed in the drone strike was an American citizen, Kamal Derwish, thus establishing a legal precedent for how the government was going to respond to citizens that went overseas to join enemy forces: The United States would use lethal force against external enemies regardless of national affiliation.

Kamal Derwish was known as an al Qaeda recruiter for militant Islamic training camps in Afghanistan. He was famous for the role he played in the recruiting of six American citizens—the Lackawanna 6—from Buffalo, to an al Qaeda training camp in early 2000. Derwish, was killed while traveling in a vehicle carrying an al Qaeda lieutenant who played a key role in the attack on the USS Cole. By November 19, a Yemen news agency had confirmed that one of the passengers in the vehicle was American citizen Kamal Derwish. The American government, originally denied the allegations that it had killed an American citizen. Yet, once the facts could no longer be denied, the Bush administration shifted its stance and claimed that Derwish was not specifically targeted. However, the Administration claimed that his death was justified because he was associated with a high ranking member of al Qaeda. Nevertheless, even if the Bush administration did target Derwish, the Administration believed that it was

legal because the President has the authority to order a strike on Al Qaeda operatives overseas, even if they are American citizens (Purdy & Bergman, 2003).

The power to order a lethal strike against American citizens overseas serves as a stark reminder of the rhetorical force of presidential definition. The lack of a clearly delineated battlefield and clear inside/outside borders that determine who is domestic/friend and foreign/enemy gives further credence to the Administration's need to monitor the population in an attempt to detect potential terrorists. Then once citizens are suspected of consorting with the enemy or becoming radicalized, they can be classified as enemy combatants and as such no longer are afforded the constitutional protections of citizenship. Through this act of definition, the president has the ability to detain enemy combatants without due process, torture them, or potentially, as in the case of Derwish, marked them for death.

The drone strike that killed Derwish also highlights the secretive nature in which the Bush administration approached the war on terror. The next section will follow how President Bush used national security rhetoric to justify secretive surveillance and warfighting policies. The section first takes up how he reconciled the secretive nature of the war on terror with democratic values of transparency. Then it explores how President Bush explained to the public the surveillance policies that were in place. His rationalizations are then contrasted with the information disclosed to the public by Edward Snowden and various news organizations. Finally, the section takes up how the policies of mass surveillance were used to begin the implementation of algorithmic citizenship through the collection and sorting of citizens' communications into a digital

profile determining normal communicative patterns of citizenship from abnormal potentially terrorist modes of communication.

The secretive presidency

The technique of presidential definition, specifically in regards to national security, provides President Bush a way of framing the war on terror that was nearly immune from public criticism or debate. Indeed, a major trump card that the President played was that the office of the president provides a superior epistemological vantage point than that of the public; he had unique access to information that the public did not. Therefore, President Bush argued that he was simply acting in the best interest of national security based on information that was classified from the public. He reinforced the asymmetry of knowledge by articulating government secrecy as being vital to national security. This creates a circular narrative where the government denies the public access to information in order to keep it secure. Rather than a spirited public debate about how the nation should respond to the terrorist attacks or conduct a war on terror, President Bush was able to claim that the public should support the war on terror because the government was better informed and was acting in the public's best interest. This was only enhanced by the President's rhetoric constituting himself as the decider-in-chief.

The implications of President Bush's use of presidential definition here fused together national security with demophobia, flipping the traditional democratic values of transparent government and private citizens; after 9/11, the government was to be private and citizens were to be transparent. For example, shortly after the attacks on 9/11, the President was asked if he would explain what military options were on the table for a

response. Bush respond by stating, “This is an administration that will not talk about how we gather intelligence, how we know what we're going to do, nor what our plans are” (WH, OPS, 2001, September 15, para. 28). Thus, while information was vital for the war on terror as a key resource and weapon to identify the enemy, the public was shielded from the knowledge of how the government was conducting the war on terror and collecting intelligence.

This policy of secrecy intensified when President Bush issued Executive Order 13292 that amended Clinton’s policy for how information could be classified for national security purposes (WH, OPS, 2006, March 25). President Clinton’s executive order created a standard that information could not be classified if there was significant doubt about the need to do so. President Bush removed that standard so that information could be classified even if there was significant doubt about its need (Kosar, 2009). Furthermore, he authorized secrecy by classifying any information given to the United States received in confidence from foreign governments. Beyond increasing the scope of material that could be classified, President Bush also increased the number of people who were able to classify documents. For instance, the Vice President now could classify information while performing executive duties. Additionally, the executive order eased the government’s ability to reclassify previously declassified records and it moved the automatic classification date of records back 25 years or more. It also eliminated the requirement that agencies had to prepare plans for declassifying records. To shroud declassified information even further, the President cancelled the order that created a government-wide database for declassified information and replaced it with a program in

which the Director of the Information Security Oversight Office would coordinate and link declassified documents together (Kosar, 2009). Even if information did overcome all of these obstacles to finally be publicly released, the executive order permitted the Director of the CIA to block declassification attempts unless overruled by the President.

This executive order allowed President Bush to classify information as top secret, meaning that he was able to classify all documents outlining his surveillance program as a national security secret. Meanwhile, he claimed that secrecy was necessary to preserve the open and transparent democratic forms of government brought about by the free flow of information. The Reporters Committee for Freedom of the Press (RCFP) argued that the Bush administration was rolling back open communication under the guise of conducting the war on terror (Daugherty, 2003). Among the list of secrecy policies that concerned the RCFP was the Administration's reinterpretation of the federal Freedom of Information Act that allowed agencies to deny access to public records by claiming that such disclosure would be a breach of national security.

When information did find its way to the media, the Bush administration aggressively pursued whistleblowers for leaking national security-related information. This led to subpoenas issued to reporters and in some cases citations for contempt of court against journalists who would not reveal their sources. Those who leaked information to the public were castigated as being criminals who helped the enemy rather than being viewed as champions of democratic transparency. For example, Defense Secretary Donald Rumsfeld sent out a memo to all members of the DOD in which he warned against the dangers of leaking information to the press (Garamone, 2002). The

memo claimed that leaking information was helping the enemy win the war on terror and costing Americans lives. Within this discourse, information become a matter of life and death and anyone who shared classified information, even if it is in the name of preserving democracy, was framed as culpable for the loss of American life.

Despite the appeals to national security, the media began to report details of the President's Surveillance Program. On December 17, 2005, President Bush acknowledged publicly the existence of the secret mass surveillance program being carried out by the NSA. This knowledge was made public only because the *New York Times* had uncovered information about the program and released the story (See Risen & Lichtblau, 2005). Even after the release of *Times* story and the President's acknowledgment, the public was only privy to knowledge about the Terrorist Surveillance Program, which collects information both coming in and going out of the United States if there is reason to believe that one or more parties is associated with terrorism. The public was told this surveillance was legal because it monitored the communications of non-citizens, who do not have constitutional protection against U.S. surveillance. Yet, the Bush administration never reveals any other surveillance program that do not rely on the same legal justification. The other surveillance program that collected citizens' communications were classified and thus kept outside of the public's knowledge (Fine et al., 2009).

President Bush scathingly criticized the disclosure of classified information stating, "our enemies have learned information they should not have, and the unauthorized disclosure of this effort damages our national security and puts our citizens

at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country" (WH, OPS, 2005, Dec. 17). During his press conference, he was asked if he could point out a single example where his surveillance program had worked. Rather than answering the question, President Bush remarks:

> it's really important for people to understand that the protection of sources and the protections of methods and how we use information to understand the nature of the enemy is secret. And the reason it's secret is because if it's not secret, the enemy knows about it, and if the enemy knows about it, adjusts…revealing sources, methods, and what we use the information for simply says to the enemy: change. (WH, OPS, 2005, December 19, para. 119)

Rather than provide the public with factual reasons to endorse his surveillance program, the President relies on counterfactuals. For example, citizens are encouraged to accept and support secret surveillance programs because, had they been in place, they theoretically could have identified the 9/11 attackers and prevented the attack from ever occurring. President Bush highlighted previous failures when the government could not identify the connection between terrorists abroad communicating with people in the U.S. As support for his claim, the President reiterated that on 9/11, two of the hijackers communicated to known members of al Qaeda that were overseas (WH, OPS, 2005, December 19). Thus, President Bush authorized surveillance over citizens' communications if at least one or more parties were physically located outside of the physical territory of the U.S.

Secrecy also operates as a biopolitical tactic that undermines democracy in order to best protect the public. Transparency and open debate about surveillance policy in congress was considered dangerous because it aided terrorists. For example, President

Bush argued that: “an open debate about law would say to the enemy, here is what we're going to do. And this is an enemy which adjusts” (WH, OPS, 2005, December 19, para. 52). To avoid revealing our counter-terrorism game plan, the President cannot afford to reveal much information about his counter-terrorism policies. As a result, public debate is minimized because the public does not have the information needed for a vigorous debate to occur in the first place. Thus, while citizens are entitled to their own opinions, for their own safety, they should trust the President as Decider-in-Chief and the narratives circulated in presidential speeches and media updates.

The media also inquired as to why President Bush needed secret surveillance programs as opposed to using the legal programs that were currently in existence such as seeking warrants for communication intercepts through Foreign Intelligence Surveillance Act (FISA) courts. His response was that the government does not have the time needed to always go through the FISA courts. However, since 1979, FISA court have only denied five of almost 19,000 surveillance requests. Furthermore, these courts operate in secret, so no information is revealed to the public. Yet, President Bush reiterated time after time to constant media inquiries that this is a different kind of war against a different kind of enemy; the government needs the ability to quickly monitor and track an enemy who constantly changes phone numbers and other modes of communication. According to his reason, to fight this enemy, the government required a different program that the President had the powers to implement (WH, OPS, 2005, December 19).

Moreover, the Administration believed that it needed unfettered flexibility to fight terrorism. As President Bush explains:

> We know that a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives. To save American lives, we must be able to act fast and to detect these conversations so we can prevent new attacks. (WH, OPS, 2005, December 19, para. 8)

The call for flexibility and quick response begin the justifications for the transition towards government 2.0. In order to best protect the population, the government required flexible and instantaneous access to communications in order to identify how terrorists are collaborating, detect a potential attack, and take action to prevent it.

Overall, President Bush's surveillance speech reveals how presidential definitions rhetorically function in relation to surveillance. The President is able to strategically disclose a specific legal surveillance program which is used to reassure the public that the government is not abusing its power. Meanwhile, the public is not informed about many other government surveillance programs that are defined as essential to national security and are classified as top secret. Furthermore, the use of presidential definition in this case articulates and constitutes transparent citizens and a secretive government through demophobic references to national security. Not only are citizens not to be trusted with information regarding how the government is conducting the war on terror, they are algorithmically profiled and watched so that potential radicalized or terrorist suspects can be identified and apprehended.

Metadata, communication patterns, and whistleblowers

Although President Bush declared that the government was interested in capturing foreign communications, he identified an ideological threat that requires the government to surveil domestically in search of enemies that infiltrate national borders. To monitor

domestic information, the *USA Today* on May 11, 2006 reported that the NSA was collecting the metadata of American citizens, not just the communications coming in and going out of the country as President Bush had stated. Relying on Section 215 of the Patriot Act, the NSA had been collecting the phone records of AT&T, BellSouth, and Verizon consumers—the three largest telecommunications companies in the country, providing service to more than 200 million customers. The companies were reported to have been contacted soon after 9/11 by the NSA. The NSA relied upon a biopolitical pitch to persuade telecommunications companies to comply: "National security is at risk, and we need your help to protect the country from attacks" (Cauley, 2006, para. 31). In order to protect the country from attacks, the NSA needed telecommunications companies to turn over their "call-detail records," a complete listing of the call histories of their millions of customers (Cauley, 2006). Telecommunications companies were asked to provide updates so that the NSA would be able to keep better track of the nation's calling habits. The result was that the NSA was able to collect citizens' metadata and analyze information in a way that flagged potential threatening communication patterns.

Data and information from citizens were being collected to analyze and determine normal communication patterns from abnormal communications associated with terrorists. The collection of metadata is part of a data-mining program that works to determine the communications profiles of normal citizens and those suspected of terrorism. By collecting metadata, the government is able to determine the network of associations and communication patterns of citizens (Greenwald, 2013). That is, the

government is able to identify who people are talking to, how they are spending their money, what their personal proclivities are. As Timothy Lee (2013) writes, "the idea is that NSA researchers can build a profile of 'typical' terrorist activity and then use calling records- and other data such as financial transactions and travel records- to look for individuals or groups of people who fit the pattern" (para. 13). The algorithmic profiling of consumer information and personal communications work to materially identify good normal citizens and abnormal radicalized or terrorist ideologies.

The government justifies collecting metadata of citizens based on the fact that it is not as invasive as collecting the actual content of communications. Yet, the collection of metadata can have chilling effects on free speech. For instance, if the government is able to look at journalists' phone records, it can determine who reporters have been talking to and uncover sources. Furthermore, the metadata can then be used to collect information in order to conduct politically blackmail. Such monitoring is likely to deter whistleblowers from talking to the media — for fear of losing their jobs or worse. That makes it harder for the public to learn about government misconduct, making such abuse likelier in the future (Lee, 2014).

The importance of having whistleblowers became even more pronounced once revelations came out that the government was collecting far more than just metadata. For example, NSA programs such as Trailblazer, PRISM, UPSTREAM and many more allow the government to access American's emails, phone records, text messages, video chats and other forms of communications. On May 18, 2006, the *Baltimore Sun* reported that the government had shelved a program that allowed the state to monitor online

communications in a legal manner (Gorman, 2006). The rejected program, ThinThread, would have used more sophisticated sorting methods to identify suspects, recognize and encrypt U.S. phone numbers and communication data to ensure privacy, employed an automated auditing system to monitor the analysts handling of the information so as to prevent abuse or misuse, and analyze the data to identify relationships between callers. Only when evidence of a potential threat was found would the decryption of the records be allowed (Gorman, 2006). Instead of opting for this program, NSA director Hayden pushed for a $1.2 billion program known as Trailblazer, a competitor to ThinThread. The NSA did not want to switch programs because they did not want the Trailblazer program to be "outperformed" or "humiliated" (Gorman, 2006). The program the government used worked the same as ThinThread but it had stripped out all of the encryption protocols allowing the government to directly collect citizen's communications (Gilmore & Wiser, 2014). This was all made possible after President Bush transitioned the NSA from monitoring exclusively foreign communications to monitoring all data.

Prior to 9/11. the NSA to monitor domestic communications so as not to violate American citizens' civil liberties (Gorman, 2006). This was validated publicly by Edward Snowden. In an interview. Snowden described the transition of NSA surveillance post 9/11:

> NSA and intelligence community in general is focused on getting intelligence wherever it can by any means possible. It believes, on the grounds of sort of a self-certification, that they serve the national interest. Originally we saw that focus very narrowly tailored as foreign intelligence gathered overseas. Now increasingly we see that it's happening domestically and to do that they, the NSA specifically, targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyses them and it measures them

> and it stores them for periods of time simply because that's the easiest, most efficient, and most valuable way to achieve these ends. So while they may be intending to target someone associated with a foreign government or someone they suspect of terrorism, they're collecting your communications to do so. Any analyst at any time can target anyone, any selector, anywhere. Where those communications will be picked up depends on the range of the sensor networks and the authorities that analyst is empowered with. Not all analysts have the ability to target everything. But I sitting at my desk certainly had the authorities to wiretap anyone from you or your accountant to a Federal judge to even the President if I had a personal e-mail. (Rodriquez, 2013, para. 9)

To prove the accuracy of his statements regarding NSA surveillance, Snowden provided journalists with classified documents that verified the existence of a mass surveillance program conducted by the NSA. These programs all had various code names but demonstrated that the government was doing far more than collecting metadata or spying on non-citizens.

Surveillance outsourcing

President Bush was able to strategically use the power of presidential definition to rhetorically frame government surveillance as both legal and minimally invasive in regards to citizens' daily lives. The President strategically discloses certain surveillance programs that follow the letter of the law. For instance, he argued that government surveillance was only occurring if one party was presumed to exist outside the U.S. This framed surveillance as legal while obfuscating the fact that the government was finding alternative ways to circumvent the law. While Presidents Bush and Obama both contend that American citizens do not have to worry about government surveillance because they are only monitoring foreign communication, what was not mentioned was the numerous

other surveillance programs or the outsourcing of surveillance work to other countries with laxer laws.

Geo-location, programs such as MUSCULAR and PRISM, and tracking cookies have all also been linked to the British intelligence agency, Government Communications Headquarters (GCHQ). The Snowden leaks revealed that from 2011 to 2013, the US government paid at least £100 million to GCHQ. It is possible that this is because GCHQ is not constrained by laws against domestic spying. GCHQ bragged that it has supplied "unique contributions" to the NSA when it was investigating an American citizen for an attempted car bombing in Times Square in 2010 (Hopkins & Borger, 2013). Additionally, the British government disclosed that GCHQ does not need a warrant to tap into bulk communications data collected by the NSA (Volz, 2014). While both British officials and the NSA deny that they use data sharing to circumvent the law, they did rely on the rhetorical justification that law abiding citizens have "nothing to fear" when it comes to government surveillance (Bloomfield, 2013). However, it becomes more difficult not to worry about such developments when the GCHQ lawyers boast in legal briefs about how Britain has a "light oversight regime compared with the US" (Bloomfield, 2013, para. 4).

In order to demonstrate the ways that presidents use definition to frame their surveillance as legal, the following sub-section follows some of the secret NSA surveillance programs that were made public through the Snowden leaks. Describing the secret surveillance programs provides a materialist map of the way that consumer behavior and digital communications are surveilled through numerous modes that are

used to articulate algorithmic citizens. Moreover, this materialist map marks how government surveillance is used to govern the population through the president's ability to define the situation and to classify and control information. Finally, mapping the disparate surveillance programs in relation to one another shows the numerous ways in which algorithmic monitoring operates. In articulating together surveillance programs that are seemingly different provides a map into the collaborative process that goes into the constructing of digital profiles that are connected to physical bodies. As a crucial element of the constitution of algorithmic citizenship, the linking of bodies to data allows the government to determine normal communication patterns from abnormal or suspected terrorist communications.

PRISM. One of the most publicized secret NSA programs was PRISM. The code name seems quite apt given that the etymology of the word "prism" is associated with surveillance and transparency. For instance, prism comes from the Greek words *prisma*, meaning something sawed and *prizein* meaning to saw (Oxford Dictionaries, 2016). Furthermore, *Merriam-Webster Online Dictionary* (2016) defines prism as "a transparent body that is bounded in part by two nonparallel plane faces and is used to refract or disperse a beam of light." *Oxford Dictionaries* (2016) explains that the term prism can be, as it states, "used figuratively with reference to the clarification or distortion afforded by a particular viewpoint." In other words, a prism is articulated alongside transparent bodies and is figuratively used to reference how things are concealed and revealed through a particular perspective. The PRISM program certainly operates according to this logic: citizens' communications are collected through

performances of transparency and analyzed to determine if suspicious terrorist activity is revealed.

As discussed in Chapter 1, PRISM allowed the government to collect information directly from corporations such as Facebook, Google, Microsoft, Skype, and Yahoo. The program was launched after President Bush's secret surveillance program lacked a credible source to provide it legal authority. This was important because communications companies lacked guaranteed protections that if they released consumer information to the government that they would not be legally liable for violating consumers' privacy. Thus, at the end of the Bush administration's second term, congress passed the Protect America Act of 2007 and the FISA Amendments Act of 2008, providing legal amnesty for private companies that cooperated voluntarily with U.S intelligence agencies (Gellman and Poitras, 2013). In exchange for immunity from privacy violation lawsuits, companies such as Google accepted a directive from the attorney general and director of national intelligence to open their servers to the FBI's Data Intercept Technology Unit, which served as a liaison between the NSA and the private companies (Gellman and Poitras, 2013).

PRISM was different from the President's Surveillance Program in that it operated under section 702 of the FISA Amendments Act, authorizing the NSA to conduct warrantless surveillance of communications by foreign nationals believed to not be on U.S. soil (MacAskill, 2013, Aug 23). However, the Snowden revelations exposed that 702 operations collected large quantities of data because it gathers excess data from individuals associated with a suspect and the NSA cannot filter out purely domestic

communications that are caught in the electronic sweep (MacAskill, 2013, Aug 23). Unlike the warrantless mass sweeps so prevalent during the Bush administration, PRISM only allows for the NSA to collect data from corporations so long as they meet a system of qualifications. For instance, analysts key in "selectors" or search terms that are designed by the NSA and the private companies are presented a court order to turn over any information that falls within those parameters. To collect this information, the NSA must have 51 percent confidence in a target's "foreignness"' (Gellman and Poitras, 2013). This provides the government with the ability to frame its surveillance program as targeting only suspicious communications that is most likely occurring outside of the U.S. While U.S. citizens are not the direct target of surveillance per se, much like the President's Surveillance program, American citizens' electronic content can be collected if it is in some way connected to someone suspected of terrorism. This allows the government to collect information on citizens if they are connected by two hops or were friends of a friend who was suspected of terrorism.

The ability to gather citizens' data associated with suspected terrorists supports a rhetorical strategy to persuade people that they are not at risk of having the government collect their personal data. Yet, in an electronic world so heavily interconnected, there is little guarantee of this privacy. For example, Stanley Milgram first formulated the small world theory contending that any two people in the U.S. are connected by no more than six degrees of separation. Building on Milgram's theory, the Yahoo Corporation funded a study testing the small world theory and found that Facebook users were separated by only four degrees of separation (Backstrom et al., 2012). While it is far beyond the scope

of this project to support or defend Milgram's small world theory, the implications of this work provide insight into the rhetorical framing behind the government's claims about only targeting suspected terrorists or their associates. If, as the proponents of government 2.0 claim, social media provides more avenues to connect people together, then the likelihood that ordinary citizens are associated with someone who is suspected of terrorism is also going to increase. Despite the government's argument that citizens do not have to fear NSA data collection, the mathematical probability would indicate that it is likely that many innocent people's data is getting captured in PRISM sweeps.

Of course, companies such as Facebook and Google have all released statements claiming that they do not and never did participate in secret government surveillance programs. Yet, the NSA slides released by Snowden offer other alternatives regarding how the government gains access to corporate data. Because NSA surveillance is classified, it is impossible to determine how much access the NSA has to private companies' servers. However, the NSA slides do reveal that there are numerous surveillance programs that operate together to collect data. It is possible that technology companies were providing legally-requested data for the PRISM. If this is the case then the government might have used another program called Upstream to collect data at key geographic points existing outside the territorial borders of the U.S. (Lee, 2013, June 12).

Upstream and MUSCULAR. According to NSA slides, Upstream collects communications from fiber cables and infrastructure at key data flows junctures (Ball, 2013). For example, a NSA slide noted that much of the world's communications flow through the United States. This is because multinational corporations such as Google

have data centers all around the world and information can flow from center to center. The NSA slides explain that a target's email, phone call, or texts will take the cheapest path rather than the most direct physical path (*Washington Post*, 2013, June 6). The ramifications of this program are that entirely domestic communications by American citizens can theoretically move outside of the country and thus could be legally captured (*Washington Post*, 2013, June 6). Thus, an email between two American citizens can still move outside of territorial borders if Google, for instance, moves the exchange between its center in London and San Francisco. Because the information is flowing into or outside of the country, the government can claim legal authority to collect the data as it moves outside U.S. borders (Washington Post, 2013, June 6).

While the NSA slides encouraged the government to use the PRISM program to directly access private companies' servers and databases and Upstream to collect data at key points as it moves across national boundaries, new information was revealed that highlighted that the government directly hacked into the communications links of Google and Yahoo data centers. The program was named MUSCULAR and it worked by intercepting and then copying entire data flows across fiber-optic cables that carry information from corporate data centers (Gellman & Soltani, 2013, October 30). MUSCULAR allowed the government to find key foreign locations where Google or Yahoo's data was not encrypted and to copy both content and metadata in order to mine for potentially suspicious communication.

SSO program. In addition to these other programs, the NSA's Special Source Operations branch also had a secret program that reportedly intercepted email address

books and "buddy lists" from instant messaging services from communication that moved across global data links (Gellman & Soltani, 2013, October 14). Because part of the war on terror is to seek out and find all terrorists, this unnamed surveillance program allowed the government to map the affiliations and connections of suspected terrorists. According to the NSA PowerPoint presentation, the NSA can collect over 250 million addresses a year, with a typical day resulting in "44,743 e-mail address books from Yahoo, 105, 068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers" (Gellman & Soltani, 2013, October 14, para. 4).

The NSA also piggybacked on the commercial tracking that private companies use to identify and target consumers for personalized advertisements (Soltani, Peterson, & Gellman, 2013). Specifically, the NSA relied on the Google "PREF" cookie that places a tracking file used to uniquely identify a person's browser. While this cookie is typically reserved for companies to track consumers' browsing habits in order to provide specific advertising, the NSA used it to single out specific communications and send out software to hack into that person's electronic device (Soltani, Peterson, & Gellmar, 2013). This practice is used to identify specific targets who are already suspected of terrorism rather than a sifting technique that attempts to detect abnormal communication. However, for the purposes of this study, this type of program demonstrates the interconnected nature of commercial and governmental surveillance techniques and the potential for abuse that these operations might allow.

The NSA also uses commercially-gathered data to track the location of individuals. In order to access this information, the government simply used the same

commercial technology that companies such as Google use to track consumers' location and movements (Soltani, Peterson, & Gellmar, 2013). Many apps for both the iPhone and Android collect geo-location data to sell to a third-party advertiser, market location-specific advertising, or provide location-based services. By capturing this data, the NSA was able to identify the precise physical location of a mobile device in use.

While the corporations such as Facebook, Google, and Yahoo have all vehemently denied their compliance with these programs, *The Guardian* published NSA documents revealing that the companies associated with PRISM were given millions of dollars in compensation for their cooperation in government surveillance (MacAskill, 2013, Aug 23). While it is likely that the corporations directly cooperated with government surveillance, their willingness to participate is irrelevant when considering their role in the development of algorithmic citizenship; these private companies already engage in extensive domestic surveillance that attempts to map consumer proclivities to target them with personalized advertisements. As noted above, Google has a "PREF cookie" that uniquely identifies a digital user and tracks their movements online. Google saves users search records, reads the content of emails, sells the information to advertisers, and uses it to track customers. For example, Google phones learn its users' movements and can identify where they live and work. Additionally, the phones can read emails in order to provide the person with a schedule and inform them of when they need to leave for an event, even factoring in extra time for traffic. These are only a few examples of the vast surveillance capabilities that private businesses use on a daily basis. With all this information being collected by companies to determine consumers'

dispositions, it is hardly a surprise that the government wanted to use this same data to track terrorist dispositions.

The ability for the government to justify its programs due to the pervasive surveillance power of private businesses demonstrates the normalizing rhetoric that is articulated through consumer and national security practices. In order to rationalize its egregious surveillance programs, the government can simply point out how common and prevalent surveillance is in our daily lives. Private companies are collecting personal information, in many instances under the auspices of keeping it secure, so it is not surprising for the government to request that information in order to protect national security. If police are able to monitor Facebook or Twitter in an attempt to identify and prevent criminal activity or if companies are allowed to track every purchase to protect consumers from identity theft, the government contends that the NSA should be able to do the same for the detection and prevention of terrorists. Likewise, if Google can analyze all of its consumers' data in order to determine their purchasing proclivities, the government rationalizes that it should be allowed to determine if those activities and choices could have terrorist implications. Once surveillance is normalized into the banal existence of daily communications, it becomes far easier for the government to persuade the public that it is only engaging in the same type of non-invasive surveillance that consumers interact and participate with every day for their own protection.

In the war on terror, consumerism becomes an active process by which citizens directly contribute to the war efforts. Information about individual's daily activities are capable of being turned over directly to the government to be analyzed through

algorithmic calculations that sort citizens' dispositions into categories such as citizen-terrorists or a citizen-soldiers. The NSA already has agreements with numerous corporations to release American citizens' personal information directly to the government (Macaskill and Dance, 2013). Even if technology companies claim that they are coerced or required by law to turn over the information that they collect, the problem, from the perspective of how normalization rhetoric is justified, is still that they collected the information in the first place (Macaskill and Dance, 2013).

Conclusion

The materialist mapping of the surveillance and war rhetoric of President Bush highlights the initial moves made towards the constitution of an assemblage of algorithmic citizenship. In defining the war on terror, the President began the transformation of citizenship away from the traditional conception of a private citizen towards the open, transparent, and collaborative citizen. In order to render citizens open and transparent, he articulated insidious threats that required citizens to sacrifice their civil liberties in the name of national security. The omnipresent threat to America's security was framed as occurring through elaborate terrorist plots such as those that occurred on 9/11. The threats were made more terrifying by linking them to the risk of WMD use by traditionally-labeled "rogue nations" that formed the Axis of Evil. While the military was capable of waging wars against the external threat, particularly nation-states, the military is not well-equipped to engage in an ideological conflict that operates both outside and within the U.S.

In order to protect the public from the ever-present threat of domestic terrorism, President Bush implemented many policies of mass surveillance. These programs were conducted both inside and outside national borders in order to match the nature of the threat as constituted by the administration. The implementation of mass surveillance inverted the traditional mantra of transparent government and private citizens, resulting in the state's control of information to promote secretive government policies while rendering citizens' communication open and transparent. Because the government must monitor citizens for the purposes of national security, the logic dictates that the government must not provide any information that could be useful to the enemy. As such, the government refused to be open about the way that it conducts the war on terrorism, especially in regards to intelligence gathering methods. Citizens are marked as suspicious and asked to submit to regimes of surveillance as well as performing the labor of watching and reporting on others. This information is then collected, sorted, and used to construct digital citizenship profiles that statistically determine and predict normal communication patterns from abnormal and suspected terrorist behavior. The collection of data profiles constitutes the initial interpellation of algorithmic citizenship.

The next chapter adds to this material map by tracking the economic narrative of algorithmic citizenship. The economic discourse supplemented President Bush's rhetoric of the fear of terrorism to justify surveillance with the entertainment value and fun of interacting with new digital technologies. As was noted earlier in this chapter, companies have been conducting mass surveillance for advertising purposes in a much broader fashion than the government. Taking IBM as a case study, the next chapter follows the

economic logic behind mass surveillance and maps the transition towards government 2.0. By following the corporate calls for transparency, discourse about the amusement and pleasure of participating in system of big data, and rhetorical circulation of government 2.0 rhetoric, Chapter 3 examines how the economic logic simultaneously informs the political logic of the war on terror and vice versa.

CHAPTER 3: A RHETORICAL ANALYSIS OF IBM'S THINK

While President Bush left office in 2008, it was not until 2013 that the general public became aware of the extensive government surveillance programs that the former president implemented. In particular, the public became aware that the NSA was working with private businesses to collect American citizen's data. Information about the PRISM program disclosed by Snowden to *The Guardian* and *Washington Post* revealed the names of major corporations, such as Facebook, Google, Microsoft, Skype and Yahoo, which participated these programs. Yet IBM, a company that specializes in data, was never implicated in the revelations about PRISM or any other secret surveillance program. Despite not being listed, the company's Senior Vice President of Legal and Regulatory Affairs and General Counsel, Robert C. Weber released an open letter in 2014 regarding the company's relationship to government surveillance. In the letter, Weber (2014) stated that IBM did not disclose any consumer information to the government as part of the PRISM program. Furthermore, Weber clarified that IBM did not participate in other projects such as providing backdoors or releasing source code or encryption keys to the government. If the government decided to request information, IBM vowed to take all legal means to fight any request for consumer data.

By publicly denouncing secretive government surveillance and data collection, IBM rhetorically casted itself as an institution that can be trusted with data because it is open and transparent. Meanwhile, IBM publicly celebrated itself as a private contractor, assisting and enhancing data collection and predictive analytics for governmental organizations such as local law enforcement, national security agencies, and the military.

In deploying a rhetoric of transparency, IBM was able to simultaneously condemn secret government surveillance and mandates that businesses turn over consumer data while also publicly collaborating with government organizations in developing the data collection methods used in mass surveillance.

Inextricably linked to the rhetoric of transparency is IBM's corporate belief that data is the next great natural resource. Under this paradigm, data must be collected so that the value can be extracted from it. In order to harvest data, IBM openly admits to needing the public to develop trust in new technologies (Weber, 2014). In a move to increase their credibility and gain public trust, IBM relies on the promotion of privacy and security. For example, in making a commitment to privacy to its clients, IBM argues that the company, "will continue to invest in world-class security technologies and services, and…engage the free flow of data while promoting strong security. IBM will also continue its decades-long tradition of privacy leadership" (Weber, 2014, para. 18). The stated goal for IBM is to establish trustworthiness with the public so that citizens will interact with new technologies and produce data that can be collected and used for the purposes of regulating society.

IBM promotes algorithmic regulation and government 2.0 through an economic logic working to discourage the government from decrypting business communications and encroaching on private businesses. In its letter regarding government surveillance, IBM pointed out that most of its business is not about directly collecting consumers' data, but instead working to connect businesses with one another. This allowed IBM to claim that it does not participate in government programs such as PRISM because it does not

collect consumer social media communications. Instead, IBM promoted collaboration between Facebook and the government to collect data on consumers in the name of counter-terrorism. As such, IBM works with civil and government officials, military organizations, national security agencies, and police forces to promote new forms of collaborative, interactive, and multi-directional communications between government, businesses, and citizens.

Using IBM as a case study, this chapter demonstrates the economic logic behind government 2.0 and the role it plays in the constitution of algorithmic citizenship. This logic holds that the collection of communication and use of surveillance produces value because data is conceptualized as a natural resource. While the previous chapter demonstrated the political logic deployed through the rhetorical tropes of collaboration, openness, and transparency, this chapter follows the economic logic behind these rhetorical tropes as they worked to inculcate in citizens a mindset to be receptive to participating in an informational economy that shares data freely. The economic logic relied on advertising enjoyable aspects of surveillance such as entertainment and fun to naturalize and habituate consumers' identification and participation with technologized subjectivities. To achieve this result, IBM promoted programs that are designed to persuade citizens to accept and interact with digital technologies. Exhibits such as THINK combined social entertainment with education in order to emphasize the importance of data for society to advance and progress.

IBM is a corporation that has transformed from a computer hardware manufacturing company into one that specializes in data. As such, it has a vested interest

in advancing the idea that data has economic, political, and social value because this is highly profitable for the company. In order to transform data into a valuable informational commodity, it must first be coded with an economic logic. The discourses of collaboration, openness, and transparency facilitate the neoliberal production of economic value by encouraging consumers to provide their data and allow it to be shared in an open network. The shared information becomes economically valuable as companies sell the collected data to other companies that are targeting people through personalized advertising. This individualized advertising uses consumers' digital profiles and dispositions in a co-constitutive process that cultivates a personalized consumer subjectivity. The interactive process of data collection and disclosure culminates in a subjectivity in which consumers actively shape who they are while simultaneously being shaped by an algorithmic framework that determines a set of identification possibilities. This economic data generates political value because it maps the population's dispositions and uses that information to manage and regulate society. This biopolitical mapping becomes a form of homeostatic monitoring that works to identify and apprehend or eliminate the threatening elements of the public.

This chapter tracks the rhetorical circulation of terms like collaboration, openness, and transparency as they are coded with value and overdetermined in an economic and political logic advanced by IBM. The chapter begins with IBM's rhetoric about global drivers that necessitate a transition towards government 2.0. In order to implement government 2.0, citizens must participate in a sharing economy with open data. To demonstrate how IBM normalized this participation in the sharing economy, the chapter

examines the THINK exhibit as it articulated citizenship with data collection and algorithmic predictive modelling. Finally, the chapter investigates how IBM celebrated its participation in government surveillance as proof of the successful implementation of transparency and government 2.0. Specifically, this section explores several case studies: the SIFT program that monitors social media; Blue CRUSH, a program that uses predictive analysis to predict criminal activity; and the Human Terrain Mapping project, which provides the military with information gathering technology for mapping foreign populations into an algorithmic model that is used to determine matters as significant as life and death.

IBM and government 2.0

IBM is a multinational conglomerate that was heavily invested in the financial valuation of data and the implementation of government 2.0. Because the theory of government 2.0 conceptualizes government as a platform connecting and regulating its users, IBM became one of the primary developers of this base operating system. In order to sell consumers on a transition to government 2.0, IBM published several studies that theorized how the world is rapidly changing and what governments can do to adapt to these developments. According to IBM, there are six independent drivers that were responsible for rapid transformations that were remaking the cultural, economic, political, and social terrain. These drivers were: demographic changes, environmental concerns, globalization, societal relationships, social stability, and technology (Cortada, Dijstra, Mooney & Ramsey, 2008). IBM used these the existence of these forces as rhetorical

justifications to rearticulate the public's relationship to government by constituting and diagnosing dangers that can only be resolved through IBM's government 2.0.

IBM's discursive strategies for implementing government 2.0 shed some insight into how social institutions such as multinational corporations and the state utilized the same biopolitical mapping for a range of different purposes that are sometimes in tension with one another. Foucault (1979) noted how the state has a vested interest in mapping the demographics of its population. But little did he realize the extent in which technology would enhance the capabilities to biopolitically map. IBM maintained that the world was becoming increasingly globalized and, as such, biopolitical mapping through data collection needed to be intensified to accommodate the rapidly changing world. For instance, because people can quickly move and relocate around the world indicates that countries face rapidly changing demographics and emigration and immigration will have global consequences. In other words, migration does not only affect the countries where people are leaving or moving but instead impact all places that are interdependent with those countries. For example, IBM marketed the effects of globalization as contributing to the "rising average age in many developed countries, such as Japan; falling average age in many developing countries, such as India; and a shift in the male/female ratio in China" (Cortada, Dijstra, Mooney, & Ramsey, 2008, p. 1). By constituting data as a natural resource, IBM augmented biopolitical mapping on a global scale to calculate, identify, and predict changes in global demographics at an ever quicker pace. The collection of data is used under the paradigm of government 2.0 to

algorithmically regulate society through personalized strategies tailored to the unique demographic shifts facing each specific population.

The second driver of accelerated globalization means that the radically different and constantly changing demographics can have larger and unpredictable effects. According to IBM, the world cannot be viewed as a collection of disparate countries; it must be examined as thoroughly interdependent. This basic tenant of globalization is heavily promoted by IBM as it rationalized the need for a new form of government that can react to global interdependence. According to IBM, accelerated globalization means that countries and social groups are becoming more interconnected as flows of bodies, capital, and information move between previously independent and sovereign institutions. IBM, as a multinational corporation perpetuated the hastening of globalization. For instance, the idea of a multinational corporation challenges the traditional notion of geographic boundaries by employing people and operating across the world. Thus, companies like IBM necessitated global flows of labor from China, India, and other locations where workers are leaving their countries in order to compete for jobs in the global labor market (Cortada, Dijstra, Mooney & Ramsey, 2008). The use of job outsourcing also magnifies the nature of globalization. For example, in the United States, manufacturing jobs are being outsourced to countries with laxer labor or wage laws. Moreover, the trend of accelerating globalization demonstrates that national economies are inextricably linked to the global economy. The U.S. credit crisis in 2007 had far reaching effects on banks all around the world that far surpassed U.S. territorial borders.

Globalization also had profound implications for the second driver: environmental shifts such as climate change. Emergent environmental concerns required that governments become "more attuned to what the earth can provide and what it can tolerate" (Cortada, Dijstra, Mooney, & Ramsey, 2008, p. 2). With rapid environmental changes, governments had to learn to regulate and preserve natural resources. In response to these needs, IBM stressed the importance of and addressing problems such as global warming and climate change and implementing green policies. To address these concerns, IBM argued that governments should collect and use the next great natural resource: data (Weber, 2014). In the IBM *2012 Corporate Responsibility Report*, Chairman, President, and Chief Executive Officer Ginni Rometty stated: "We believed this so-called 'Big Data' constituted nothing less than a new natural resource. What steam power, electromagnetism and fossil fuels were to earlier eras, data could be to ours" (p.5). By collecting as much data on the environment as possible, corporations and governments could statistically predict potential environmental problems and take action to preserve a state of homeostasis.

With its move to constitute data as the next important natural resource, IBM suggested that corporations and governments must tend to evolving societal relationships. This driver highlights how digital communications and social networks were altering how citizens and consumers connect to individuals and organizations around them. As globalization intensifies, IBM maintained that social life will transform away from the models based on "proximity, common language, and culture" towards more globalized decentralized networks that form through flexible, spontaneous, and global collaborations

(Cortada, Dijstra, Mooney & Ramsey, 2008, p. 5). Nealon (2012) describes this as "just-in-time capitalism," a phase in which companies work perpetually to provide consumers with experiences, products, and services (p. xi). As citizens become more tech-savvy, governments are called on by IBM to adapt to their constituencies and adopt practices such as providing government services on a "just-in-time" 24 hours a day, 7 days a week basis much like those provided by businesses (Cortada, Dijstra, Mooney & Ramsey, 2008). According to the company, governments must also transform their traditional functions such as legislating policy in order to best adapt to meeting the needs of the just-in-time flexible economy.

As governments are encouraged to adapt to the technological capacity of its citizenry, IBM maintained that society needed to confront the threat to the social order produced by technological advancement. IBM's researchers argued that, as the world becomes more globalized, interdependent, and technological, threats such as natural disasters, pandemics, and terrorism could escalate and effect larger populations (Cortada, Dijstra, Mooney & Ramsey, 2008). For example, terrorism is posited as a product of the neoliberal flexible economy. This is because terrorists operate through decentralized networks, with each cell operating as an independent node in "a decentralized, dehierarchized organization that relies on fluid and temporary connections—a distributed, postmodern organization" (Andrejevic, 2007, p 169). Therefore, within this frame, terrorists are considered to be an outgrowth of flexible capitalist economies. Just as workers can now work from the beach, coffee shop, or hotel lobby, terrorists can be extremely technologically savvy and work from mundane locations all over the globe.

Additionally, terrorists can operate as single individual "lone wolfs" or in small cells devising an explosive device capable of shutting down an entire city.

According to IBM, terrorism is not the only effect of a technological society. As technology continues to develop in ways previously unimagined, societies are encouraged to continue to modify and adapt. Currently, technology is developing far quicker than governments are able to legislate and regulate. Take for instance the issue surrounding the use of domestic aerial drones. Currently, people can commercially buy drones with cameras on them and fly them around recording everything that they see. This created situations where a person can fly a drone around a high-rise apartment complex and record intimate details of people living in the building. In this case, the citizens were familiar with how to use the technology, but the government had not been adapted laws and regulations fast enough to match current technological trends. In a government 2.0 paradigm, the government was expected to collaborate with technology companies and apply algorithmic regulation to quickly adapt laws to deal technological changes.

Because these drivers affect every government differently, IBM suggested that governments tailor individualized strategies to deal with their unique situations. While each government's specific strategy will have to be altered to their specific circumstances, IBM suggested that governments shift away from the approach of "slow, measured actions in the face of change" to an anticipatory approach to governance (Cortada, Dijstra, Mooney & Ramsey, 2008, p. 2). Rather than being reactionary, government 2.0 required governments to anticipate and predict which drivers were of

most consequence and respond in a manner that was "proactive, designing and then implementing customized strategies and solutions" (Cortada, Dijstra, Mooney & Ramsey, 2008, p. 2). To this end, IBM advanced what it called "perpetual collaboration," which it defines as "multilayered communication in many forms, connecting with entities both within and across country and organizational boundaries" in order to address the effects of global drivers (Cortada, Dijstra, Mooney & Ramsey, 2008, p. 2). Furthermore, IBM suggested that perpetual collaboration "supports the objective of exchanging information in any form, for any channel, between any type of sender and receiver. It is intended to leverage available capabilities across all facets of a society, not just within the governmental environment (Cortada, Dijstra, Mooney & Ramsey, 2008 p.7). As outlined by IBM, perpetual collaboration has four components: (1) organization, culture and governance; (2) partnerships, intermediaries and exchanges; (3) personalized interaction and services; and (4) knowledge creation and sharing (Cortada, Dijstra, Mooney & Ramsey, 2008).

Taken together, the four components of perpetual collaboration provided the theoretical justification for the development of algorithmic citizenship. The first element concerned the question of governmentality and invoked the call for increased transparency. As IBM explained, "a key element will be increased transparency about the effectiveness of public initiatives that measure results, communicate lessons learned and value experimentation. That also leads to mutual dependences for success among governments, businesses, and other institutions and citizens" (Cortada, Dijstra, Mooney & Ramsey, 2008, p.8). Here, the call for transparency worked by promoting data as a

natural resource to be collected, sorted, and utilized. In order to have transparency, the data that was collected must be made publicly available. Then the data could be measured to determine how effective the system of governing was based upon analytical calculations.

The second component involved collaboration as a value for government 2.0. Specifically, this constituent was based on forming new alliances, connections, and partnerships among differing agencies, businesses, governments, organizations, and services. To examine this at work, one only has to look at how IBM shifted from being one of the world's largest manufacturers of computers into a provider of numerous services. IBM was no longer concerned with manufacturing products; it was concerned about connecting businesses, organizations, and people together. While perpetual collaboration required new linkages to be formed, the manner of governing the new connections required individualized strategies.

The third part dealt with implementing personalized or flexible modes of governing rather than a one-size-fits-all program. Take for instance the marketing strategy which advanced the argument that,

> IBM leads the market in Portal and Collaboration capabilities; Government customers worldwide are using IBM Portal and Collaboration tools to deliver innovate services to their constituents; IBM will continue to extend our leadership through industry accelerators to address specific industry business problems; IBM software provides robust, secure, manageable solutions to deliver the latest Web 2.0, easy, fast, flexible technologies to your users; IBM portal solutions offer faster time-to-market and higher ROI than building custom solutions. (Tay, 2010, p. 37)

IBM provided a campaign strategy that adapted the concepts of web 2.0 into the governing practices of government 2.0. The fast and flexible technologies were used by

governments to communicate and connect with citizens through interactive modes. Interactive communication with citizens presented the possibility for flexible policies that used data to determine how to tailor individualized responses to specific problems on a globalized level. For instance, there were hundreds of governments that all relied on IBM to provide web 2.0 collaboration between groups such as citizens, employees, immigrants, intelligence agencies, and militaries. In creating a personalized response, IBM was able to create economic partnerships that expanded all across the globe.

To best form these financial networks, IBM relied on the fourth component that examined how information and knowledge was accessed and shared between people. For example, IBM CEO Rometty argued that the coming shift to adopting algorithmic citizenship, government 2.0, and predictive analytics will require a cultural shift in thinking (qtd. in Goudreau, 2013). This cultural shift moved the informational economy away from the assumption that possession of knowledge is valuable to one in which sharing knowledge is valuable. Thus, within this discursive frame, simply providing information was not as valuable as how one was rated by consumers and other networks for sharing such information. This was the sharing economy of algorithmic regulation, in which every activity and transaction between consumer and producer was based in a reciprocal rating process.

The hasty celebration of the sharing economy advanced by O'Reilly and others in the tech industry assumed that transparent data dismantles the hierarchical relation between consumer and. For instance, the ride-sharing company Uber connects drivers with passengers looking for a ride. People who want to use this system download a

computer application on their smartphone and register with Uber by providing their credit card and personal identification information. The Uber application then uses GPS data in smartphones to provide the location of consumers and drivers and connect them together. Payment for the ride is taken electronically and there is no process of negotiation or physical transfer of cash. After the payment process, consumers are asked to rate their driver and drivers are asked to rate their passengers. This type of reciprocal rating process was touted as transformative of the hierarchal business relationship. For example, drivers can theoretically refuse to pick up passengers who have low ratings, much in the same way that passengers can decide if they want to use a particular driver based on ratings.

The Uber model provides an example of how data was used as a resource through the process of personal disclosure and rating others. Perpetual collaboration required citizens to identify with a technological subjectivity of information sharing and transparent performances. Citizens had the means to access information networks and systems and the knowledge to interact and use online services. If citizens were tech-savvy, then governments were expected to adapt and provide the same online services to citizens that private businesses provided to their consumers. Specifically, IBM conceptualized government 2.0 as a conglomerated activity shared between citizens, businesses, and government employees and institutions (Tay, 2009).

Within this rhetorical mapping of government 2.0 and perpetual collaboration, social relations were often governed through algorithmic regulation that relied on results-based metrics that worked to maximize revenue. This new mode of governing relied on a

neoliberal model that shifted the responsibilities of governing onto citizens. For instance, IBM described this framework as a "self-service model for routine tasks, enabling employees to focus on critical issues" (Tay, 2009, p. 6). Communication and the sharing of personal information was no longer a passive system in which users merely stared at a screen. People now had the ability to collaborate online, actively participate in the production of knowledge through wikis or blogs, and engage in multi-directional information sharing. This new mode of interactive sociality was expanded to the arena of governance through the rhetorical constitution of government 2.0. For example, IBM described this transference to governing in stating:

> The interactive nature of today's Internet is a huge leap beyond what previously consisted of passive "surfing" to gain information. The Web has become easier to use as it evolved into what is now broadly described as "Web 2.0." It offers richer user experiences that include the opportunity to collaborate online through the creation of new content and vast opportunities for multi-directional information sharing. In a natural progression, citizens and other constituents increasingly expect this same sort of connectedness when they interact with government. As a way of enabling government/constituent collaboration using Web 2.0 characteristics, we envision the evolution of "e-government" – which describes governments' successful use of information and communications technologies – into "Government 2.0." Rather than citizen interaction and business transactions based on one-way information transfer, Government 2.0 can better address demands for personalization and connectedness through features that rely on various communication tools including online communities, blogs and other types of social networking. Sample programs within this category include citizen interactions, self-service and citizen self-responsibility. Strategy modifications are expected to include: Evolving government strategies – especially in procurement – to exploit value from engaging or creating networks; [and] Devoting a measured, protected amount of resource – both people and budget – to foster innovation. (Cortada, Dijstra, Mooney & Ramsey, 2008, p. 11)

IBM's discourse on government 2.0 interpolated a new communicative citizenry through the rhetorical process that transferred a corporate approach of customer service into a model of state governance. Because IBM specialized in data collection and analysis, it was able to use its data to construct a new mode of citizenship and governance that derived from an economic perspective. In other words, IBM used marketing data to determine the preferences of its consumers. This use of targeted personalized advertisements by IBM reaffirmed and affixed digital profiles to material subjectivities. The data was used then to regulate society through the implementation of a form of biopolitical governance adapted from customer service.

Algorithmic governance intensified security rhetoric through statistical calculation and risk assessment. IBM declared that perfect security was only a fantasy; governments had to calculate risks and weigh them against the costs to society. Therefore, IBM researchers argued that, in order to fight the risks of terrorism, government 2.0 must collaborate and share resources and knowledge between all levels of government and direct "social programs and communication efforts at interdicting the human conditions that can spawn disorder" (Cortada, Dijstra, Mooney & Ramsey, 2008, p. 11). As a result, IBM relied on a similar logic of collaboration deployed by the Bush administration during the war on terror. In order to fight social threats, the government must collect as much information as possible and then share it among all agencies to identify and apprehend problems before they occur. Technology became a platform for government 2.0 to outsource and out-task its work, by creating multi-directional

exchanges of information between the government and the public (Cortada, Dijstra, Mooney & Ramsey, 2008).

IBM and citizenship

The transition to government 2.0 was co-constitutive in the production of a new mode of citizenship. Citizens were no longer passive consumers, which is not to say that they do not consume. Rather, for government 2.0 to function most efficiently, citizens must enact their citizenship through the active sharing of data and information. Furthermore, for government 2.0 to work, citizens must be technologically savvy. As was previously stated, IBM marketed the necessity of government 2.0 because consumers rely on technology. Yet, in many cases citizens were technologically savvy because it was a necessity for existence. For instance, consider how difficult it would be to find employment today without access to a cell phone, computer, and internet connections. It is even becoming increasingly difficult to walk into a business and ask to fill out an application. Many companies have computers set up, so that when people come in to look for employment, they are directed to the computer stations and asked to submit their application online. In order to participate in today's society, citizens must possess some form of digital technology and the knowledge of how to use it (Allabaugh, 2012).

To possess knowledge was one thing, but citizens were encouraged to directly participate and interact with digital applications that collected and shared data with others. Good democratic citizenship had been linked historically to the citizen-orator, who was trained to speak publicly (Greene, 2003). Training in good citizenship was connected to the ways that communication functioned as a cultural technology. More

recently, this has shifted so that citizens are not merely capable of communicating through eloquent speeches, but, instead, are active participants in an informational economy in which all communications were to be collected as data that produced some form of value. The new communicating subject was called on to communicate freely, to participate in digital media that recorded communications, and provided the labor of watching and recording others and offering feedback on all information received. Good communicative citizenship culminates in a situation where all of the data produced could be translated into statistical algorithms that were used to predict and regulate society.

The training of citizens to become transparent algorithmic citizens was reflected in the rhetoric found in IBM's THINK exhibit. THINK introduced people to a historical linear narrative that articulated data collection with human progress. Those who visited the THINK exhibit interacted with and experience, data mapping first hand; this process naturalized predictive analytics and articulated it with citizenship and good government. The next section of this chapter tracks how the THINK exhibit operated as a rhetorical technique to promote algorithmic citizenship by immersing citizens into an interactive space designed to persuade them to adopt practices of collaboration and transparency.

THINK

The term "THINK" was adopted as IBM's corporate slogan by Thomas Watson in 1911. It did not take long before this slogan was plastered on buildings and signs all across the United States. THINK worked to develop a corporate culture which MIT Sloan School Professor Edgar Schein, the coiner of the term, defined as "a set of basic tacit assumptions about how the world is and ought to be that is shared by a set of people

and determines their perceptions, thoughts, feelings and, to some degree, their overt behavior" (IBM, 2011, March 11, para. 2). IBM management asserted that culture is the essence of management; by dictating culture, people do not have to be regularly told what to do but, instead, make the right decisions because they already know what to do (IBM, 2011, March 11). Therefore, corporate culture worked rhetorically to create a consensus about the world and then it offered this ontological framing to its constituency. The public was asked to accept this corporate culture through a dual process of identification and interaction.

In 2011, as part of its 100-year anniversary, IBM articulated its slogan into an experience with its THINK exhibit to share with the public how it understands "how the world works and how to make it better" (IBM, 2011, para. 4). Thus, the THINK exhibit took a slogan for corporate culture and expanded it into an interactive campaign to understand human culture writ large. The THINK exhibit was first displayed at New York City's Lincoln Center and later opened at Disney's Epcot Park in Orlando, Florida and Chicago's Museum of Science and Industry. The original exhibit was 7500 square foot pop-up interactive experience. The exhibit was comprised of three unique displays: the data wall, immersive film, and interactive experience. The data wall provided the visitors with a 123-foot digital wall. As IBM describes it:

> The wall visualizes, in real time, the live data streaming from the systems surrounding the exhibit, from traffic on Broadway, to solar energy, to air quality. Visitors discovered how we can now see change, waste and opportunities in the world's systems. (IBM, 2011, March 11, para. 6)

The immersive film consisted of a media field featuring 40 seven-foot screens that played a 12 minute film. IBM described what the public experienced as:

> A kaleidoscope of images and sound surrounded them. They were enveloped in a rich narrative about the pattern of progress, told through awe-inspiring stories of the past and present. They were inspired to think about humankind's quest for progress, and about making our world work better, today. (IBM, 2011, March 11, para. 7)

Lastly, the exhibit culminated in an interactive experience in which IBM stated:

> At the conclusion of the film, the 40 media panels became interactive touchscreens, transforming the space into a forest of discovery. Visitors could explore our quest to see more—from clocks and scales to microscopes and telescopes, RFID chips and biomedical sensors. They learned how maps have been used to track data, from early geographical maps to the most recent databases and data visualization platforms. They interacted with the models used to understand the complex behaviors of our world—from weather prediction algorithms to virus spread simulations. They heard from leaders of world-changing initiatives about how they built belief. And they read about some of the most inspiring examples of systemic progress around the world. Each touchscreen also gave visitors the opportunity to provide their point of view and learn what others were thinking. (IBM, 2011, March 11, para. 8)

The educational and entertaining aspects of the THINK exhibit encouraged people to interact with data mapping technologies which encouraged people to become good algorithmic citizens. People were taught that sharing data was fun and essential for human progress, which simultaneously worked to assuage any fears the public might have about participating in regimes of surveillance while also working to appropriate any criticism of the subjectivities that were produced. Indeed, the public was encouraged to further participate in interactive social conversations on Twitter by using #THINK as well as #IBM100 (Friedman & Lanspery, 2011). This process naturalized the collaborative process of the sharing economy while further collecting data that could be used to generate personalized advertising revenue.

The THINK exhibit targeted the general public as its audience. Unlike the corporate advertising, scientific research, and technical manuals used to market IBM to

the government, the THINK exhibit became an interactive site that used entertainment and pleasure to encourage the public to identify with data collection. The public was encouraged to attend a free large social gathering that provided educational and exciting activities that emphasized the importance of data for society. By interacting with the exhibit, the public became willing participants and potential public advocates of the practices of government 2.0. IBM was able to create a fun social event that generates publicity while simultaneously training citizens to participate in algorithmic regulation. If the people enjoy themselves, they were encouraged to publicly contribute to the conversation through the use of social media.

One way that IBM's THINK exhibit provided entertainment was through a video that provided visual mapping regarding the importance of data for human history to progress. The THINK video began with a collection of footage about human developing tools. The audience was shown a person making arrows or spear tips, another person molding a pot from clay, and a third person twisting in a screw. A voiceover remarked that since the beginning of their existence, humans have worked to make the world better by making it more accessible, efficient, productive, and safe. Next, the exhibit suggested that IBM has identified the pattern of progress. For instance, in using the example of space exploration, IBM noted that we first observed space with our eyes. Then we invented tools to see farther and with greater detail. Seeing with greater acuity was not good enough, so humans next created maps, and, as the video asserted, "mapping revealed relative position, scale, relationships, patterns. Over time we came to understand the dynamic relationships of the celestial bodies, the rules principles and laws

that govern our solar system. Seeing, mapping, and understanding culminated in a powerful force: belief" (IBM, 2011, October 24, p. 2). The next scene of the video is a clip of President John F. Kennedy talking about going to the moon. Thus, shared belief was credited with emboldening humans to progress and transform what was considered possible.

Overall, IBM identified the pattern of human progress: observing how the world behaves; mapping what we found; understanding causes and effects; believing we can create new outcomes; and acting to design, build, and improve systems around us (IBM, 2011). By following this pattern of progress, IBM argued that it had a prescription for dealing with the potential problems presented by the six drivers of government. Following the patterns of progress, IBM maintained that we can now transform the essence of humanity by reducing reality to data. For instance, IBM (2011) claimed that we can now see every biological change, cell, and heartbeat as a data point and it can be mapped into a more comprehensive picture. This data allowed for mapping patterns across entire populations, factoring in environment, genetics, and personal history. Information mapping was marketed to people as an essential method in making the world safer by collecting and using data to analyze how the world worked in order to predict future events. This scientific and technological framing of progress worked to normalize data collection, as the public was able to select their own path to learning about the various ways that data helped humans and society to progress. Moreover, the public was able to interact with technological exhibits while they learned about activities such as predictive policing. These people were taught that these programs created economic

prosperity, enriched social life, and made the world a safer, more sustainable, and livable environment. In other words, by interacting with the THINK exhibit, the public was being trained to accept mass surveillance as part of a cultural value of transparency and progress while having fun at the same time.

The THINK campaign was quite indicative of the shift from government 1.0 to 2.0 and from citizenship to algorithmic citizenship. People were encouraged to participate in an interactive technological learning environment that followed the IBM's *Pattern of Progress*. For instance, IBM invited the public to attend the New York exhibit for free and designed the exhibit so that any member of the public could interact and thus be hailed as algorithmic citizens. In the name of progress, IBM took visitors on a tour of a linear historical voyage of data collection. The collection of data was based on utilizing various surveillance technologies to record and capture data and information. As IBM explained:

> Visitors…learned how maps have been used to track data from early geographical maps to the most recent databases and data visualization platforms. They interacted with models used to understand the complex behaviors of our world—from weather prediction algorithms to virus spread simulations. They heard from leaders of world changing initiatives about how they built belief. (IBM, n.d. para. 8)

Surveillance and the mapping of data was used rhetorically to persuade the public to believe in a specific mode of progress. The THINK campaign was promoted as an attempt to educate and inspire the public to understand and embrace the use of surveillance technologies. Indeed, IBM polled users when they left the exhibit to determine whether they enjoyed the experience and were inspired to embrace IBM's

discursive framing of embracing the use of data in order to make the world a better place (Communication Arts, 2013).

In order to promote the THINK campaign, IBM also developed an application that could be downloaded on smartphones, tablets, and other devices. Educators were encouraged to use THINK by bringing it into the classroom to help educate students. For instance, New York Science (2012) marketed the educational application in stating:

> Using the THINK app… students will explore how progress is shaped through a common and systematic approach that follows a five-step process of Seeing, Mapping, Understanding, Believing and Acting (SMUBA). Your students will explore the process of innovation and participate in as many as three units, featuring hands-on lessons that will to help them become innovators in their own right and to take actions that can help them become forward-thinking citizens of the world. (para. 1)

These sentiments were echoed in Obama's 2013 State of the Union speech, in which he applauded the collaboration between the City University of New York, IBM, and the New York Public Schools in developing a curriculum that prepared students to graduate with a high school diploma and an associate's degree in computers or engineering (WH, OPS, 2013, February 12).

As a result, education became an important part in the promotion of self-government and the corporate citizenship advocated by IBM and, in a different way, President Obama. Citizenship, as President Obama informs us:

> …doesn't just describe our nationality or legal status. It describes the way we're made. It describes what we believe. It captures the enduring idea that this country only works when we accept certain obligations to one another and to future generations, that our rights are wrapped up in the rights of others; and that well into our third century as a nation, it remains the task of us all, as citizens of these United States, to be the authors of the next great chapter of our American story. (WH, OPS, 2013, February 12, para. 91)

Both IBM and President Obama articulated citizenship with being "Smart": both in the technological sense of smart technologies and the IBM slogan of building a smarter planet. Indeed, IBM (2012) celebrated its role in integrating corporate citizenship through programs that captured data and used it to regulate and govern society. The form of algorithmic regulation and government 2.0 was marketed as an efficient, fun, and personalized method of governance. The IBM THINK campaign invited its audience to interact, participate, work with systems of mass surveillance, and treat data as a natural resource.

The rhetoric of IBM's THINK exhibit and advocacy of government 2.0 combined the fear of unknown danger with the excitement and fun of technology. A globalized world, with new interactive communications between government and citizens presented, on one side, the idea that technology was fun and productive. However, one the other side, IBM still maintained that the world was a dangerous place that could be made safer through the use of data and transparency. Digital technologies provided the possibility to communicate and interact with others in ways that were not possible before. Those new forms of communication, therefore, contained the possibility for social connections between individuals or groups that also presented a threat to society. Consequentially, IBM reinforced the idea that people should be afraid of criminals and terrorists who are able to operate in decentralized and flexible networks. This is evidenced by IBM's research that advanced the idea that terrorism was a major driver against which the government 2.0 would have to develop an effective strategy.

In an attempt to formulate a neoliberal response to counter-terrorism, IBM marketed a holistic approach to predicting criminal and terrorist activity. This system was one that worked to collect and sort disparate surveillance data. In most instances, surveillance data was scattered across different levels. For example, government and law enforcement agencies had their own means of collecting data through such methods as police surveillance, closed-circuit televisions, and satellite or drone cameras. Similarly, yet separately, private businesses collected customer information and used private surveillance cameras. Additionally, individual citizens maintained surveillance by using their cell phone cameras or other electronic recording devices. Within this disconnected system, there was little data sharing. For instance, private companies only shared their information with police after a crime was committed or after the police requested such information. In comparison, new method predictive policing approaches called for by IBM worked to collect all of the disparate data, use it to create a real-time map of what was occurring, and share this information to help increase public safety.

Within this rhetoric about an effective response to global crime and terrorism, public safety was discursively framed through economic terms and associated with data collection to determine normal from abnormal behavior, communications, and dispositions. For example, collaboration and transparency were advanced as values that were necessary to protect individuals from private property crimes such as having a stolen credit card or identity theft. Additionally, businesses were encouraged to participate in surveillance and information sharing so that crimes could be predicted and deterred. If a crime did manage to occur, having surveillance and sharing that

information made it possible to identify and apprehend the perpetrator and restore a sense of security. This predictive model was linked to economic security because the abnormal or social threatening elements within business transactions and the larger economy could be detected, located, isolated, and monitored. IBM theorized that, if citizens and businesses freely share their information with law enforcement agencies, it would increase public safety by helping to secure economic prosperity (IBM Social Media, 2010). Thus, IBM marketed a holistic approach to public safety, based on the idea that the private sector had an obligation to collect data and share it in order to predict future events. This approach as consistent with the neoliberal ideology of collapsing distinctions between the public and private spheres so as to place the burden of security onto the citizens rather than the state (Andrejevic, 2007).

Because the communicating subject was also a data sharing subject, data could be used to construct a statistical model of reality. Data analytics works through a threefold process that is descriptive, real-time and predictive. These analytics worked to historically anatomize past events inscribed in data by taking past information—e.g., bank statements, consumer purchases, emails, medical records, or phone calls—and detecting repetitive routines. Taking the data that was collected and organizing it into patterns worked to establish a predictive model for answering the question, "what will happen next?" (*Insider Surveillance*, 2014).

Predictive analytics rhetorically functioned through a process of inscribing identities onto material bodies based on past data. The use of digital data to discover a subject's identity was a production of algorithmic citizenship. This data mapping of

information onto material bodies algorithmically worked to identify who a subject was and then identify the most efficient ways of regulating those subjects in order to make them adopt specific modes of subjectivity. Furthermore, the configuration of algorithmic citizenship could be used to overcome obstacles presented through other modes of citizenship. Take for instance the NSA domestic spying discussed in Chapter 2. While the NSA was prohibited from directly spying on US citizens, it used browsing data to assign a percentage score to everyone on the internet. If that score dropped below what the data constitutes as 50 percent "American," then NSA tracked them because their algorithmic citizenship identified them as most likely being "foreign," regardless of the national origin or physical location of the person (Birdle, n.d.). As a result, data collection had profound implications on citizenship, connecting information with bodies that had severe material consequences, even if it had little direct material connection.

Predictive analytics

After examining how private data collection was rationalized by IBM in ways that led to the development of biopolitical predictions, I now turn to examining how these predictive analytics discursively functioned in a government 2.0 paradigm. IBM described predictive analytics as occurring through a three-step process. The first step was to collect all available data. This measure was not to be taken lightly as the existence of big data—large amounts of data that are both structured and unstructured—required that all possible information be collected. This means that even unstructured data such as "emails, text messages, audio and video files, health records, journals and open-ended survey responses" must be collected (IBM, 2011, March 17, para. 4). This data was then

used to define and describe "normal" behavior and data (IBM, 2011, March 17). The ability to associate statistical patterns with a standard of normality meant that data that deviated from the norm was identified and classified as abnormal and thus suspicious.

The practice of data normalization was highlighted by IBM (2011, March 17) as occurring through three general approaches: prediction, association, and clustering. Prediction analyzed historical patterns to determine the most likely future results. Association linked events that occur together and makes a determination of what action is likely to occur given a specific series of events. Clustering worked by identifying groups of data that share similar characteristics. Once the data was analyzed for patterns and norms, the data was made accessible and comprehensible so that people could use it to identify problems in real time and take specific action. This was the way in which raw data was transformed into a valuable commodity that worked to detect and identify abnormal, criminal, or terrorist data subjects.

In order to detect patterns of criminality, police and government officials relied on the same logic that corporations used to determine consumer purchasing trends. They operated under the assumption that criminals are consumers of crime; therefore, they followed similar patterns as other consumers and, through predictive technologies, the police could follow these trends and patterns and attempt to prevent crime or terrorism from occurring (Lever, 2012). Corporations and private businesses typically market personal data collection as a more efficient form of advertising. Companies can collect data and run it through their algorithm in order to advertise to specific individuals rather than marketing to homogenized demographics. The more insidious side of personalized

advertising, however, is that data collection can be used for the purposes of social profiling as well as targeting and marking bodies as abnormal, statistically deviant, and likely to be associated with criminality or terrorism.

Law enforcement agents attempted to rationalize this profiling by appealing to the neutrality of quantitative mathematical equations. The logical syllogism at play in the arguments being used to justify quantitative mathematics was: morality is inherently human; math is not human; therefore, math cannot be immoral (Kun, 2015). However, this argument failed to acknowledge the role that humans played in the collection of data and the way that it is subjectively analyzed. For example, human bias can be naturalized into the algorithmic processes which can infer concepts such as race and use them indirectly in the decision making process (Kun, 2015). For instance, Jeremy Kun (2015) provided a picture of a Google webpage search which he typed in the search terms, "transgenders are." The algorithm suggested finishing the query with: crazy, freaks, gross, sick, and wrong. When I personally used these same search terms in Google, I was provided the following auto-completion suggestions: delusional, mentally ill, and sick. Google's autocomplete feature is a quantitative collection of data that summates all the searches on Google and displays the most common completions of a given search. Even though this process appeared to be neutral and used math to count all of the search terms, the algorithm detected trends that represent biased and harmful stereotypes.

The practice of predictive policing that was championed by IBM as an example of social progress and public safety also worked to intensify the stereotypical association of personal characteristics with criminality. For instance, predictive policing often weighed

an individual's associates' and acquaintances' backgrounds, geographic location, prior criminal record, and socio-economic status. This information was used to determine the likelihood that a person was going to be a criminal (Desouza & Smith, 2014). In cities like Chicago, once people were identified as likely being criminals, the police would visit them and issue them a warning that they were being watched and should refrain from committing crimes (Desouza & Smith, 2014). For individuals who had already committed a crime, their data was being used against them to determine sentencing. This type of evidence-based sentencing was a practice that quantifies the risk that an individual represents to the community in the future and worked to predict the likelihood of recidivism. However, with the collection of big data, judges were also able to take into account personal characteristics such as a person's economic background, education level, employment history, or other factors that are then used to justify legal sanctioning.

Moreover, the use of data to scientifically predict a criminal's disposition was far more dangerous because of its appeal to neutrality. For example, in 2013, there were 1,574,700 people in state and federal prisons. Out of that number, over 37 percent of the men incarcerated were black and 22 percent were Latino (Carson, 2014). While the majority of female prisoners were white, the imprisonment rate for black females was twice the rate of whites (Carson, 2014). It was these kind of statistics that could be used to justify racial targeting of minority populations because one in four black men was likely to be incarcerated. Because black men were likely to be targeted, predictive analytics advocates asserted that police should increase its surveillance of black men because statistics prove that they were more likely to commit more crimes. The same

logic extended itself to the targeting of Muslims in the name of counter-terrorism. Intelligence agencies were more likely to target someone if they were a Muslim with family in Pakistan or Yemen.

The value placed on statistics in the use of targeting minority populations was reaffirmed by reports such as the Department of Justice's 2015 *Investigation of the Ferguson Police Department,* which demonstrated how public safety was couched in terms of generating economic revenue and how arrests were often racially biased. Given that the police had a history of racial profiling, it was not a vast leap in logic to find that the same predictive analytical logic was applied by police officers to justify state-sanctioned killing of black people. Relying on information produced through computer algorithms, police officers operated through a conditional "if/then" automated response rather than any form of deliberation. Thus, the racial implications of the use of this response system was that when a police officer encountered a black man that he deemed suspicious, the officer had to weigh the possibility that the man may be armed or physically resist arrest. If the officers assumed any of those possibilities, then they proceed algorithmically: if a suspect was a threat, then they must be apprehended. In order to apprehend the suspect, a police officer justified using appropriate force, which in many cases, could be lethal.

With this broad understanding of how algorithmic profiling operates, I now move to examine specific IBM programs that publicly market algorithmic profiling and big data collection for the purposes of governing and protecting the population. The first one is IBM's SIFT program that monitors social media to quickly identify abnormal or

threatening communications and alert the proper authorities. Building on the social surveillance of the population, I next explore IBM's predictive policing program Blue CRUSH. Lastly, I investigate IBM's Human Terrain program, noting how big data and predictive analytics are used at a global military level to secure the population through the elimination of external threats.

Monitoring social media through SIFT

The economic logic entangled with discourses about open and transparent data, collaboration, and corporate citizenship have the material biopolitical consequence of transforming citizenship into an algorithmic calculation that demarcated the population into normal or abnormal communicators. Despite its claims to not participate in secret government surveillance programs, IBM publicly advertised its social media surveillance program, Social Intelligence Fusion Toolkit (SIFT) program that is powered by IBM portal software. The SIFT program collects citizens' digital communications and searches them for illegal activity that is then reported to authorities. This program is celebrated and justified by IBM because it promoted the value of searching public data combined with the biopolitical rationality of protecting citizens from crime or terrorism. This was reinforced through the IBM argument that, "Smart is… [m]onitoring publicly available data to detect illegal activity" (IBM, 2014, May 28, p. 1).

IBM and other private companies were now working with law enforcement officials to monitor citizens' public communications on websites such as Backpage, Craigslist, Facebook, Flickr, Twitter, and other social media (IBM, 2014, May 28). This surveillance was made possible in part because IBM advocated for openness and

transparency of data. Because most of these media were considered to be public domain, the data that was produced on them was not legally considered private. Therefore, IBM and its partner companies searched publicly available data by conducting keyword searches and looked for posts that could suggest criminal or terrorist activity. The information was distributed to federal and local agencies, because the searches could be based on jurisdiction and limited to a space as small as one square mile. Entire network searches could then be stored as evidence and used in court cases and reports of criminal activity could be sent immediately to law enforcement (IBM, 2014, May 28).

IBM (2014, May 28) maintained that this technology worked under the values of government 2.0 because the data collection software and portal was "a powerful solution for delivering web content and applications in an integrated, differentiated and personalized web experience" (p. 2). Moreover, this technology was designed to enhance collaboration among agencies, such as the "U.S. Coast Guard, state police, the Department of Homeland Security and the local sheriff's department with intelligence for decisions that protect all citizens" (IBM, 2014, May 28, p. 1). Thus, the new biopolitical response of protecting the population depended on private companies analyzing data and sharing it with government agencies in order to map abnormal or threatening communication.

IBM's collaboration with law enforcement demonstrated how the discourse of collaboration, openness, and transparency fused an economic logic with a biopolitical rationalization of using that data to predict and determine threats that could be contained or eliminated quickly. Arguments in support of the use of the SIFT program contended

that communication on social media was public communication and therefore must be open and transparent in order to determine normal safe communication with unusual, potentially dangerous communication. For example, "bad guys" such as criminals, gang members, and terrorists used social networks to communicate and collaborate in ways similar to the good tech-savvy citizen. In order to determine who was "good" or "bad," all public information must be sorted through in order to determine communication that was likely associated with criminality. IBM marketed this in its example of someone tweeting about "packing heat" or the use of slang suggesting that a drug deal was occurring. According to IBM, SIFT technology could be used to determine the meaning behind slang terminology, establish it was a threat that needed to be controlled, and then share it with other members of law enforcement to surveil those who used such unapproved rhetoric.

Blue CRUSH

IBM's SIFT program sought to persuade the public that the police needed to be able to monitor social media communications as a form of public communications so that criminal activity could be detected. Through programs such as Blue CRUSH, IBM worked to coordinate the collaboration between SIFT data collection and advanced crime prevention and policing analytics. The request for the public participate in open and transparent communication was magnified through interactive collaborative processes that allowed citizens to contribute directly in the policing of their own communities.

Blue CRUSH (Criminal Reduction Utilizing Statistical History) was founded through the collaboration between the Memphis Police Department (MPD) and retired

professor Richard Janikowski. A criminology professor at the University of Memphis, Janikowski researched the use of statistical data for crime prevention. Utilizing statistical software provided by IBM, the CRUSH program was founded with the principles of collaboration between academia, law enforcement, and private businesses. Blue CRUSH implemented the IBM model of a smarter city and smarter law enforcement through a three tier process instrumented, interconnected, and intelligent. It was instrumented in that Blue CRUSH collected and sorted information from the police department's criminal reports and records, as well as from other sources. Then Blue CRUSH integrated statistical modeling and analysis to determine where crime was occurring and shared that information instantly with the police department. This tracking of criminal activity was calculated to determine patterns of criminal activity which were used later to predict future crime hot spots and direct police to act preemptively (IBM, 2011).

At the heart of the program was a predictive model that incorporated up-to-date crime data from sources that range from the MPD's records management system to video cameras monitoring events on the street (IBM, 2011). Blue CRUSH relied on mass surveillance and received information from citizens and police sources. In order to get the help of citizens, the police and their partnering academic researchers attended more than 200 community and neighborhood watch programs in an attempt to solicit support. To collaborate and sort all of the information gathered, the police department built a $3.5 million Real Time Crime Center, which monitors and records every reported crime, report, and phone call made to the police (Figg, 2014). Furthermore, police officers carried personal digital assistants (PDA), providing faster communication for officers.

Additionally, surveillance cameras were mounted in high-crime areas to both deter criminal activity and provide more data for the police to utilize. Some police vehicles were also equipped with license plate reading cameras so that vehicles could be tracked and located more efficiently.

Blue CRUSH worked by using statistical calculations to produce multilayer maps that isolate criminal hot spots, while providing the police with information regarding changes in criminal activity based on previous factors such as police deployments and alternative tactics. This information allowed police to see, for instance, that burglaries were higher in one neighborhood, while car thefts were occurring at a higher rate in another area of town, allowing the police to respond accordingly. This new method of policing was credited by the Memphis police department as resulting in over a 30 percent reduction in serious crime and a 15 percent reduction in violent crime (IBM, 2011).

Predictive policing, in some instances, offered some intuitive and positive crime prevention techniques. For example, Janikowski argued that in the 1990s, Memphis ranked at the top of the nation in forcible rapes (Figg, 2014). However, by taking an analytical approach, the police and researchers discovered that pay phones in low-income areas were by and large in dimly lit locations outside of the purview of businesses. In analyzing the data concerning rape locations, the police were able to target these areas and make adjustments, such as moving the pay phones inside of stores and increasing police presence in designated spaces. While these programs were not connected specifically to Blue CRUSH, they did demonstrate how data collection could dramatically decrease forcible rapes in the Memphis area. In another positive application,

the Memphis Police Department was able to identify a number of crime hotspots, resulting in 1,200 arrests for largely "quality-of-life" crimes. The police department also identified the major sites where drug, graffiti, and prostitution were happening and increased arrests for these crimes.

Overall, the Memphis CRUSH program worked to combine data analytics to diagnose the key areas where crime occurred and relied on surveillance and police presence to deter crime. However, police deterrence would not have worked without getting citizens to police themselves. Thus, in addition to data analytics, the police engaged in public outreach programs in an attempt to persuade the members of the public to surveil their own communities. In order to implement Blue CRUSH, the Memphis Police Department increased contact with community leaders and neighborhood groups, developed "diversified and sustained media exposure," and engaged referral agencies and service organizations (Memphis Police Department, 2014). The popularity and success of the Blue CRUSH program provided police with the ability to develop the Community Outreach Program (COP) that worked to establish better relations between police officers and the community (Figg, 2014). The COP program also worked to train citizens to detect and report suspicious behavior. It did this through several programs such as basketball tournaments, black history trivia nights, and police ride-a-longs. Moreover, the program provided citizens training in hopes that they could serve as liaisons between the police and the community (Memphis Police Department, 2014).

While the Blue CRUSH program had some positive effects on the Memphis community, it also produced some problematic effects. First, recruiting members of the

community to surveil one another worked to cultivate a culture of suspicion. Walter Benjamin (2003) wrote that, "In times of terror, when everyone is something of a conspirator, everybody will be in the position of having to play detective" (p. 21). CRUSH and predictive policing began with a discourse of suspicion that framed anyone as potentially involved with crime; thus, everyone needed to be vigilant and report any potential threats. As a result, members of the Memphis community were recruited through public relations and educational awareness campaigns to take on the role of citizen-detectives in order to be suspicious of others around them and to report any threat to law enforcement.

Second, encouraging members of the community to work alongside law enforcement can erode trust in the community. Arun Kundnani (2014) explained that when law enforcement recruited individuals in communities to act as informants and spy on one another, surveillance was no longer a problem of monitoring threats but instead was "intertwined with the fabric of human relationships and the threads of trust upon which they are built" (p.13). Minority communities were uniquely targeted for surveillance by law enforcement, using data to objectively confirm that criminals or terrorists have statistical demographic commonalities. Furthermore, the government has a long history of spying domestically and working to infiltrate minority groups through programs like the FBI's COINTELPRO. For instance, the American Indian Movement, Black Panthers, and civil rights leadership were all targeted by government surveillance, which produced distrust between specific minority communities and law enforcement (Kundnani, 2014). It was because of these historical tensions that the police offer

numerous community programs such as black history trivia in order to rebuild a relationship between law enforcement and minority communities. In the name of helping to build community relations, the police encouraged people to be suspicious of those around them and to spy and report on their neighbors. Instead of serving as a bridge to racial harmony, these programs worked to sow distrust in communities by encouraging members to inform on one another and to provide data that was used to target suspicious elements of community.

Overall, community policing concealed the asymmetrical power imbalances that used citizen's immaterial labor to contribute in the construction of statistical criminal profiles that reaffirms and magnifies existing racial stereotypes about the community. Foucault (2003) explained the biopolitical situation that comes when citizens are encouraged to report on one another, stating, "[u]ltimately everyone in the Nazi State had the power of life and death over his or her neighbors, if only because of the practice of informing, which effectively meant doing away with the people next door, or having them done away with" (p. 259). While it is not my intention to compare the U.S. domestic surveillance to that of Nazi Germany, it is possible for me to draw a parallel regarding the biopolitical implications of citizens spying on each other. While reporting one's neighbor as a criminal or terrorist may not mean that an authoritarian state will kill that person, it does operate in ways to statistically configure a person as a threatening element who could be targeted and potentially killed. As both Presidents Bush and Obama have made clear, if a person was associated with terrorism, they could be denied the privileges and rights afforded to him or her by citizenship. Moreover, there was a

legal precedent that justified the elimination of threats, even if they were citizens, by drone strikes. For instance, Imam Luqman and Ibragim Todashev were examples of citizens identified as being associated with terrorism who were killed abroad by the U.S. government. The next program discussed, the Human Terrain Systems Project, further tightens the linkage between analytic threat profiles and military and CIA combat operations.

Human Terrain System project

While IBM publicly denounced playing any role in secret surveillance for counterterrorism purposes, it publicly celebrated assisting the military with overt counterterrorism surveillance to aid in the transition towards government 2.0. Specifically, IBM posited itself as playing an instrumental role in the military's Human Terrain System (HTS) project. In order to promote the HTS, IBM relied once again on discourses of collaboration and transparency. The rhetorical strategies exposed how the economic rationale of government 2.0 produced value through analyzing and sharing information between civilian academic scholars and the military. For example, the HTS relied on collaboration with social scientists such as anthropologists, asking them to study local populations in order to provide a cultural topology for the military to analyze.

In developing software for this program, IBM facilitated the transition towards the neoliberal privatization of warfighting and corporate war profiteering. By marketing themselves as providing a product that helped the military in national security, IBM directly profited from the war on terror. First, IBM benefited from the war itself because they could sell technology to the military that was used in the war. Second, because IBM

has a contract with the military, they could promote this connection in order to generate public appeal for their services. IBM is very transparent about advertising their collaboration with the military as a positive contribution to national security; it was not difficult to find many IBM statements about the company's connection to HTS and how this would aid in a transition to government 2.0. Finally, IBM further profited from selling its technology in the private sector to companies and businesses that were looking to invest in military-grade technologies.

HTS was inextricably linked to the production of algorithmic citizens, the cultural mapping of normal and abnormal dispositions, and the targeted killing of specifically demarcated bodies. IBM may not have participated in secret government programs; however, it did participate openly in developing and selling software used for the purposes of national security. For instance, when a military team in Afghanistan needed to quickly transform vast sums of raw data, including the full spectrum of human-, communication- and imagery-related intelligence to identify patterns and relationships, it turned to IBM's i2 Analyst's Notebook software. This program allowed the military to combine all data collected from various individuals and units so that it could be sorted to determine relationships and patterns, converting disparate data into a cohesive picture that could be easily shared. IBM promoted this technology because it allowed the military to maintain a predictive and anticipatory form of surveillance that was capable of anticipating the "cause and effect of actions" (IBM, 2013).

IBM used collaboration rhetoric to market itself as providing services that helped soldiers collect real-time data about the cultural that they were confronting. The fact of

the matter was that IBM worked to connect the military with private academic contractors that were attempting to distinguish between the vast cultural differences between various members of al Qaeda and the Taliban into an orientalist cultural topography that could be used by the military to understand the local population. In other words, the collaboration was an advertisement for the neoliberal practice of outsourcing warfighting from military soldiers to private contractors. For example, the anthropologists are not soldiers; they are private researchers who are paid to research and analyze the cultures of the areas with U.S. militarily engagement. In doing this work, the private researchers used stereotypical ideas of culture to homogenize a group of people that hailed from over 60 countries into a single unified group known as al Qaeda (Gonzalez, 2007). However, these researchers were not only recruited by government agencies; numerous private companies that the government outsourced to help fight the war on terror also relied on hiring academic researchers to serve as cultural analysts who worked to provide intelligence in warfighting (Gonzalez, 2007).

The purpose of the HTS scholars' was to come into countries where the U.S. was conducting military operations and served as translators and researchers who collect information on the area. The information was to be used to create a cultural map of the area that was used to gain a military advantage or identify enemies that needed to be eliminated. Yet, the lofty aims of the problem were not met with success. Unfortunately, in many instances, the western academics who were collecting the information did not have the local cultural knowledge necessary to create an accurate understanding of the terrain (Gezari, 2013). According to the *New York Times*, there was an area of

Afghanistan where over 90 percent of women and 63 percent of men could not read or write (Gezari, 2013). Given the literacy rates, it was hardly surprising that the area relied on the production of an oral culture that used allegories, jokes, metaphor, parables and stories to express meaning. However, soldiers and HTS members were trained to read technical military manuals and they applied very literal meanings to the stories that they encountered. Thus, a great deal of cultural misunderstanding occurred as the members of HTS decoded the Afghani stories through a western cultural lens. The misunderstanding could have resulted in the loss of human life as military decisions were made based on flawed analysis.

In 2007, the American Anthropological Association's (AAA) Executive Board issued a statement condemning the HTS project and its use of academics as private military contractors. The primary criticism was that, when the military brought in scholars such as anthropologists as private contractors, the researchers would cease to be distinguishable from military operatives. This argument is supported by news reports that the anthropologists and other academics would carry weapons and wear military attire (Gezari, 2013). Moreover, the AAA worried that informed consent was difficult to receive because the anthropologists were being paid by the military, thus possibly compromising their honesty with the research subjects about the nature of their work. Most worrisome of all was that the information collected by anthropologists was used to identify and select military targets, which violated the AAA code of ethics that research subjects would not be harmed by researchers.

In comparison, IBM did not have similar ethical qualms about aiding HTS and, instead, focused on the collaborative manner in which the program advanced the practices of government 2.0. IBM developed the software that was capable of taking all of the information collected by the cultural experts, analyzing it, filtering out the unnecessary information, and sorting it in a useable manner. IBM marketed this service by stating:

> the offerings target law enforcement, defense, government agencies, and private sector businesses to help them maximize the value of the mass of information that they collect to discover and disseminate actionable intelligence to help them predict, disrupt and prevent criminal, terrorist, and fraudulent activities. (IBM, 2012, para. 40)

In a rather technical manner, IBM used language about intelligence gathering adaptability and efficiency to describe its role in the HTS program:

> Supporting simple to complex scenarios, the IBM i2 Intelligence Analysis product portfolio is a flexible, scalable, enterprise-class intelligence environment that aggregates investigative, analytical, operational, strategic, and command level capabilities and tools, including advanced security features. It creates an ergonomic environment that works across all phases of the investigative and analysis process to help break down information silos and enable close-working and collaboration at local, national, and global levels to generate evidence-based actionable intelligence for more rapid decision-making. (IBM, 2012, para. 15)

In using this technical language, IBM was able to bypass the ethical questions posed by contributing directly with government surveillance programs that are denounced for militarizing academic scholars and civilians. Instead, IBM posited itself as promoting the efficiency and flexibility required for government 2.0.

By promoting itself as a proponent of transparency of government 2.0, IBM was able to profit from the demand for global surveillance in the war on terror. For instance,

Army Lieutenant Colonel Anthony Cruz (2011) argued that IBM applications such as Watson were essential for engaging in counterterrorism activities. He maintained that IBM software provided the military with the technological ability to sift through immense amounts of data collected from numerous disparate sources and reduce it into useable intelligence. Cruz (2011) further noted that IBM's technology was capable of deciphering and translating any language that the military confronted and, with advanced biometrics, determine facial features in order to identify enemies. In other words, users of the software could take information collected by language and biometric facial recognition technology and use that information to link suspected terrorists with a digital profile. In doing so, users of the program were able to use surveillance information to identify enemies and mine for patterns of suspicious activity. As a consequence, enemies that were identified by the information gathered could be placed on the government's kill list.

While IBM profited directly from information used to identify and kill suspected enemies, there was the possibility that IBM might expand the market to include automate warfare. Cruz (2011), for instance, believed that IBM technologies such as Watson would provide the military with a superior method of controlling swarms of drones. This was possible because robots or an AI controller would be better able to control and execute swarm attacks, whereas a single person would find it difficult. While this scenario may not happen, IBM was highly invested in domestic surveillance and war profiteering. Specifically, IBM provided the services that were used to construct terrorist profiles and identify suspicious communication patterns. This allowed IBM to directly

profit from government surveillance while promoting itself as adhering to the values of transparency. IBM was able to dissociate itself from irresponsible companies such as Facebook, who released user data to the government or participated in secret surveillance programs such as PRISM. Yet, at the same time, IBM openly sold the government the information gathering tools that it needed to monitor social media sites such as Facebook.

Collaboration, openness, and transparency rhetoric coalesced together in IBM's marketing materials to promote its participation with government surveillance as an efficient, progressive, and smart transition towards government 2.0. In framing its participation with government surveillance as collaborative business, IBM was able to draw distinctions between itself and unethical companies that participated in secret government surveillance programs. Because IBM was open about its business transactions with the government and military, this behavior was advanced as a sign of the success of efficiency and transparency. The collection of data was reframed not as promoting government surveillance and instead is portrayed as a progressive politics of using data to make government smarter. The public was then encouraged to embrace and interact with government 2.0 because sharing data was an exciting adaptation of the values of collaboration and openness.

Conclusion

IBM's advertising strategy to promote government 2.0 relied heavily on the construction of data as a natural resource. In order to harness this resource, it relied on the circulation of rhetoric about collaboration, interactive participation, and transparency. The move towards openness constituted a decisive discursive shift away from the Bush

administration and towards an alternate mode of citizenship and governance. For example, the Bush administration implemented policies of mass surveillance and information gathering that were shrouded in secrecy and classified in the name of national security. Classifying information as secret provided the Administration the advantage of moving government surveillance outside the realm of public deliberation; however, it simultaneously ran the risk of generating public backlash if the secret was exposed. By and large, the Bush administration was able to contain leaks regarding government surveillance for the majority of its time in office. However, once information leaked, the Administration's surveillance programs were often legally rationalized and hailed as effective tools in the fight against terrorism.

By the time the public became aware of the extensive nature of government surveillance, President Obama was entering into his second term in office. The leaks revealed that private companies were cooperating with government surveillance programs by turning consumers' information over. The link between targeting consumers for advertising and national security purposes was established and private businesses specializing in consumer data were going to need a new rhetorical strategy to maintain consumer trust. IBM relied on the construction of algorithmic citizenship, circulating collaboration and transparency as values that the public needed to adopt. By framing data as a natural resource, citizens were encouraged to engage in transparent performances that provided useful information for effective government. Put differently, government 2.0 provided a useful heuristic for soliciting citizens' participation in providing their data. Citizens were encouraged to open themselves up to be rated and

rate others in a new interactive mode of government that requires the participation of algorithmic citizens.

Examining IBM as a case study in the implementation of government 2.0 provides insight into the economic logic that accompanied the production of algorithmic citizenship. Part of the strategy was to make economic systems such as globalization and technological modes of subjectivity seem inevitable. For example, IBM posited globalization as natural and inevitable. Furthermore, citizens were framed by IBM as being technologically savvy. As a result, this rhetoric of inevitability normalized economic logics of globalization and neoliberalism as a natural development and, as such, governments must adapt accordingly. Therefore, government 2.0 was shaped by economic expectations that it operated in line with private business that provide flexible 24 hours 7 days a week services to its users. Returning to O'Reilly's notion of algorithmic regulation, the government was posited as being a platform that provided flexible services and interactive communication to its citizens. Under this government 2.0 paradigm, citizens were re-conceptualized as consumers or users that interacted with a government platform.

While the articulation of citizenship with consumerism has the potential to operate as a rhetoric of control and governmentality, it also has the ability to provide citizens with new modes of connectivity, interactive communication, and public engagement. Rhetorics of collaboration, openness, and transparency provide citizens with the ability to quickly access information about how government operates, communicate directly with those in power in more flexible ways, and engage in public

debates that are visible to incredibly large and diverse audiences. In fact, it exactly this balance between algorithmic citizenship and government 2.0 that Barack Obama campaigned on in 2008 and then had to navigate throughout his presidency.

The next chapter explores the presidential rhetoric of Barrack Obama as he navigates the informational continuum from secrecy to transparency. While President Bush secretly implemented government surveillance in the war on terror, many of the details were leaked later during President Obama's term, requiring him to publicly address and unveil those programs. This development required President Obama to rhetorically strike a balance between promoting transparency and national security while publicly addressing how surveillance and warfighting have intensified. Analyzing President Obama's rhetoric provides insight into how the economic logic of transparency was over-coded into a political logic. That is, while this chapter mapped the economic logic embedded within the rhetoric of collaboration and transparency, the next chapter follows how Obama deployed the same discourse into a political strategy for conducting the war on terror.

CHAPTER 4: THE MOST TRANSPARENT ADMINISTRATION IN HISTORY

In the lead up to the 2008 election, President George Bush received the lowest public approval rating for a president ever, polling at a dismal 22 percent (CBS News, 2009). Public support for the Bush presidency was rapidly dwindling, but there were two specific issues that dissatisfied American people: the economy and wars in Afghanistan and Iraq. Support for the war on terror had declined from almost 90 percent approval in 2001 to 47 percent by 2008 (CBS News, 2009). Furthermore, while public approval was high for the war in Iraq in 2003, by 2008, support had all but dissipated. However, Bush's foreign policy was not the only problem; 2008 brought about one of the worse global financial crises in history. Both the automobile manufacturing and banking industries required massive financial bailouts to remain solvent and unemployment rose at an alarming rate. The resulting unpopularity of the Bush presidency paved the way for the 2008 election to be framed as a continuation of the faulty status quo or a vote for change.

Obama capitalized on the public disapproval of the Bush administration by campaigning on a slogan of "Change." Releasing *The Blueprint for Change: Obama and Biden's Plan for America*, Obama's campaign promoted the 2008 election as a referendum on the business as usual politics of the Bush administration (Obama for America, 2008). The changes in policy were not necessarily directed at Republican nominee John McCain's policies as much as they mark significant departures from Bush administration's politics of secrecy. In calling for change, Obama utilized a rhetoric of transparency that articulated civic engagement, democratic values, good citizenship, and

openness associated with being an American. The joining of transparency with good citizenship worked to establish and implement government 2.0 and infusing data as an essential regulatory mechanism of governance.

This chapter follows the Obama administration's circulation of transparency rhetoric and the promotion of government 2.0. Specifically, this chapter takes up how discourses of transparency are deployed to strategically intensify the manner in which the U.S. conducted its war on terror. First, I examine how Obama's campaign utilized American exceptionalist rhetoric to encourage other governments to be open and transparent. Second, this chapter explores how, when faced with public controversy regarding government surveillance and other abuses of the war on terror, Obama redirects criticism towards the previous administration. Third, the chapter tracks how Obama deployed the state of exception to rationalize citizens' participation in intelligence gathering by organizations such as the CIA and NSA. Fourth, the chapter maps how Obama strategically modified the way in which the U.S. engaged in intelligence gathering and warfighting to be more in line with the shift to personalization and government 2.0 by articulating the war on terror through the logic of endo-colonization. This logic redefined the enemy as domestic radicalized citizens instead of external non-citizen threats, which is a significant shift from the previous administration. Finally, the chapter follows the transparency and 2.0 discourse as it was redeployed in *Inspire* magazine, personal interviews, and recruiting propaganda. Al Qaeda terrorists drew upon transparency and 2.0 rhetoric when criticizing the US for promoting secrecy and recruiting followers to join their cause. This analysis demonstrates how both al Qaeda

and the U.S. government relied on transparency rhetoric that interpellated people to identify with specific civic and religious ideologies and subjectivities.

In order to map how President Obama's surveillance and war rhetoric intensified during his presidency, this chapter begins by charting the Obama campaign's rhetoric and early public addresses regarding the importance of transparency. Next, the chapter examines the elimination of Osama bin Laden as a pivotal moment in the redirection of the war on terror away from an external enemy and towards domestic radicalization. To further explain this argument, the chapter explores the public speeches and legal documents that justified the lethal operation against American citizen Anwar al-Awlaki. In a deeper examination of the justification to use force rather than criminal sanctions against domestic radicalized citizens, the chapter analyzes the text of Senator Rand Paul's filibuster of John Brennan's CIA nomination, several speeches about domestic radicalization after the Boston Marathon bombing, and President Obama's May 23rd speech in which he officially defined the primary enemy to the U.S. as homegrown extremists. Finally, this chapter takes up the public controversy about Edward Snowden's disclosure of government surveillance and Obama's response to the leaks to highlight the contradiction that exists between Obama's pledge for transparency and its implementation, especially in regards to national security.

The 2008 presidential campaign and shining light of transparency

If we theorize that the Bush administration operated along a traditional political axis of government 1.0, or representative republicanism that allows elected officials to govern in the name of the people, then Obama campaigned on the promise of

implementing government 2.0 to govern through transparency and collaboration with the people. This promotion of government 2.0 was evidenced by Obama's campaign pledge to be the most open administration in history. If Obama was to become the most transparent administration, according to this reasoning, the previous administrations relied on some degree of secrecy. Taking aim at the Bush administration's use of secrecy through a national security rationale, Obama's campaign championed greater openness in government and called for active collaboration with citizens in the production of policy. In comparison with the Bush administration's secretive war making, Obama pledged to defeat al Qaeda through legal means, end the war in Iraq, and eliminate the ability for the president to hide behind state secrets privilege. While pointing out that former Vice President Dick Cheney used state secrecy to provide corporations such as Halliburton access to government contracts in Iraq and elsewhere, Obama sought to limit corporate influence over government policy (Obama for America, 2008). Additionally, to promote transparency, Obama vowed to make as much policy information as possible available to the public and implored citizens to inform themselves on the issues. If the people disagree with Obama's policies, they were encouraged to voice their opinions on the campaign website so that they might play an active role shaping policies.

According to Obama, change occurred through openness. He expressed this idea through the metaphor of sunlight as the curative for the corruptive darkness of secrecy. Quoting former Supreme Court Justice Louis Brandeis, Obama (2007, Sept. 22) stated:

> …sunlight is the greatest disinfectant. The more people know about how federal laws, rules and regulations are made, and who's making them, the less likely it is that critical decisions will be hijacked by lobbyists and special interests. I think the current administration knows that, too, which

> is why it's been the most defiantly secretive government in modern times. It's time to change that. (para. 38-40)

Two months later, in November, Obama delivered a speech at Google's Mountain View, California headquarters on the benefits of government transparency and the important role that technology and open information plays. Obama explained that technology is a powerful tool that can help bring about an open and democratic society. He contended, "It's no coincidence that one of the most secretive administrations in our history has favored special interests and pursued policies that could not stand up to the sunlight" (Talks at Google, 2007, 9:14-9:32). Later in a town hall meeting in Cape Girardeau, Missouri, Obama (2008, May 13) again calls out the Bush administration for its secrecy, stating: "this whole issue of transparency, sunshine, this has been the most secretive administration in our history. I mean, they won't let you know what's going on on anything" (42:10). The discursive choice to define the previous administration as being shrouded in secrecy worked to frame the Bush administration as undemocratic while it positioned Obama as being a champion of democracy, shining a light so that liberty might prevail.

Obama invoked the metaphor of sunlight in order to note the importance of transparency for a democratic society to thrive; this framed the election as a referendum on the Bush administration in order to save our democracy. Whereas the Bush administration frequently defended national security as being a priori to an open democracy, Obama maintained that transparency was essential for democracy to function and thus was not a value that can be simply sacrificed. Thus, shinning a light on Washington and exposing the secrets to the curative sunlight was Obama's preferred

choice. To cultivate a democratic culture of transparency, Obama advanced a plan to expose the prevalent backdoor deals made by Washington lobbyists. One part of this idea included Obama launching an attack against the secretive practices and special interest politics of the Bush administration, specifically exposing how Vice President Cheney engaged in secret meetings with Halliburton and provides it with no-bid government contracts to rebuild Iraq. In response to the secretive politics of Bush and Cheney, Obama (2007, Sep. 22) vowed to make all legislation publicly available online so that citizens could freely view it before it was signed. Further, citizens were promised transparency regarding government spending in hopes that it might deter lobbyists from seeking large corporate tax breaks and other legislative favors (Obama, 2007, Sep. 22). As far as campaign promises were concerned, Obama intended to become the most transparent president in history.

Exactly a year later, Obama (2008, Sept. 22) advocated for the adoption and transformation of government 2.0. In the name of bringing about change, Obama (2008, Sept. 22) promised that he would "make our government open and transparent so that anyone can ensure that our business is the people's business" (para. 26). To increase transparency, Obama proclaimed he would put an end to pork-barrel spending by making legislation available to the public online. The stated intention for this policy was to encourage active and engaged citizens whom are informed on political issues and serve as a bulwark against covert corporate influence through lobbyists and special interest groups. Thus, to help inform the public, Obama campaigned on creating a database that exposed the connections between lobbyists and members of congress (Sweet, 2007). As

Obama (2008, Sept. 22) efficiently summarized the point of this policy, there should be "[n]o more secrecy" (para. 26).

Obama's transparency campaign manifested itself in the Obama-Biden plan. This plan focused on exposing the corrupting influence of lobbying through actions such as: encouraging Americans to engage the government again; exposing federal earmarks, contracts, and tax breaks; freeing the executive branch from special interest influence; and spending taxpayer money wisely. Part of the pledge to use taxpayer funds more appropriately was to increase protections for whistleblowers of government corruption. Within the rhetoric of the Obama-Biden plan, whistleblowers were cast as engaging in courageous and patriotic acts that saved lives and valuable taxpayer dollars. For example, the Office of the President-Elect stated, "Obama will strengthen whistleblower laws to protect federal workers who expose waste, fraud, and abuse of authority in government" (para. 21). This was quite a prelude for a president who would be later confronted with one of the largest whistleblowing controversies in U.S history.

Obama's transparency rhetoric earned him the support of Tim O'Reilly, an online publisher and early proponent of Web 2.0 and government 2.0, who began publishing articles on his tech blog encouraging people to vote for Obama. O'Reilly (2008, Oct 29) proclaimed that Obama was the best presidential candidate for a transitioning into the government 2.0 era. According to O'Reilly, Obama's campaign demonstrated the candidate's ability to use technology to interact with citizens as well as provide a platform for them to voice their opinions and help shape policy. Regarding the war on terror, O'Reilly (2008, Oct 29) claimed that Obama's suggestions marked a decisive shift

from the Bush administration approach. Rather than participate in secrecy through the theater of national security discourse and expanded presidential power, Obama represented a candidate of change who might treat terrorists like Internet "griefers" and respond with a military strategy adopted from the Internet adage "do not feed the trolls."

When President Obama first took office in 2008, he begins to implement the Open Government Initiative. In his first full day of office, he speaks out against Washington's secretive culture. Obama declared an end to the era where "if there was a defensible argument for not disclosing something to the American people, then it should not be disclosed" (WH, OPS, 2009, January 21, para. 12). The President instead suggested that, "transparency and the rule of law will be the touchstones of this presidency" (WH, OPS, 2009, January 21, para. 15). In order to encourage the American people to directly participate in the act of governing, Obama released a memorandum entitled "Transparency and Open Government" (Executive Office of the President, 2009). The memo advanced transparency rhetoric in order to promote and instill the practices of government 2.0. Specifically, the memo called for the government to be open so that it could be held accountable by its citizens. Additionally, it advised the government to be made available so that citizens could contribute to policymaking. Finally, it demanded that the government be collaborative, so that agencies, citizens, and organizations could all directly communicate and cooperate in the governing process. The White House website included a Sunset Clause that made legislation, regulations, and policies available for public viewing while it also served as a site where citizens could provide feedback in the policy making process. Forums for citizens to provide their ideas for

policies and participate in brainstorming, discussing, and drafting legislation were also available on the website (Lee, 2009).

Nine days before taking office, President-elect Obama appeared on *This Week with George Stephanopoulos* to conduct an interview over a range of topics regarding his upcoming presidency. Several of the questions pertained to intelligence gathering and national security and Obama's responses provided a glimpse into how he was going to deal with the issues moving forward. For example, Stephanopoulos asks Obama if he believed that Americans were safer or more insecure than was believed during the campaign because of the national security updates that presidential candidates received. After clarifying that confidential information could not be revealed, Obama ambiguously responded that while progress has been made in regards to our information gathering and predictive capacity, the threat posed by individuals willing to commit acts of terror remained a reality (Stephanopoulos and Obama, 2009).

The response provided an opening for Stephanopoulos to play a clip from Cheney offering Obama advice on how to deal with national security when taking office. In the excerpt, Cheney stated:

> Before you start to implement your campaign rhetoric you need to sit down and find out precisely what it is we did and how we did it. Because it is going to be vital to keeping the nation safe and secure in the years ahead and it would be a tragedy if they threw over those policies simply because they've campaigned against them. (Stephanopoulos and Obama, 2009, para. 118)

Obama retorted that he completely agreed that his administration should acquire as much information about national security policy as possible rather than enforcing mere campaign rhetoric; yet, he argued that he had collected information about and disagreed

with several policies of the previous administration. Of those policies, Obama most strongly objected to the use of enhanced interrogation and practices like waterboarding, which Obama considered torture. As Obama notes, "it is possible for us to keep the American people safe while still adhering to our core values and ideals" (Stephanopoulos and Obama, 2009, para. 125). Despite making this argument, Obama's rhetoric changed sharply in discussing whether national security organizations committed crimes against America. When Stephanopoulos inquired if Obama would investigate the Bush administration for illegal wiretapping of American citizens or for war crimes, such as the use of illegal torture techniques, Obama declared, "we need to look forward as opposed to looking backwards" (Stephanopoulos and Obama, 2009, para. 131).

Given Obama's sustained criticism of the Bush administration's war on terror tactics, this seemed like a rather surprising response; however, it was not that shocking. Relying on the logic that the exception proves the rule, Obama maintained a biopolitical rhetorical defense of national security in which exceptional individuals operate outside the law so that they can best secure the American people from danger. Because the Attorney General is the people's lawyer, Obama argued, it would not be right for the people to prosecute those who were working diligently to keep them safe, even if it meant that these exceptional people undermined basic constitutional freedoms. Obama's seemingly innocuous statement however revealed that his transparency rhetoric was an intensification and inversion of the democratic myth of open government and private citizens. For example, the exceptional employees working for national security agencies such as the CIA and NSA were allowed to render citizens transparent through mass

surveillance in order to identify and apprehend or eliminate potential terrorists. Meanwhile, these very individuals who were conducting the surveillance were shielded from public view and were not held accountable to the people. Instead, the public was told that it should not look backwards; it should look to the future and whatever it might entail.

Once President Obama articulated together his rhetoric of transparency with a logic of exception, he combined this discourse with a rhetoric of American exceptionalism. In November 2009, the President travelled to Shanghai to deliver a town hall style meeting with a group of students, some of whom were physically present and others who were participating online (WH, OPS, 2009, November 16). He delivered a short address and then participated in a question and answer session with students. The speech discussed the importance of economic and international relations between the People's Republic of China and the United States and a brief discussion about universal human rights. Some of the questions that President Obama faced afterward included issues regarding China's firewall, China's hosting of the World's Fair, and his winning the Nobel Prize. Many of the questions, however, were about transparency and the values of a digitally open society.

The promotion of openness was quite complicated given the context in which an American president was speaking to an audience whose government was not only censoring coverage of President Obama's speech but also tightly restricting use of the Internet. Despite the regulated nature of China's firewall, the President maintained that open access to information and active political participation were universal human rights

that should exist in any country, whether it was the China or the United States (WH, OPS, 2009, November 16). One reporter mentioned the Chinese firewall and asked if people should be able to use Twitter freely (WH, OPS, 2009, November 16). President Obama responded by calling for open and free flowing information. He declared himself to be a supporter of "non-censorship" by saying, "I think that the more freely information flows, the stronger the society becomes, because then citizens of countries around the world can hold their own governments accountable. They can begin to think for themselves (WH, OPS 2009, November 16, para. 80). Therefore, the President framed transparency as a core democratic value as it provides an avenue in which the people can hold those in power accountable. According to President Obama, citizens are able to participate and mobilize easier if they are able to access and share information.

The invocation for openness during the President's town hall worked as an exceptionalist trope that privileged American capitalist values. While U.S. politicians have chastised China for human rights abuses, President Obama expanded this criticism to include censoring of the Internet. Transparency becomes part of the exceptionalist belief that oppression and tyranny cannot withstand the sunlight provided by openness. This was exceptionalist because the rhetorical promotions of democracy, openness, and transparency were leveraged against nations that Obama encouraged to become more democratic. Yet, the President was not encouraging or pressuring the Chinese government to become more democratic. Instead, by accepting that China had different cultural values regarding censorship and human rights, President Obama in effect positions America as open and tolerant America in comparison. Rather than serve

democratic ends, the trope of openness was promoted to encourage the Chinese people and government to be transparent in order to bolster economic globalization. The President argued that open access to information in a globalized society expedited business opportunities. These economic relations were credited by him with creating a more open and peaceful society. As evidence of this point, he pointed to the increased cross-strait relations between China and Taiwan. Without having to choose a side, President Obama was able to suggest that increased trade between China and Taiwan had helped to bring a peaceful solution to an otherwise volatile situation.

Despite the President's staunch defense of online transparency for the purposes of exposing human rights abuses when he was in China, his stance changed in 2010 when WikiLeaks released classified documents about the U.S. war in Iraq and the war on terror. The WikiLeaks disclosure required a discursive reconfiguration regarding how to advocate for transparency while also arguing for the need to classify and keep vital national security information safe. On July 27, 2010, President Obama delivered remarks that rhetorically framed his administration's plans for balance these issues. In this speech, he expressed concern that the disclosure of information could endanger individuals in the field. However, the WikiLeaks revelations did not present a major national security dilemma because the information that was leaked was already publicly available (WH, OPS, 2010, July 27). The President's address was then supplemented by National Security Advisor General James Jones, who indicated that the military abuses reflected in the leaks were merely an extension of the Bush administration's policies. Jones' timeline for the WikiLeaks documents covered the period from January 2004 to

December 2009, which was theoretically Bush's second term in office. This deflection allowed the Obama administration to maintain its credibility on transparency while blaming the problems on the previous administration. This rhetorical strategy of scapegoating the previous administration was used again when the Obama administration pointed to December 1, 2009, when a new strategy for dealing with Afghanistan and Pakistan was announced. The strategy marked a strategic shift in the promotion of economic development and collaboration with Pakistan to fight violent extremism.

Killing Bin Laden and reestablishing a threat

The call for collaboration with Pakistan became more urgent in 2011 when the U.S. located bin Laden living in an affluent suburb inside of the country. On May 1, President Obama, without notifying the Pakistani government, ordered a small military team to invade bin Laden's compound to capture or kill al Qaeda's leader. The ability to track down and kill bin Laden was enabled by a strategic shift in how the U.S. conducted the war on terror. While Obama campaigned on withdrawing ground forces from Afghanistan and Iraq, he compensated for this reduction in forces by increasing his reliance on aerial drone strikes, "smart" bombs, and special force operations. The intensified warfighting strategy that allowed the U.S. to locate and eliminate bin Laden demonstrated a significant shift away from large-scale troop deployment to specialized missions to eliminate designated targets. The rhetoric surrounding the death of bin Laden exposes how the Obama administration intensified and reconstituted the surveillance and warfighting strategies of the Bush administration. Due in part to the success in shifting

strategies, Obama faced the challenge of identifying a threat and enemy that had lost its organizational and symbolic figurehead.

On May 2, 2016 at 12:03 a.m., Tommy Vietor, spokesperson for the National Security Council, held a press briefing regarding the successful military mission to eliminate bin Laden. After quickly addressing the press, he introduced several unnamed senior administration officials who took turns providing information about the operation. The first official began his update with a description of how Obama intensified intelligence gathering and warfighting strategies, stating:

> From the outset of the administration, the President has placed the highest priority in protecting the nation from the threat of terrorism. In line with this, we have pursued an intensified, targeted, and global effort to degrade and defeat al Qaeda. Included in this effort has been a relentless set of steps that we've taken to locate and bring Osama bin Laden to justice. Indeed, in the earliest days of the administration, the President formally instructed the intelligence community and his counterterrorism advisors to make the pursuit of Osama bin Laden, as the leader of al Qaeda, as a top priority. (WH, OPS, 2011, May 2, para. 2)

Obama verified that shortly after taking office, he ordered CIA director Leon Panetta to make capturing or killing bin Laden the top priority in the war against al Qaeda (Phillips, 2011).

The decision to locate and eliminate bin Laden was very popular. Yet, the ability to successfully execute the plan reflected the intensification of Obama's military strategy and the nation's attitudes towards lethal combat operations. Bin Laden had been on the FBI's most wanted list since 1999. Presidents Clinton and Bush 44 were unsuccessful in capturing or killing bin Laden. After all, how does one find an elusive enemy that was known to hide in caves, remote deserts, rugged mountains, or secret military compounds?

The U.S. Senate Committee on Foreign Relations, led by Senator John Kerry, conducted a study determining that in December 2001, bin Laden was located in the Afghanistan's hazardous mountainous terrain of Tora Bora (U.S. Senate. Committee on Foreign Relations, 2009). The bombings of the area were so intense that even bin Laden expected that he was going to die as he produced his last will and testament on December 14. However, there were very few American soldiers on the ground in Tora Bora and Secretary of State Donald Rumsfeld denied requests for military reinforcements to wage a ground assault or to guard the mountain paths leading to Pakistan. This decision allowed bin Laden and his security team to walk into Pakistan completely unharmed. As a result, bin Laden eluded U.S. forces until the Obama administration located him in Attobad, Pakistan.

President Obama's ability to track, locate, and kill bin Laden in an affluent suburb in Pakistan was credited to the CIA, NGA, and NSA's intelligence work (WH, OPS, 2011, May 2). According to a senior administration official, the CIA used information gathered from detainees to flag key individuals who were providing direct support to bin Laden (WH, OPS, 2011, May 2). One specific individual was identified as a trusted courier who was living with and protecting bin Laden. Following the courier allowed the CIA to focus on a specific compound, described by a senior administration official as, "custom built to hide someone of significance" (WH, OPS, 2011, May 2). By analyzing the association created by the capture of Khalid Sheikh Mohammed and Abu faraj al-Libbi, the courier's behavior and personal and familial background, and the elaborate security and the predicted expectations of bin Laden's hideout, the government created a

statistical calculation of likelihood that determined that they had found bin Laden. The statistical calculations determining bin Laden's whereabouts resulted in the deployment of a small U.S. team who successfully infiltrated the compound and killed al Qaeda's top leader.

Bin Laden's death ushered in a new rhetorical paradigm for President Obama, solidifying the intensification of government surveillance and warfighting. Using statistical calculations and personalized targeting generated from kill lists such as the disposition matrix, a small group of American forces went into a sovereign nation that the U.S. had not declared war against and eliminated the figurehead and primary signifier of the terrorist enemy. By altering its warfighting strategy, Obama was able to finally collect on Bush's frontier bounty of "Wanted: Dead or Alive." Yet, the elimination of bin Laden did not signify the end of the war on terror as much as it served as a marker for the transformation of the war on terror into an endo-colonization war against the people it was meant to protect. Killing bin Laden demonstrated that the U.S. was capable of engaging in a globalized conflict and that it did not matter where terrorists was physically located because they could be tracked, captured, and killed anywhere. This complete control over the globe represents the logic of endo-colonization: once the binary of external/internal was collapsed, the government turned its colonizing gaze inward and protected itself against internal threats.

With the death of bin Laden, the Obama administration created a new rhetorical justification for continuing the never-ending war on terror. For instance, on May 2, 2011, Obama delivered the news of bin Laden's death to the American people. Obama used the

speech to both celebrate the success and hard work of U.S. intelligence and to warn the public against the ubiquitous threat of terrorism. Obama stated:

> For over two decades, bin Laden has been al Qaeda's leader and symbol, and has continued to plot attacks against our country and our friends and allies. The death of bin Laden marks the most significant achievement to date in our nation's effort to defeat al Qaeda. Yet his death does not mark the end of our effort. There's no doubt that al Qaeda will continue to pursue attacks against us. We must –- and we will -- remain vigilant at home and abroad. (WH, OPS, 2011, May 2, para. 11-12)

These sentiments that the war on terror has not ended with bin Laden's death were then echoed by an Obama administration senior official who warned the press and, by extension, the American public about the increased terrorist threat to the homeland and to American citizens abroad (WH, OPS, 2011, May 2). Noting that bin Laden's death was the single greatest victory of the war on terror and that al Qaeda would not be able to recover from this loss, the official stressed to the public that it was still very much at risk from an insidious terror threat (WH, OPS, 2011, May 2). Since the government could no longer point to a visible external threat to justify the war, the Obama administration began to rhetorically frame the threat as something that could occur anywhere and at any time by radicalized individuals rather than groups. Due to the molecular nature by which terrorists were dispersed globally, leaders were forced to rely on new rhetorical techniques to justify and continue the war on terror. In his study of biopolitics and governmentality, Foucault (1988) diagnosed that the split between using the rule of law to control internal threats and deploying the military to control external threats had merged in a neo-liberal order. This system worked by combining both the rule of law and non-military bureaucratic agencies to control both internal and external threats. As

we see in the emergence of organizations such as the CIA, FBI, and NSA overseeing both internal and external security and sharing information and responsibilities as overseen by the Department of Homeland Security in the post-9/11 environment, this collapse of the distinction between external and internal security was already at play.

Additionally, Paul Virilio provides a supplement to Foucault's theory of governmentality to explore this shift in modern warfare discourse. In his ruminations about the nature of colonization and war, Virilio (2000) argued that traditional notions of civil war, colonialism, and warfare were outdated and meaningless as both colonization and warfare no longer targeted external populations but instead turned inwards against a state's own population. Rather than wage a traditional war that claimed Afghanistan for the U.S., both Presidents Bush 44 and Obama increased surveillance and similar security measures to monitor all potential threats, external or internal. This new mode of boundless warfare no longer sought reconciliation; instead, it wanted to completely vanquish those who disrupted the harmony of the homeostatic security state (Virilio, 2000). This notion of warfare explains the political exigency of the U.S. war on terror after the death of bin Laden and helps explain the transition towards the ever increasing reliance on drone warfare to target and vanquish radicalized American citizens.

As a result, the killing of bin Laden marked a rhetorical moment in which the Obama administration used endo-colonizing discourse to redefine the war on terror. While the Bush administration defined the war on terror as a boundless global conflict to search out and eliminate external al Qaeda and affiliates threats, Obama intensified this discourse by finding and killing the group's leader and numerous other key figures within

the organization. The elimination of major al Qaeda leaders resulted in the materialization of endo-colonization where the external threat to the U.S. had been minimized if not vanquished. As a result, President Obama redefined the nature of the threat and the enemy away from an external threat and redirected the nation's energy and focus inwards. Now, the new threat was a dangerous ideology capable of infiltrating the psyche of citizens, transforming them into radicalized homegrown extremists.

Domestic radicalization, endo-colonization, and the targeting of American citizens

Obama used presidential definition to rhetorically shift the focus of the war on terror away from external threats and towards radicalized domestic extremism and homegrown terrorists. This part of the chapter examines this rhetorical shift in regards to presidential definition of radicalized extremism and homegrown terrorists. First, the section follows the rhetoric surrounding Anwar al-Awlaki, an American born cleric who relocated to Lebanon where he spoke to numerous individuals who carried out terrorist attacks and wrote for the al Qaeda magazine *Inspire*. Second, it examines the public discourse surrounding the lethal drone strikes killing al-Awlaki, his son Abdulrahman, and American born Samir Kahn. Specifically, this section of the chapter follows Ron Paul's filibuster of John Brennen's nomination to the CIA as he protested the possibility of the use of drones on American soil. Third, this section analyzes the rhetoric that surrounded the Boston Marathon bombing. This sub-section examines how terrorists appropriated government 2.0 and transparency rhetoric to rationalize attacks against Americans and how this attack became a pinnacle event in establishing the threat of domestic radicalization as the primary focus of the war on terror. Finally, this section

assesses President Obama's May 23, 2013 speech which redefined the war on terror, defining homegrown extremists as the top concern of national security and rationalizing lethal drone operations as essential anti-terrorism operations.

Anwar al-Awlaki. Al-Awlaki was the first American citizen to be killed by a lethal drone strike. Al-Awlaki was targeted not because he was a soldier carrying out combat operations. Indeed, it was unlikely that he killed anyone. Rather, al-Awlaki was killed because he was a radical cleric who materially supported terrorism by using composition and speech to persuade others to join al Qaeda. He was accused of using persuasion to encourage the murder of innocent people around the world and was allegedly responsible for planning the attempted Christmas attack by Umar Farouk Abdulmutallab, the "Underwear Bomber," and another failed attempt to blow up a U.S. cargo plane (WH, OPS, 2011, September 30). On September 30, 2011, the President addressed the nation to applaud the U.S. intelligence community's success in targeting and killing another high ranking al Qaeda member. What was not mentioned in Obama's speech was that Anwar is also an American citizen and the first citizen to ever be officially targeted for a drone strike. While Chapter 2 discussed how Bush killed an American citizen in the first U.S. lethal drone strike, the primary difference between the strikes on Derwish and al-Awlaki was that the former was collateral damage while the later was an intended target. Indeed, the Bush administration claimed that it never approved a lethal operation that specifically targeted an American citizen (Leonard, 2010). However, the Obama administration changed the course of the war on terror by adding Anwar al-Awlaki to the CIA kill list (Miller, 2010). This move meant that al-

Awlaki could be targeted and killed by not only the military but also lethal CIA operations.

To justify the use of lethal force against American citizens, the Obama administration needed to establish the privileges of citizenship as contingent on whether citizens engaged in acceptable performances. The President's rhetoric tactics to rationalize government kill lists and targeted lethal operations deployed legal rhetoric and presidential definition to redefine citizens as potential enemies, militants, or terrorists. In other words, President Obama's legal authority to target and kill American citizens required a new legal interpretation and precedent that circumvented traditional legal understandings of due process rights. The new legal interpretation authorizing kill lists and drone strikes became more persuasive in the legal system because the President was able to use the presidential authority to define the threats against the country. In this case, the potential threat was American citizens. Within this discourse, citizens relinquished their privileges and rights afforded by citizenship when they performed in ways defined as threatening or unacceptable by the Administration. Because the executive branch was able to authorize citizens' deaths, there was a finality about the President's determination; the dead could not legally contest their guilt or the validity of information that placed them on kill lists.

On February 4, 2013, NBC News released a classified White Paper from the Department of Justice that "set forth a legal framework for considering the circumstances which the U.S. government could use lethal force in a foreign country outside the area of active hostilities against a U.S. citizen who is a senior operational leader of al-Qaeda or

an associated force of al-Qaeda—that is, an al-Qaeda leader actively engaged in planning operations to kill Americans" (DOJ, 2011, Nov. 8, para. 1). It is obvious that the White Paper was not the minimum requirements for killing American citizens; instead, it was specifically written, albeit not without specific reference, for the intended purpose of legally rationalizing the drone strikes against Anwar al-Awlaki. According to the White Paper, there are three conditions that had be met in order for the U.S. to carry out a lethal operation: (1) a high-level government official had determined that the targeted individual poses an imminent threat; (2) capture was infeasible; and (3) the operation was carried out in a manner consistent with the laws of war (DOJ, 2011, Nov. 8).

Despite outlining these legal parameters, through the DOJ White Paper, the legal conditions to conduct lethal operations were drastically redefined under the Obama administration. For instance, the White Paper legally justified the government's ability to conduct a lethal operation inside a country without first declaring war against that nation. Further, the lethal operation was not even considered a violation of national sovereignty. In this case, the U.S. either needs the consent of the host nation or it can determine that the host nation is unable or unwilling to suppress the threat and thus choose to unilaterally intervene (DOJ, 2011, Nov. 8). Additionally, the Authorization for Use of Military Force (AUMF) did not set any geographic limitations for operations and, as a result, the U.S. government could interpret this to mean that force was not restricted only to "hot" battlefields such as Afghanistan or Iraq.

While the legal parameters for where lethal operations could take place was broadened, the discursive boundaries for what constituted an "imminent" threat against

the U.S. was substantially expanded. As the White Paper explained, the U.S. did not need "clear evidence that a specific attack on U.S. persons and interests will take place in the immediate future" (DOJ, 2011, p. 7). Instead, because the U.S. perceived al Qaeda as constantly engaged in planning future attacks, the government's was justified to preemptive kill potential terrorist subjects for almost any reason in any location. Additionally, the government rationalized the need for expansive preemptive drone strike authority through a rhetoric of self-defense and legal necessity to preserve the lives of American citizens. For example, the White Paper argued that, within the AUMF, the President's constitutional responsibility to protect the nation and the inherent right to national self-defense is recognized in international law and provided the legal authority to use whatever means necessary to fight al Qaeda and its affiliates (DOJ, 2011, Nov. 8). Moreover, if the U.S. believed that an al-Qaeda operational leader was involved in planning an attack and there was no evidence that they had renounced or abandoned such activities, the government had rhetorically labeled those persons as an imminent threat (DOJ, 2011, Nov. 8).

While the government insisted that its preferred method of dealing with terrorists was to capture them, the DOJ White Paper introduced several exceptions to this policy that broaden the government's permission to kill terrorists. For example, a person could be killed if s/he cannot be captured during an appropriate window of opportunity. Furthermore, if the host country does not consent to a capture operation, the U.S. could eliminate the threat unilaterally. Additionally, if a capture operation presented undue risk to U.S. personnel, the government could use a drone strike instead of putting troops in

harm's way. Consequently, while the Obama administration claimed publicly that its top priority was to capture terrorists for information gathering purposes, the rhetorical constitution of legal concepts such as imminent danger and legal permission to kill help explain how the Obama administration intensified the war on terror by moving away from capturing enemies and towards terminating them, even if they were American citizens.

While the original DOJ White Paper did not specifically mention al-Awlaki, the American Civil Liberties Union (ACLU) was able to get the government to release a second DOJ memorandum that directly addressed the constitutional basis for the government targeting and killing of al-Awlaki. The document noted that al-Awlaki was a high ranking senior member of al-Qaeda who worked to recruit individuals to join the organization (DOJ, 2010). Although the memorandum was highly redacted, it stated that it was reasonable to assume that al-Awlaki posed an imminent and continued threat to the United States and thus was not protected by his citizenship status.

This represented an important shift in the rhetorical justification of the war on terror. The argument presented by the DOJ (2010) was that "public authority" justified the attack. Public authority justification means that criminal prohibitions do not apply to governmental actors who were acting based on the authority of the people. By invoking this legal authority, Obama was relying on the legal exception that it was permissible to engage in actions that were prohibited so long as one was doing it in the name of American people. For instance, police officers can use lethal force to apprehend dangerous suspects or detain or imprison them against their will. While the laws

regarding police force were outlined by specific state laws, there was no federal law which defined the public authority justification to use drone strikes (DOJ, 2010). Thus, the DOJ relied on the federal definition of murder, which applies to "unlawful killing[s]." In order to justify targeting American citizens through drone strikes the government needed to provide evidence that the acts were lawful killings. To prove this point, the DOJ argued that, because of the public authority justification, lethal actions against citizens were allowable and lawful (DOJ, 2010). Thus, the memorandum argued that either the CIA or DOD could legally target and kill al-Awlaki as part of the lawful conduct of war and that their actions were permissible because they were encompassed under the public authority justification (DOJ, 2010).

The killing of Anwar al-Awlaki revealed how the government constituted the threat posed by rhetoric's materiality. For instance, in the case of al-Awlaki, the Obama administration did not demonstrate that al-Awlaki took up arms against the U. S. Additionally, they did not demonstrate that he physically participated in any form of confrontation with the U.S. What we do know is that he was a radical cleric, a preacher who communicated with Umar Farouk Abdulmutallab—the "Underwear Bomber" and the Fort Hood shooter, Nidal Hasan, and three of the 9/11 hijackers. Further, he wrote articles for al-Qaeda's magazine, *Inspire*. The government did not charge him with a crime nor did it release any evidence that al-Awlaki planned any attacks (Miller, 2010). Instead, it was al-Awlaki's speech—publicly defending terrorist attacks and the violence committed by people whom which he communicated—that defined him as constituting a material threat to the U.S. As Chapter 1 noted, the Supreme Court had already ruled that

communications with terrorists can be criminalized as providing material support for terrorism. Absent the government providing any evidence that a1-Awlaki was part of any plans to carry out attacks of terrorism, the public could infer that the communication with and radical preaching to terrorists were factors lead to the political decision to target and kill him. Within this framing, speech and actions cannot be legally separated and al-Awlaki's discourse served as material proof that he was active involved in hostilities against the U.S. Because of his rhetoric, a1-Awlaki could be lawfully targeted and killed without having to be charged with a crime.

Ron Paul's filibuster and domestic drones. The legal justification for targeting and killing American citizens articulated by the DOJ White Paper was a politicized issue during John Brennan's Senate nomination to the director of the CIA. Senator Rand Paul sent a letter to Brennan on February 20, 2013 asking if the president had the power to use a drone strike against a citizen on U.S. soil. Attorney General Eric Holder responded, noting that while purely hypothetical, "it is possible to imagine an extraordinary circumstance in which it would be necessary and appropriate under the Constitution and applicable laws of the United States for the President to authorize the military to use lethal force within the territory of the United States" (Office of the Attorney General, 2013, March 4, para. 3).

The ambiguity of the answer led Senator Ted Cruz to question Holder on March 6, 2013 at 9:30 a.m. regarding the constitutional basis for killing an American citizen if they did not pose an imminent threat and were in U.S. territory. Senator Cruz questioned Holder using several hypothetical scenarios to which Holder denied the premise of the

question, responding that he did not think that it would be appropriate to use that kind of lethal force because law enforcement was already capable of dealing with domestic threats (Federal News Service, 2013 March 6). After Cruz rephrased his question several times, Holder finally clarified that he did not think that it would be constitutional for the government to use lethal force against American citizens who do not pose an imminent threat on American soil (Federal News Service, 2013 March 6). While Cruz announced that he was satisfied with this answer, he renounced the legal gymnastics Holder used before answering the question definitively.

At 11:47 a.m. on the same day, Senator Paul began what would be a nearly 24-hour filibuster of Brennan's confirmation. The purpose of the filibuster was not necessarily against Brennan's qualification, but instead it served as a political stand against the legal ambiguity surrounding the use of lethal operations against American citizens. As Paul stated:

> I will speak as long as it takes until the alarm is sounded from coast to coast that our Constitution is important, that your rights to trial by jury are precious, that no American should be killed by a drone on American soil without first being charged with a crime, without first being found to be guilty by a court. That Americans could be killed in a cafe in San Francisco or in a restaurant in Houston or at their home in Bowling Green, KY, is an abomination. (U.S. Senate, 2013, P. S1150)

Paul then equated the use of use of lethal drone operations against American citizens to the fictional world in *Alice in Wonderland*, stating:

> They say Lewis Carroll is fiction; Alice never fell down a rabbit hole, and the White Queen's caustic judgments are not really a threat to your security. Or has America the beautiful become Alice's Wonderland?
> ``No, no!" said the Queen. ``Sentence first--verdict afterwards."
> ``Stuff and nonsense!" Alice said loudly. ``The idea of having the sentence first."

> ``Hold your tongue!" said the Queen, turning purple.
> ``I won't!" said Alice.
> [``Release the drones,"] said the Queen, as she shouted at the top of her voice." (U.S. Senate, 2013. P. S1150)

The filibuster provided Paul with a platform to speak up against the endo-colonizing logic of Obama's drone policy that erased the division between domestic/foreign, friend/enemy, and inside/outside. With his filibuster speeches, Paul drew attention to the problem that the war on terror, as justified by the Obama administration, has no legal, temporal, or geographical limitations. While these concerns were not exclusive to just the Obama administration's policies, Paul did highlight how these practices intensified under Obama's tenure as president.

Paul's filibuster could have marked an important protest against the discourse and logic of government 2.0 as it was applied to the war on terror in general and lethal drone strikes in particular. The fact that Brennan was the target for opposition to the drone policy was rather significant given his centrality to government 2.0 application to the war. As Chapter 2 noted, Brennan was the mastermind behind the Disposition Matrix and the presidential kill list. Further, the hearing was about the appropriateness of Brennan's appointment as head of the CIA, the very organization carrying out the majority of drone strikes. As Paul pointed out during his filibuster, Brennan was asked if there were any geographic limitations to the drone program and he responded that there were not (U.S. Senate, 2013, March 6). So while Brennan might not be the person that Paul was directly speaking out against, his nomination to head the CIA signified the Obama administration's commitment to government 2.0 that was being used to conduct the war on terror.

Yet, despite the seemingly stringent stance Paul took regarding the use of drone strikes against American citizens, the Kentucky Senator railed against a straw person scenario while reaffirming status quo policies. Paul clarified that he was not against killing an American citizen if they were a known terrorist on American soil so long as they pose an imminent threat. The filibuster was an attempt to get an admission from the President that the government would not use drones against citizens on American soil who posed no immediate threat. Paul did not take a stance against the ever-broadening definition of imminent threat; instead, he declared that citizens who are committing crimes can be met with lethal force. For instance, after the Boston Marathon bombing, Paul was quoted as saying, ""I've never argued against any technology being used when you have an imminent threat, an active crime going on," he continues, "if someone comes out of a liquor store with a weapon and fifty dollars in cash … I don't care if a drone kills him or a policeman kills him" (quoted in Koebler, 2013).

Ultimately, the debate surrounding the use of drone strikes to kill American citizens was framed and resolved through transparency rhetoric. For example, Senator Cruz's questioning of Brennan and Senator Paul's filibuster only operated as criticisms of the clandestine nature of the Obama administration's drone policies, not the actual justification for the strikes. As soon as Brennan, Holder, or Obama openly addressed the subject, the public debate to a large extent ceased. This exemplified the persuasive force of transparency rhetoric. In this instance, the Obama administration provided a few clarifying details about how the U.S. conducted lethal drone operations and the public debate was quashed. Simply by being more open than the previous administration about

its military and surveillance programs, the Obama administration's programs such as CIA drone strikes, the disposition matrix, government kill lists, and signature strikes were accepted and legitimized without significant public debate. It did not matter that the government has created a personalized killing protocol with little oversight because at least the legislators and the public knew about it.

However, the use of transparency rhetoric was not unique to the U.S. government. Transparency rhetoric and the logic of government 2.0 was used also by al Qaeda to recruit followers and rationalize acts of terrorism. To understand how this rhetoric was deployed by al Qaeda, this section of the chapter follows the rhetoric circulating around the Boston Marathon bombing. The bombing intensified the call for transparency as law enforcement began to crowdsource for surveillance footage that could help apprehend the perpetrators. Agencies such as the Boston Police Department and the FBI turned to social media sites such as Twitter to communicate with the public. After the attacks, the government and private businesses used the event to call for increased surveillance and the necessity of rendering the public transparent. Meanwhile, the bombing suspects--the Tsarneav brothers—despite not being affiliated with al Qaeda directly were linked to propaganda that was spread through Al Qaeda's *Inspire* magazine. Analysis of this magazine indicates that transparency and government 2.0 were tropes deployed to encourage acts of terrorism such as performed by the Tsarneavs.

Boston marathon bombing. Almost two months after Senator Paul's filibuster, the legal and rhetorical limits to the use of lethal domestic drone strikes were put to the test. On May 15, 2013, the Boston Marathon bombing solidified the endo-colonizing

logic of the war on terror, articulating surveillance and government 2.0 activities like crowdsourcing together with notions of citizenship and drone targeting. Shortly after the bombing, the Boston was put on lock-down. The Boston Police and FBI utilized social media such as Twitter to communicate with citizens and solicit help in identifying and apprehending the perpetrators. The Internet was abuzz as numerous participants shared their personal video footage from their cell phones and other similar devices. The combination of corporate, municipal, and personal surveillance was quickly disseminated to the public who collectively worked as citizen-detectives to identify and locate the bombers.

The crowdsourcing of information and surveillance footage resulted in identifying the Tsarnaev brothers as suspects. Dzhokhar Tsarnaev became a citizen on September 11, 2012. Tamerlan Tsarnaev was a legal permanent resident whom filed for citizenship and was awaiting a decision at the time of the bombing. In 2011, the FBI received notification from a foreign government stating that Tamerlan was a radical follower of Islam and should be investigated (FBI, 2013). As a result, it was ordered to increase surveillance on Tamerlan, checking government databases to "look for such things as derogatory telephone communications, possible use of online sites associated with the promotion of radical activity, associations with other persons of interest, travel history and plans, and education history" (FBI, 2013). The FBI also interviewed both Tamerlan and his family (FBI, 2013). Despite this, the agency was unable to finding anything that could connect Tamerlan to any form of terrorist activity and thus had no reason to prevent him from entering the country.

Before this attack, the issue of conducting drone strikes against citizens on American soil was a very contentious topic and a source of serious political deliberation. However, the Boston bombing quickly changed the nature of the national debate. For example, the general public, Senator Paul, and several other members of congress approved of the use of drone strikes to kill the Tsarnaev brothers (Koebler, 2013). Despite the popularity of using drone strikes in this occasion the discussion of this option failed to account for how the justification to use drones in these instances operate as exceptionalist discourse that is reappropriated by terrorist organizations to recruit more terrorists. The Tsarneav brothers, for instance, were linked to *Inspire* magazine, an al Qaeda magazine that frequently published articles about U.S. drone strikes and made calls for personal jihads against the West. It is believed that this rhetoric from *Inspire* might have influenced the brothers towards radicalization (Rotella, 2013).

The first English issue of *Inspire* was released in 2010. The magazine included an article from American-born Anwar al-Awlaki and was possibly released by another American citizen, Samir Kahn. The first issue included a section entitled, "Open Source Jihad." The concept was defined, according to *Inspire* as, "A resource manual for those who loathe the tyrants; includes bomb making techniques, security measures, guerrilla tactics, weapons training and all other jihad related activities" (AQ Chef, 2010, p. 32). Within this section of the magazine, there was an article entitled, "Make a bomb in the kitchen of your Mom," written by AQ Chef. The article provided step-by-step instructions on how to make a pressure cooker bomb akin to the ones used in the Boston Marathon bombing. The second article in the section taught people how to avoid

government surveillance of communications by using 2.0 technology to encrypt messages.

The *Inspire* article demonstrated how the rhetoric of government 2.0 and the associated tech-savvy communicative subject was capable of materializing through molecular networks. While American politicians evoked government 2.0 and openness rhetoric to invite citizens to become transparent, al Qaeda used it to formulate opaque communications and rhizomatic terrorism. By rhizomatic, I mean a rhetorical framing of terrorism that used 2.0 concepts to promote individual acts of terrorism orchestrated by loosely connected networks of people that exist in disparate global spaces. *Inspire* provided essays that outlined how one could become a rhizomatic terrorist. For instance, articles discussed how to assemble weapons that can commit mass devastation, how to subvert U.S. surveillance in digital communications, and why individual acts of terrorism are important.

The essay about the significance of individual terrorist activities was written by Anwar al-Awlaki and was meant to address an American audience. The thesis of the article was that the U.S. government was wasting billions of dollars fighting a war on terror that cost its opponent very little money in comparison. The American people were encouraged to rethink the war on terror because of how it disrupted their daily lives. Awlaki (2010) conjured nostalgia for the "good old days" when Americans could buy an airplane ticket from a classified advertisement in the local newspaper because there was no security or identification checks required to travel. Moreover, Awlaki discussed how Americans were required to wait in long lines, undergo intense screening, and waste lots

of time and resources on security measures that could not provide absolute security. Not only were the American people not secure, but, according to Awlaki (2010), they were at an extreme disadvantage; they had to sacrifice by submitting to extreme surveillance and paying higher taxes and while corporations and politicians raked in greater profits.

Awlaki contrasted the importance of faith versus nationalism in a confrontational religious rhetoric in order to recruit people to join al Qaeda and commit acts of terrorism. In particular, Awlaki (2010) argued that al Qaeda did not hate Americans because they were American; instead, he insisted that they were against evil acts deployed in the war on terror: "we are against evil, and America as a whole has turned into a nation of evil. What we see from America is the invasion of two Muslim countries, we see Abu Ghraib, Baghram and Guantanamo bay. We see Cruise missiles and cluster bombs, and we have just seen in Yemen the death of 23 children and 17 women" (p. 57). Then Awlaki discussed how he was an American citizen involved in non-violent Islamic activism until the invasion of Afghanistan and Iraq. Yet, when he saw the military aggression taken against Muslims, he could no longer reconcile the tension between living in America and being Muslim. For Awlaki, he was forced to choose religion over country and engage in violent acts of terrorism to protect that faith.

Awlaki exposed what he believed to be the hypocrisy of Obama's transparency rhetoric in the context of how the war on terror was secretively conducted. For example, Awlaki (2010) claimed that this tension ultimately would be the reason why Obama would lose the war on terror. Pointing to Obama's campaign promises about transparency, Awlaki (2010) accused Obama of going to great lengths to secretly cover

up Hasan and the Fort Hood shooting. He also pointed to Yemen as an example of Obama's intensified war on terror, criticizing the President for deciding to engage in a military conflict inside a sovereign Muslim country. In response to these insincere promises of openness, attacks, such as the one conducted by Abdulmutallab's "Underwear Bomb" attack, were in retaliation for the cluster bombs and cruise missiles that killed women and children in Yemen, according to Awlaki (2010). He concluded his article by telling Muslims in the West that America was a land of the Ku Klux Klan, lynching, segregation, and slavery that was heading towards religious discrimination and concentration camps. Thus, Muslims had two choices: "either jijra or jihad. You either leave or you fight" (Awlaki, 2010, p.58). In other words, Muslims were given another ultimatum similar to President Bush's "you're either with us or against us." However, unlike Bush's use of a similar argument regarding international alliances in the war on terror, Awalaki based his "with us or against us" claim in an oppositional religious rhetorical frame.

While it was impossible to know definitively if the Tsarneav brothers were radicalized due to Awlaki's words, it was possible to see the similarities in the explosive devices they used and the *Inspire* instructions for a pressure cooker bomb. There were also similarities between Awlaki's article and the message that Dzhokhar inscribed on the boat he was hiding in to avoid capture. For instance, Dzhokhar wrote:

> I bear witness that there is no God but Allah and that Muhammad is his messenger (hole) r actions came with (hole) a (hole) ssage and that is (hole) ha Illalah. The U.S. Government is killing our innocent civilians but most of you already know that. As a M (hole) I can't stand to see such evil go unpunished, we Muslims are one body, you hurt one you hurt us

> all, well at least that's how Muhammad (pbuh) wanted it to be (hole) ever, the ummah [community of Muslims] is beginning to rise/awa (hole) has awoken the mujahideen ["holy warriors"], know you are fighting men who look into the barrel of your gun and see heaven, now how can you compete with that. We are promised victory and we will surely get it. Now I don't like killing innocent people it is forbidden in Islam but due to said (hole) it is allowed. All credit goes (hole). (Katersky & McPhee, 2015)

While the message was difficult to decipher due to the bullet holes, it was very similar to the rhetoric used by Awlaki, Hasan, and others: The U.S. was at war with Muslims. As such, all Muslims must join together and fight against the perceived injustices committed against other Muslims.

The issue of *Inspire* magazine released before the Boston Marathon bombing contained a series of articles that seemed to further support the terrorist acts taken by the Tsarneavs. For instance, in a question and answer session, Ramzan Ali asked *Inspire* editors about the effectiveness of individual jihads. The editors' response was that individuals were very important because they can choose any number of targets such as businesses, hotels, residences, and other places (*Inspire*, 2013). Further, they argued that the fight should be moved into the enemy's territory in the same way that the U.S. killed Muslims and occupied other countries. The claim was that these attacks would force the enemy to revise its anti-Muslim policies because it served as a form of punishment. Finally, the editors maintained that the attacks were considered important because they scare the public, especially because the attack made it very difficult to identify who executed it (*Inspire*, 2013). Thus, *Inspire* encouraged all Muslims to engage in individual

attacks in order to drain the enemy's economic resources and exhaust and punish the enemy.

The Tsarnaevs seemed to follow the model of individual terrorism advanced by *Inspire.* While the true motives of the Tsarnaevs to plant bombs at the Boston marathon may never be fully known, the charges leveled against the Tsarnaev brothers demonstrated that there was considerable fear about the economic consequences of the attack. There were two charges made against him and they were both concerned primarily with the economic effects of the bombing. First, Dzhokhar was charged with the use of a Weapon of Mass Destruction for his attempt to set off an IED (Genck, 2013). Second, Tasmaev was charged with malicious destruction of property resulting in death (Genck, 2013).

The criminal complaint made against the Tsarnaev brothers also was riddled through with an economic logic. For example, when explaining the charges and offering the evidence that the state possessed, the detailed description of the crime provided by FBI Special Agent Daniel Genck focused very little on the loss of human life or motives of the brothers. Instead, Genck emphasized the economic losses caused by the bombing. For instance, Genck's report began with the claim that the Boston Marathon brings several million dollars to the city (Genck, 2013). Seemingly validating *Inspire's* logic that individual attacks on soft targets like hotels and restaurants can cause severe disruption, the criminal complaint described the millions of dollars that are made by the hotel and restaurant industry because of the marathon. Furthermore, the complaint also noted the economic toll wrought by the explosions on private and public property. For

example, the report lists numerous economic problems that came from the closure of the marathon, the evacuation and closing of businesses near Boylstron Street, and the shutdown of all businesses in the city while the hunt for the suspects was ongoing. Only three sentences in the entire document were written about the loss of life and the toll that the attack wrought on society. Yet, even in each of those sentences, the word "death" also was accompanied by damage to personal property and private business. Ultimately, Genck's rhetoric highlighted the self-fulfilling logic at play in contemporary U.S. anti-terrorism policy: U.S. leaders constituted radical Islamic terrorists as people who desired to attack the American way of life, in particular our capitalist system. In our draconian and violent attempts to stop these terrorists, we justified attacks against economic "soft" targets, which made us overvalue the economic rather than physical costs of terrorism.

The connection between Anwar al-Awlaki and the Tsarnaevs' discourse was evidence that the U.S. government's drone strike killing of Awlaki did not eliminate his influence on potential radicalized people. While justice and righteous retaliation became powerful tropes to rally the American people against al Qaeda, the flip side of this is that the tool used to execute this war, drone strikes and the secrecy in their use, was re-appropriated by terrorists to serve as a powerful rhetorical trope to recruit people into identifying with and joining their organizations. For instance, a person named Isaac asks *Inspire* editors about their opinions on the U.S. drone strikes in Yemen (*Inspire*, 2013). *Inspire* took the opportunity to proclaim that drone strikes were an example of how America terrorized Muslims in a cowardly fashion. For example, *Inspire* editors (2013) highlighted that Obama's reliance on drone strikes, especially signature strikes, which

allow the government to target based on suspicious behavior and actions without identifying a suspect, undermined U.S. credibility. As *Inspire (2013)* noted:

> Of course! Obama is declaring a crusade! These missiles have no eyes and their launchers are more blind [sic]. They kill civilians more than mujahideen [sic]. They kill civilians intentionally and the next day we see 'CNN and ABC' acting as wikileaks [sic] and report a 'classifeid'[sic] operation in Yemen "US has killed a key Al-Qaeda figure, "who in fact is an old woman going to the hospital or a young man going to work. After all that, they claim they have a noble cause. They want nations to imitate them. They legitimize their war on AQAP. If this war on AQAP is that noble, why does it have to be that secretive? Why don't they declare this war on Yemen just like they did in Afghanistan and Iraq? Why don't they come and face the mujahideen [sic] like men instead of killing civilians indiscriminately? Where is their acclaimed value - if they have any? (p. 7)

Note here how *Inspire*'s editors specifically criticized the secrecy behind the Yemen drone strikes, thus turning the Obama administration's transparency discourse back against itself. Moreover, due to this secrecy, al Qaeda and *Inspire* were allowed to characterize the U.S. as cowardly and terroristic, something that an open democracy is supposed to cure.

Another argumentative tactic used by *Inspire* turned the logic of representative democracy back against the U.S. For instance, *Inspire* (2013) claimed that because the U.S. is a government ruled by the people, American "rulers (people) should pay for their country's action till they change their system and foreign polices" (p. 7). This logic embedded within al Qaeda and *Inspire*'s rhetoric reversed the logic of a republican government by arguing that citizens should be killed in order to exact revenge on the action of their representatives; citizens metonymically fill in for the U.S. government. According to this logic, if the leaders who are supposed to represent the people engaged in actions that targeted and killed Muslims, then Muslims had an obligation to fight back

by killing American citizens. As the Obama administration continued to focus the war on terror on individual targets and dispositions, terrorist organizations utilized a wider rhetoric of accountability and transparency to justify attacks against individuals as representatives of their larger government's ideology and policies.

While it might be easy to quickly dismiss the idea that citizens are responsible for the actions of those who govern, the rhetorical effects of how leaders constitute the people make the idea appear almost reasonable. The ability to interpellate citizens and invite them to identify collectively in a way that adhered to a particular set of values and against a common enemy worked to unify the public but also created a collective foe from the perspective of the enemy. This allowed al Qaeda to use the logics of economic value and transparency against the U.S. government in order to recruit new jihadists.

In a circular fashion, this reversal of U.S. rhetoric led the President to further emphasize the dangers posed by homegrown extremism. The next section of this chapter explores Obama's May 23rd speech that defined the next phase of the war on terrorism in a post-bin Laden era. First, the analysis examines Obama's definition of drone strikes as consistent with American values. Secondly, the subsection analyzes how presidential definition was used to redefine the war on terror through an endo-colonizing discourse of domestic radicalization and homegrown extremism. Finally, the subsection explores how Obama's rhetoric reoriented the privileges of citizenship as contingent on proper transparent performances. In many ways, the May 23 speech tied together many of the threads of discourse President Obama had used previously about the war on terror.

Obama's May 23 speech and intensification rhetoric. As a result of bin-Laden's death, the Boston bombing, and drone strikes against American citizens, President Obama was offered a rhetorical opportunity to clarify and define his counter-terrorism strategy. On May 23, 2013, the President addressed the public regarding how the U.S. was going to fight the war on terror in a post-bin Laden world. In doing so, he relied on presidential definition to distinguish his warfighting strategy from that of the Bush administration, identifying the new threat of terrorism and redefining the war on terror. First, Obama provided his rationale for intensifying warfighting through increased use of armed drones to conduct targeted lethal operations. Second, Obama redefined the threat the U.S. faced in the post-bin-Laden world: domestic radicalized subjects. According to the President, due to the success of the U.S. anti-terrorism campaign, most of the high-ranking al Qaeda leadership was eliminated. While celebrating this accomplishment, President Obama used this speech as an opportunity to redefine the primary target of the war on terror as domestic radicalization and homegrown extremists. This established an endo-colonizing logic justifying intensified surveillance and policing of domestic populations, thus turning the war on terror back on the citizens.

He began his speech by comparing his warfighting strategy with that of President George W. Bush. First, President Obama implicitly connected the Bush administration's war in Iraq with bringing al Qaeda into the region. While Bush articulated Iraq as a regime of terror and part of the axis of evil, President Obama credited himself as being the president who managed to end the war in Iraq and brought home hundreds of thousands of American troops. With this argument, the President suggested that he

deescalated conflict in the region. Second, President Obama differentiated himself from his predecessor by condemning how the former president relied on torture and methods of detainment that ran counter to the rule of law. Finally, he criticizes President Bush's definition of the war on terror as unrealistic and instead provided a new strategy for fighting the war on terror that he argued was more consistent with promoting America's values.

Obama utilized a rhetoric of intensification to distinguish himself from Bush. By intensification, I mean that the President was able to criticize and distance himself the secretive aspects of the Bush administration's strategy that were viewed negatively—e.g., torture and use of ground troops on foreign soil—while simultaneously embracing and increasing the aspects of Bush's tactics that Obama favored. For instance, Obama credited increased security measures such as surveillance with helping America more secure, while he also argued that the government should find a balance between security and privacy. Put differently, President Obama was able to capitalize on the security benefits brought about by the immense government surveillance program implemented by Bush, while taking the politically popular stance of claiming to be a defender of civil rights and liberty. Again, transparency rhetoric allowed the President to claim to be a champion of transparency by being open and publicly condemn the uglier public parts of his predecessor's policies like ground invasion and torture, while keeping his other programs secret. This allowed Obama to renounce politically unpopular issues while simultaneously reserving the flexibility of keeping security policies that he preferred classified from the public.

Using this intensification rhetoric, President Obama built off the Bush administration's stated preference for capturing enemies and interrogating them for useful information. Yet, he differentiated himself from previous administration in the way that he advocated for capture. For example, unlike Bush, Obama denounced the detaining of terrorist suspects in secretive black sites and submitting them to enhanced interrogation techniques. Likewise, Obama called for the closing of Guantanamo Bay and transferring those currently detained there to Federal Supermax Prisons. Both arguments distinguished Obama from Bush because he appeared to be more open and less repressive than his predecessor. Yet, the bureaucratic safeguards that prevented this from happening all worked to make capture less and less likely. For instance, where does the U.S. capture and detain individuals if it is not allowed to use black sites or Guantanamo Bay? Additionally, the expanded definition of imminent threat and militants, combined with Obama's public stance against putting U.S. boots on the ground, allowed for very few viable options. If the enemy was illusive and hid in remote and empty locations and the U.S. was unwilling to send in soldiers to capture them, then the result became an increased reliance on armed drone strikes. Thus, Obama could appear to be dovish and more transparent than his predecessor while actually increasing the very military tactics that fueled resentment and terrorist acts against the U.S.

President Obama often referred to his military strategy using the language of intensification. Obama claimed that he increased the war against al Qaeda while also changing the way that fighting occurs. For example, one of the primary differences that Obama highlighted was effectiveness of strategy. In this instance, the President

maintained that the U.S. needed to relentless and specifically target al Qaeda leadership, as opposed to Bush's reactive stance of labelling all those who did not choose to stand united with us—most notably, nations of concern like Iran and North Korea—as the enemy. Therefore, Obama emphasized that intensified tactics were justified as long as they produced demonstrated results. However, despite eliminating many of al Qaeda's high ranking leaders, Obama undermined his own claim about effectiveness by arguing that America was always going to be targeted for attack by various global terrorist networks. Against his claim of effectiveness, the very tactics used by the President ensured more networks of terrorists emerged. Thus, an endless cycle of ideological conflict develops between radicalized subjects and the U.S.

To wage this new intensified war on terror, Obama interpolated citizens as being active participants fighting an ideological battle. The question of how to fight terrorism was a responsibility that, according to Obama, mattered to every American (WH, OPS, 2013, May 23). Obama stated, "America is at a crossroads. We must define the nature and scope of this struggle, or else it will define us" (WH, OPS, 2013, May 23, para. 12). Therefore, the President argued that the first priority in redefining the war on terror was to understand the current threat that terrorism posed. Obama described the threat as occurring at three levels. First, there was the threat posed by al Qaeda, which had largely been dismantled and believed to no longer possess a serious threat to the U.S. homeland. Second, there was the threat presented by al Qaeda affiliates such as the al Qaeda in the Arabian Peninsula (AQAP). These groups did not possess the capability to wage major attacks on American soil and instead concentrate on localized acts of terrorism such as

the attack at Benghazi or attempts to launch attacks against Western diplomats, companies, and other targets that are overseas (WH, OPS, 2013, May 23). The third threat, and the one that Obama was primarily concerned with, was the threat posed by radicalized homegrown extremists. In the May 23 speech, Obama defined homegrown extremists as, "deranged or alienated individuals – often U.S. citizens or legal residents" who are capable of doing enormous damage, "particularly when inspired by larger notions of violent jihad" (WH, OPS, 2013, May 23).

In shifting the focus away from external threats of terrorism and towards domestic radicalization, the President posited the war on terror as occurring on the battlefield of ideology. For example, Obama declared that radicalized individuals were fueled by the common ideology: "Islam is in conflict with the United States and the West, and that violence against Western targets, including civilians, is justified in pursuit of a larger cause" (WH, OPS, 2013, May 23, para. 19). While both Bush and Obama constantly reiterated that they were not against Islam in general, the discursive terms that the Presidents relied on indicated otherwise. For instance, Obama claimed that the largest threat to the nation was homegrown extremism, which could be rooted in any faith or ideology. Yet, in Obama's rhetoric, the assumption was that this radicalization is of the Muslim faith. This was a flawed assumption, as the *New York Times* recently published an article claiming that since September 11, 2001, nearly twice as many people were killed by non-Muslim extremists than by Islamic fundamentalists (Shane, 2015). In other words, the majority of extremists who kill Americans were affiliated with antigovernment fanatics, white supremacist groups, and other non-Muslim groups. This statistic does not

even take into account mass shootings and other forms of violence that kill American citizens on a regular basis. The *New York Times* article argued that while there have been lethal attacks carried out by Islamic militants in the U.S., there have been at least 19 lethal attacks carried out by non-Muslims (Shane, 2015). Yet, when it comes to classifying radicalized acts of violence as terrorism, the Obama administration has consistently singled out Islamic extremism as the preeminent terrorist threat to the U.S. Put differently, by framing the enemy as being locked into an ideological battle against the U.S., the Obama administration must demarcate radical Islamic beliefs as suspicious and dangerous identifiers of potential terrorist activity.

Regardless of the religious qualifier, the focus on radicalization frames ideologies, thoughts, and speech as dangerous and infectious. The idea that religious extremism must be combatted assumed that "normal" people could be persuaded to adopt extreme beliefs and engage in violent actions. In defining the threat as radicalism, Obama suggested that the enemy was irrational and caught up in the throngs of passion. For instance, rather than acknowledge the possibility that drone strikes might infuriate people or that declaring war against Muslim countries might force people to choose between religion and nation, Obama declared that the real enemy was radicalized individuals that have been misled and recruited by propaganda. Rather than behaving rationally, radicalized terrorists are depicted as people infected by a dangerous ideology that persuaded otherwise good people to act in a violent manner. This ideological perspective is why Awlaki might have been considered such a threat: a religious leader who used persuasion to recruit people to identify with a terrorist subjectivity.

In order to counter the enemy whose primary recruiting strategy was interpellation, Obama responded by criminalizing radical Islamic beliefs as deviant while simultaneously constituting Americans as citizen-detectives who adopted a counter ideology within "a battle of wills, a battle of ideas" (WH, OPS, 2013, May 23). Obama's call for a counter-ideology approach intensified his 2011 counter-terrorism strategy's operational logic that was built on cultivating an informed citizenry that communicated directly with the government. In other words, Obama utilized the concepts of government 2.0 and relied on surveillance of daily communication and performances to monitor the behavior of citizens. This surveillance was then used to separate the citizens who are displaying signs of suspicious radicalized ideologies from those who are engaged in purportedly normal behavior. The rhetorical emphasis on an open society encouraged citizens to adopt the subject position of a citizen-detective, an ever vigilant and guarded subject who was willing to report suspicious or potential radicalized activity.

For example, Obama's 2011 rhetoric about his counter-terrorism strategy argued that an open society was essential to keep citizens informed and prepared to fight radicalization (WH, OPS, 2011, Aug 3). President Obama declared that a transparent society increased government and law enforcement's knowledge about radicalization. As was established in Chapter 3, the logic of government 2.0 relied on citizens producing data that could be shared and monitored with local law enforcement. In this instance, this reasoning extended into an effort to combat domestic extremism where government and law enforcement members established relationships with local community members. Obama's counter-terrorism strategy explained that the goal for these relationships was to

help law enforcement be, "vigilant in identifying, predicting, and preempting new developments" (WH, OPS, 2011, Aug 3, p. 6). In order to prevent domestic radicalization, the government wanted to conduct research and analyze local populations, communicating with local residents to enhance cultural proficiency (WH, OPS, 2011, Aug 3). Put differently, the government and law enforcement needed to surveil local populations to detect threats. Once the government was able to understand and monitor the communication and behavior patterns of local populations, it then sought to root out and resist the rhetorical underpinnings of radicalization.

The government depended on implementing surveillance at numerous levels to root out domestic radicalization. For example, traditional modes of government surveillance implemented under the Bush administration were continued by Obama. Yet, as Chapter 3 indicated, Obama began to initiate new lateral modes of surveillance encompassed through government 2.0 initiatives built around citizen-government collaboration. Because the government viewed the war on terror as occurring at the ideological level, part of the strategy to combat extremism was to forge partnerships between the Muslim-American community and law enforcement. Obama explained this approach by stating:

> …technology and the Internet increase [radicalization's] frequency and in some cases its lethality. Today, a person can consume hateful propaganda, commit themselves to a violent agenda, and learn how to kill without leaving their home. To address this threat, two years ago my administration did a comprehensive review and engaged with law enforcement.
>
> And the best way to prevent violent extremism inspired by violent jihadists is to work with the Muslim American community -- which has consistently rejected terrorism -- to identify signs of radicalization and partner with law enforcement when an individual is drifting towards

> violence. And these partnerships can only work when we recognize that Muslims are a fundamental part of the American family. (WH, OPS, 2013, May 23, para. 58-59)

Therefore, the strategy to combat domestic radicalism relied on the government using surveillance, as Obama said, "to intercept new types of communication" while also convincing Muslims to spy on one another and report suspicious activity to the very agencies that were conducting espionage on them (WH, OPS, 2013, May 23).

One implication of this counter-terrorism rhetoric was that it promoted a similar type of radical adherence to ideology within a battle of competing ideals. For instance, in the 2011 counter-terrorism strategy statement, the White House Press Secretary (2011, Aug 3) defined radicalization as "…that [which] leads to violent extremism includes the diffusion of ideologies and narratives that feed on grievances, assign blame, and legitimize the use of violence against those deemed responsible" (p. 6). To respond to this type of extremism, the Press Secretary suggested that the government should apply government 2.0 concepts such as using social media to educate citizens about the dangers posed by radicalization and, in response, promote American values as a counter-ideology. Yet, this attempt to fight the war on terror at the ideological level demonstrated how American exceptionalism functioned once again. For instance, the U.S. maintained that American values were inclusive and superior to those of extremists. Further, these inclusive values were used to form a counter-ideology that did not tolerate extremism and worked to supplant it. American exceptionalism was used to cultivate citizen-detectives who were willing participants in an ideological battle. Yet, by their own definition, Presidents Bush and Obama employed rhetorical strategies that radicalized American

citizens in ways that supported violent extremism in the form of military aggression against radicalized populations. For example, Obama made arguments that played on the grievances about the loss of life, finances, or property that occurred due to extremist terrorist acts. Much like the extremists his Press Secretary described, President Obama assigned blame to al Qaeda, bin Laden, and Islamic extremism for his military strikes. Finally, he legitimized the use of violence against those deemed responsible through drone strikes, military invasion, or other lethal operations. The fundamental difference between the Obama administration's discourse from radicalized individuals was that exceptionalism made one version seem justified while the other was not.

Another implication is that Obama use of counter-ideologies to fight domestic radicalization was combined with the intensified war rhetorical to legitimize violence against external threats. For instance, Obama drew on transparency rhetoric to depict the enemy as opaque, remote and secretive. In Obama's rhetoric, the enemy included dangerous individuals hiding out in caves, compounds, and remote tribal regions and training in empty deserts or rugged mountainous terrain. Moreover, the enemy operated outside of the logic of national sovereignty by inhabiting spaces in places such as Afghanistan, Pakistan, Somalia, and Yemen where the state had at best tenuous control. Obama even described these locations as places where the state did not have the capacity or desire to enter the territory where terrorists were inhabiting (WH, OPS, 2013, May 23). This justified intensified war tactics, in what the President described as "lethal, targeted action against al Qaeda and its associated forces, including with remotely piloted aircraft commonly referred to as drones" (WH, OPS, 2013, May 23, para. 28). Because the space

that the enemy inhabits makes it impossible to deploy Special Forces or other military forces to capture terrorists and the U.S. was not at war with the nations listed, a decision to put U.S. boots on the ground was impossible and would have likely led to an international conflict.

In addition to justifying violent against those violent militant others, the President's discourse also rationalized the use of military strikes against U.S. citizens and civilians. Although Obama went on record to argue that he believed that it is unconstitutional for the government to target and kill U.S. citizens, his statement was conditioned upon citizens engaging in approved and transparent ideological performances. As Obama explained, "when a U.S. citizen goes abroad to wage war against America and is actively plotting to kill U.S. citizens, and when neither the United States, nor our partners are in a position to capture him before he carries out a plot, his citizenship should no more serve as a shield than a sniper shooting down on an innocent crowd should be protected from a SWAT team" (WH, OPS, 2013, May 23, para. 47). Yet, the decision to deploy a drone strike was significantly different than sending in a SWAT team to eliminate a sniper. First, members of a SWAT team risk their lives to apprehend or eliminate their target. This places a certain moral cost on deploying forces in this analogy. However, Obama viewed drone strikes as moral precisely because they do not put American soldiers' lives at risk. Thus, while drone strikes might be considered moral under that view, it simultaneously intensified the use of a deadly tactic in numerous situations. Second, Obama's description of drones as precise weapons obfuscated the reality of practices like signature strikes, in which the government

determined that a series of behaviors were suspicious and constituted a potential imminent threat. To moralize drone strikes, such as the President did, required denial that drone strikes kill civilians. For example, Obama did this in stating, "there's a wide gap between U.S. assessments of such casualties and nongovernmental reports [of casualty deaths]" (WH, OPS, 2013, May 23). While true, this statement does not validate Obama's assertion that the U.S. does not kill civilians. Indeed, according to three independent organizations—the Bureau of Investigative Journalism, *The Long War Journal*, and the New America Foundation—U.S. drone strikes have killed at least 476 civilians in the 522 counted strikes (Shane, 2015).

Additionally, despite Obama's claim that he would promote greater government transparency, information on drone strikes was typically regarded as a national secret. For instance, while the President told the public that drone strikes did not target innocent civilians, the actual strikes remained classified so there was no process to verify the reports, other than through the occasional statements made by anonymous administration officials or people in the region of the strike (McCrisken, 2013). Further, President Obama had the power to define a targeted operation and distinguish it from a signature strike. This allowed the Obama administration to claim responsibility for killing individuals on a kill list, while disavowing responsibility for people killed in signature strikes. In addition, the President's ability to define a militant or terrorist became so broad that the government was able to obscure the public's information regarding causalities.

As a result, presidential definition helped explain the disparity between government and nongovernmental reports about civilian casualties in drone strikes. The

government's reliance on signature strikes meant that the person being targeted for the strike was not necessarily on the capture/kill list; instead, the target was exhibiting behavior that was considered consistent with that of terrorism. Take for instance the killing of 16-year-old American citizen Abduhlramen al-Awlaki, who was sitting in a café in Yemen. He posed no imminent threat but he became collateral damage in a strike that allegedly was not targeting him. When asked about how the Administration could justify the drone strike against Abduhlramen, former White House Press Secretary and senior advisor to the reelection campaign Robert Gibbs defended the strikes: "I would suggest that you should have a far more responsible father if they are truly concerned about the well-being of their children" (WeAreChange, 2012). The fact that the government did not have a legitimate justification for killing Abduhramen, other than victim-blaming his father, indicated that, despite all the language of precision and transparency, the government did not always know who it was killing. Indeed, of the eight known American citizens that have been killed in drone strikes, only Anwar al-Awlaki was identified and deliberately targeted (Shane, 2015); the other seven citizens were killed in strikes that were aimed at other individuals or were caught up in signature strikes.

Moreover, the Americans who were killed in drone strikes were not all terrorists or even related to people who were alleged terrorists. For example, aid worker Warren Weinstein, who had been kidnapped and was being held hostage by al Qaeda, was killed when a CIA drone targeted the compound where he was being held. In addressing the public about the strike, Obama used transparency rhetoric to help explain the

government's mistake. For instance, the President initially apologized and took full responsibility for ordering the drone strike. Then, he argued that the CIA conducted hundreds of hours of surveillance and believed that the compound only included members of al Qaeda (WH, OPS, 2015, Apr. 23). Yet, the President maintained that Weinstein was lost in the "fog of war" and his death was an unfortunate mistake (WH, OPS, 2015, Apr. 23). Overall, Obama's decision to declassify the details of this particular drone strike and to openly take responsibility for the mistake served as a testament to American exceptionalism and its dedication to democracy and transparency. The U.S. was exceptional because it was open and willing to admit and learn from mistakes. Rather than relying on classifying the drone strike as a matter of national security, the decision to be open about the mistake reaffirmed Obama's commitment to transparency and promoted the exceptionalist ethos that does not shroud itself in secrecy.

However, the willingness to admit mistakes was misleading when the Obama administration had the power to flexibly define those who were killed in a strike as "militants." Part of the Obama administration's strategy in promoting transparency was to remove the classification of "enemy combatant" used prevalently by the Bush Administration to capture, detain, or kill those labeled with the moniker. However, Obama replaced "enemy combatant" with the term "militant," defined as all military-aged males in a strike zone unless they were posthumously exonerated (Becker & Shane, 2012; McCrisken, 2013). The ability to define people as militants allowed the President to proclaim civilian casualty rates as being extremely low and explained the discrepancy between government and nongovernment reports. Because the government could

posthumously classify people as militants or suspects, the dead had no way to prove their innocence. Quite simply, there was no way to retroactively prove that the dead did not actually pose an imminent threat to the U.S. Likewise, there was no public trial that could be used to exonerate the dead and expose the government's narrative of precision killing to be a farce. The ability to denigrate the dead by labelling them as militants became all the more powerful when the government relied on strategic disclosures to take responsibility and apologize for mistakes such as killing Weinstein. The fact that the government could choose to be open gave credence to a belief that when it killed a person named and labeled as a "militant," that person was indeed a dangerous enemy.

In conclusion, the endo-colonizing shift away from an external enemy and towards a domestic subject ideologically interpreted as a threat became a way in which citizen's everyday behaviors and communications were regulated in ways to participate in the war on terror. In this case, President Obama's use of the transparency trope worked to invite citizens to submit to government surveillance and be vigilant and spy on others. While Obama paid lip service to the importance of openness and the cleansing power of sunlight, it was an asymmetrical form of transparency. For example, citizens were encouraged to be open so that the government could determine abnormal from normal activity. However, Obama's attitude changed in regards to citizens reporting government activity that seemed suspicious to the media. Even though Obama campaigned on openness and the importance of whistle-blowers to democracy, he eventually declared, "As Commander-in-Chief, I believe we must keep information secret that protects our operations and our people in the field. To do so, we must enforce

consequences for those who break the law and breach their commitment to protect classified information" (WH, OPS, 2013, May 23, para. 37). This contradiction demonstrated the asymmetrical relationship that citizens had with surveillance and transparency: the government will be open and transparent to the people on the condition that the people do not take it on themselves to expose government surveillance.

Edward Snowden leaks and Obama's rhetorical response

Less than a month after President Obama delivered his May 23 speech on counter-terrorism, *The Guardian* and *Washington Post* began to release stories about the mass surveillance programs carried out by U.S. counter-terrorism agencies. Snowden, a former NSA employee, had downloaded thousands of classified documents, contacted members of the media, and distributed the documents so that they could be made available to the public. Beginning June 5, 2013, the public became aware of the numerous secret surveillance programs carried out by the government against its own citizens. As indicated in Chapter 2, these programs were involved in the algorithmic profiling of citizens to determine who was performing as either a good citizen or suspicious and threatening domestic radical.

As a result of the leaks, on August 9, 2013, the President released a statement announcing reforms to curtail the NSA programs. The White House once again used transparency rhetoric in an attempt to restore its credibility in light of the revelations that the Administration had violated citizens' privacy in the name of national security. For example, the Administration quickly acted to send a signal to the public that the President was taking action to ensure strong governmental oversight over this surveillance and

clear protections were being put into place to prevent future abuse (WH, OPS, 2013, Aug 9). In particular, four specific actions, outlined in a White House statement, were being taken by the President to increase transparency and increase public trust in the safeguards already in place. First, the Obama administration claimed it would work with congress to reform Section 215 of the USA Patriot Act (WH, OPS, 2013, Aug 9). Second, the Administration and congress would improve the public's confidence in the Foreign Intelligence Surveillance Court (WH, OPS, 2013, Aug 9). Third, the intelligence community would be directed by the President to declassify as much information as possible without jeopardizing national security (WH, OPS, 2013, Aug 9). Finally, the President would form a group of external reviewers to assess the surveillance programs and provide a report about how to best maintain the public's trust and an effective foreign policy (WH, OPS, 2013, Aug 9).

President Obama framed his decision to speak about government surveillance as an example of exceptionalist government transparency. As Obama stated, "American openness -- because what makes us different from other countries is not simply our ability to secure our nation, it's the way we do it—with open debate and democratic process" (WH, OPS, 2013, Aug. 9). Besides its obvious exceptionalist tone, the ability to cast strategic disclosure of government surveillance in this way was an example of what Engels and Saas (2013) call acquiescence rhetoric. In this instance, acquiescence is the ability to articulate together government surveillance and transparency in order to persuade the public that mere status updates by the president is the same as an informed and open public debate. For example, Obama used his status as president to inform the

public that the government was spying on them but insisted on the biopolitical impulse that the data collected was only being used for counter-terrorism purposes and was not being abused. Rather than offering an informed debate about whether or not the government should be conducting mass surveillance for counter-terrorism purposes, the public was provided a technical status update confirming that surveillance was being conducted, but the public was asked not to worry because technical safeguards were in place to prevent future abuse. Further, citizens were asked to have faith in the Administration because this was America and these kinds of abuses do not occur here, despite evidence to the contrary.

On January 17, Obama spoke at the Department of Justice to address government surveillance and Snowden's leaks. While Obama campaigned on the importance of curative sunlight, it appeared that Snowden's disclosures brought the sun too close as Obama renounced the leaks as producing more "heat than light" (WH, OPS, 2014, Jan 17). Based on this change in position, it seemed as though the biopolitical imperative of protecting national security superseded Obama's original praise of whistleblowers. To mask over this substantial change in position, Obama's used three rhetorical strategies: first, Obama defended the importance of surveillance for national security; second, Obama blamed all of the problems of government abuse on the Bush administration; and third, despite the fact that Obama was only discussing surveillance because it was leaked to the public, Obama offered his open discussion as proof of his Administration's commitment to transparency.

President Obama began his speech by framing surveillance as an intrinsic component to the founding the nation (WH, OPS, 2014, Jan. 17). Specifically, Obama articulated the NSA's mass surveillance program as a modern manifestation of Paul Revere and the "Sons of Liberty." Through this conceptualization, citizens were asked to support government surveillance because without it, the U.S. would never have been able to win the Civil War, World War II, or the Cold War. According to Obama, the 9/11 attacks marked a pivotal moment that altered how surveillance and warfighting were to be conducted. Within this logic, the traditional Realist methods of conducting foreign policy – e.g., gathering international intelligence and waging wars against nation-states—had to be modified and updated to deal with a new globalized and non-state centric political arena. To effectively fight the war on terror, the U.S. needed a counterterrorism strategy capable of tracking individuals or small groups acting independent of a sponsor state. For instance, intelligence agencies were asked to do more than monitor nation-state communications and instead were called on to identify, target, and preempt individuals believed to be responsible for current or possible future attacks (WH, OPS, 2014, Jan 17). In other words, Obama informed the American public that the changes in government surveillance were important for preventing terrorist attacks and saving lives globally. In order to fight these terrorist threats, the government employed algorithmic governance in order to, as Obama stated, "unravel a terrorist plot; intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised or to ensure that hackers do not empty your bank accounts" (WH, OPS, 2014, January 17, para. 24).

Thus, the government had to collect and monitor data so that it could best protect American citizens.

While working to reassure American citizens that government surveillance was only used to protect rather than harm them, Obama shifted the blame onto the Bush administration. For example, Obama criticized policies such as enhanced interrogation and warrantless wiretaps that were instituted without public debate (WH, OPS, 2014, January 17). Yet, despite the fact that Obama knew about, continued, and even renewed the surveillance policies implemented by the Bush administration, Obama claimed that his predecessor was accountable for the "worst excesses that emerged after 9/11" (WH, OPS, 2014, January 17). The ability to blame the Bush administration for excessive surveillance allowed Obama to argue that, in comparison, his Administration was rather transparent. By publicly discussing some surveillance policies, Obama sought to establish ethos with the public regarding how committed his Administration was to the values of openness and transparency.

However, Obama's openness about government surveillance was framed along the traditional biopolitical demarcations of inside/outside and citizen/non-citizen. For instance, Obama did not discuss any of the programs that may collect citizens' data; instead, he chose to discuss surveillance conducted against non-citizens or people communicating with non-citizens. According to the President, intelligence agencies tap into daily communications in order to pinpoint "an al Qaeda cell in Yemen or an email between two terrorists in the Sahel" (WH, OPS, 2014, January 17, para. 11). Obama further explained that there were absolutely no legal restrictions in regards to surveillance

against non-citizens, noting that intelligence agencies "cannot function without secrecy" and outside of public debate about the matter (WH, OPS, 2014, January 17). Therefore, while upholding the values of democracy and the importance of public debate, Obama was able to bypass criticism by informing the public that he already had listened to the debates and made a decision on the matter on the public's behalf. According to the President, the public could rest assured because the he had already established sufficient oversight through congressional and regulatory committees and FISA courts and he listened to critical opinions from civil liberty and privacy advocates and national security advisors. Thus, in an exceptional fashion, Obama suggested that debates about government surveillance were not conducted in the open with public input because the he had already had the debates in private and determined the best course of action.

While Obama shared the public's concern about the government's ability to abuse surveillance technologies, he defended his choice not to stop the programs because he felt that they make the nation more secure and that he had learned nothing to indicate that the intelligence community was abusing their surveillance powers (WH, OPS, 2014, January 17). Even though the public was made aware of excessive surveillance abuse by Snowden, Obama sought to persuade the public to support surveillance based on the assumption that he had exceptional knowledge and that the surveillance operators were exceptional Americans who should work outside the law. Within Obama's discursive frame, citizens should appreciate that U.S. intelligence operatives were law-abiding patriots, ordinary people laboring to connect, identify, and predict potential terrorist

activity in order to prevent another 9/11-style attack (WH, OPS, 2014, January 17). For example, Obama noted the innocent and noble nature of these employees in stating:

> After all, the folks at NSA and other intelligence agencies are our neighbors. They're our friends and family. They've got electronic bank and medical records like everybody else. They have kids on Facebook and Instagram, and they know, more than most of us, the vulnerabilities to privacy that exist in a world where transactions are recorded, and emails and text and messages are stored, and even our movements can increasingly be tracked through the GPS on our phones. (WH, OPS, 2014, January 17, para. 30)

By casting intelligence workers as average patriotic Americans, Obama relied on as argument of exceptionalism. Of course intelligence workers are more aware than most ordinary citizens about the vulnerabilities of privacy because they are the people who collect, sift through, and track people by gathering information. However, what Obama failed to note is that these members of the intelligence community have an asymmetrical and exceptionalist relationship to ordinary citizens. Intelligence workers were situated in an exceptional space outside the rule of law where they have exclusive access to information that they used to defend the law in the name of the public. The importance of the task became the exceptional logic that dictated who does and does not have access to information. Yet, the question still remained: if intelligence employees were exceptional citizens who protected other Americans, then why should the public not defer to Snowden, a former member of the intelligence community who provided material proof regarding the rampant abuse of surveillance power?

The President was able to position himself as more credible than Snowden due to his use of definition and exceptionalist ethos. While Snowden leaked materials to the media to inform the public, Obama relied on exceptionalist logic in discussing

governmental oversight of surveillance. For instance, Americans were told that they could trust that surveillance was not being abused because there is a Review Group on Intelligence and Communications Technologies that wrote surveillance reports and suggested changes (WH, OPS, 2014, January 17). Obama also noted that he consulted with the Privacy and Civil Liberties Oversight Board created by Congress. However, while oversight was important, it was a far cry from the type of transparency advocated by Obama in almost every other instance. For example, the general public was not informed about the surveillance policies in place nor did it get to debate about what the policy should have been or how it was implemented. Instead, the public is asked to trust the process even though the review boards do not answer to the public or operate transparently.

Obama also deployed American exceptionalist rhetoric as he rationalized the importance of government surveillance. The President stated, "America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people" (WH, OPS, 2014, January 17, para. 26). Within this discursive frame, surveillance was a necessity given America's exceptional status as an economic, military, and technological superpower. Thus, the U.S. was not just defending the security of its own citizens, but also collects information to preserve global security. By framing surveillance as a global matter, Obama deployed an exceptionalist ethos that reinforces the idea that America was the best and most open country. As Obama argued, "no one expects China to have an open debate about their

surveillance programs, or Russia to take privacy concerns of citizens in other places into account. But let's remember: We are held to a different standard precisely because we have been at the forefront of defending personal privacy and human dignity" (WH, OPS, 2014, January 17, para. 59). In other words, the only reason that surveillance was being debated in the U.S. was because of America's exceptional status as a superpower and defender of global human rights.

Beyond this exceptionalist framing, President Obama's justification of government surveillance exposed how the political logic of American exceptionalism is simultaneously an economic logic of government 2.0 practices. By defending surveillance, Obama reinforced the idea that government surveillance was no different than corporations monitoring and tracking of consumer data on a daily basis. For instance, corporations track consumers' purchases and website search strings and visits. According to Obama, if companies were allowed to take customers' information and use it to construct digital profiles for commercial purposes, then the government should have been able to do the same thing to detect threats to the population. Further extending this argument, the President argued that, in many instances, the government does not have to spy on citizens itself; instead, it could outsource the work to private companies and then order the companies to turn over their data to the government. Obama acknowledged that this outsourcing process occurred in noting that the FBI can issue a national security letter requiring companies to provide specific information to the government without disclosing the orders to the subject of the investigation (WH, OPS, 2014, January 17). Although Obama claimed that the regulations on government surveillance need to be

stricter, the fact that he even included this revelation demonstrated how the government relied on the permissibility of cultural practices such as consumerism to rationalize how it conducted the war on terror. Therefore, consumerism became a method by which citizens communicated, personalized their identities, and provide the possibility of tracking what was labeled pathologizing behavioral and communicative patterns.

Obama's reliance on corporate data collection for national security purposes was hardly surprising given his history with technology companies and his campaign for transparency. Even the way that Obama campaigned normalized data collection of American citizens by using information to craft personalize marketing strategies to persuade people to vote for him. For example, relying heavily on predictive analytics, Obama's campaign team conceptualized the electorate as a collection of individual citizens who could be measured and assessed on their own terms (Issenberg, 20012). When campaigning in 2012, Obama's campaign team felt confident that it knew the name of every one of the 69,456, 897 Americans who voted for their candidate. As a result, the team also had access to information about the citizens who were not registered, did not vote, or were not likely to be persuaded to vote for Obama in the next election. By adopting a micro-targeting strategy, Obama's team was able to mine public data to identify individuals that needed to be registered to vote, mobilized to action for the campaign, or persuaded to vote a specific way. Therefore, this data constituted a new political currency that could predict individual behavior. As Issenberg (2012) noted, "To derive individual-level predictions, algorithms trawled for patterns between these opinions and the data points the campaign had assembled for every voter—as many as

one thousand variables each, drawn from voter registration records, consumer data warehouses, and past campaign contacts…the campaign didn't just know who you were; it knew exactly how it could turn you into the type of person it wanted to be" (para. 11-12). Given Obama's proclivities for activating algorithmic citizenship to get elected, it is not surprising that the same practices would be used to govern afterwards.

Moreover, the reliance on algorithmic governance became a key justification in defending surveillance tactics such as the collection of citizen metadata. Obama relied on a typical defense for the practice by saying that the surveillance program "does not involve the content of phone calls or the names of the people making the calls" (WH, OPS, 2014, January 17, para. 35). While it was true that metadata was just a collection of data about data, the President was wrong in claiming that companies and the government do not know the names of people linked to phone calls. Instead, the government was able to collect the phone records as well as the lengths of the calls. Additionally, the government had the phone numbers that were being used and had the capability to research the identity of the owners of those numbers. While the government did not know the exact content of the conversations, it knew who they were between and how long they were communicating. For instance, this meant that the government knew that the number (555) 555-1234 belonged to John Doe and that someone using that number made numerous phone calls to a specific location. This information then could be used to ascertain private information about those people's lives, even though the government claimed that it was only collecting metadata. Even if the government did not know exactly who was on the phone, it could establish a communication profile and attempt to

determine suspicious patterns like if a certain phone call was communicating with a number that was used by a suspected terrorist.

The collection of metadata was an extension of algorithmic citizenship that became a primary method of profiling potential terrorist subjects. For example, Obama cited the phone use of one of the 9/11 terrorists as evidence for the need for metadata collection: "One of the hijackers–Khalid al-Mihdhar–made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw the call but it could not see that the call was coming from an individual already in the U.S." (WH, OPS, 2014, January 17, para. 39). Thus, Section 215 of the Patriot Act was implemented to map the communications of terrorists to see who they were contacting and map the network connections. The Obama administration justifies this program through a security rhetoric while simultaneously downplaying the collection of ordinary citizens' information. By discursively distinguishing between metadata and daily communications, the government could claim that it was not listening in on your conversations. Instead, what it was legally doing was monitoring metadata to determine if citizens were performing as normal algorithmic citizens or if there were suspicious patterns emerging.

Ultimately, the use of algorithmic governance to rationalize surveillance directly contradicted and undermined Obama's transparency rhetoric. After defending government surveillance, Obama invoked transparency as essential for preventing any further abuses. However, this was an empty claim. While Obama outlined a plan that included more transparency, there was no explanation about how the government was going to be more open. It was just a series of vague statements that the government

should be more transparent and that the President planned to work with the Attorney General and other officials to review what data should be declassified to the public. Even if there was an attempt for the government to become more transparent, it was always a retroactive transparency telling the public what had happened afterwards rather than an open democratic releasing of information. Moreover, this retroactive transparency prevented the public from having an informed discussion to determine what forms of surveillance were acceptable. In the case of the Department of Justice White Papers, the public was provided the legal interpretation that authorized the government to conduct a drone strike against an American citizen who was considered a high-ranking al Qaeda official. However, the public did not get to debate about the merits of whether our government should be able to kill American citizens who were located on foreign soil; instead, the public was simply informed on how it was legally justified. In the case of the National Security Letters, citizens were not provided the opportunity to discuss whether corporations should be allowed to release their personal information to the government without their knowledge; instead, they were retroactively provided information that they were previously denied. As a result, transparency worked as a value that encouraged citizens to be open to companies and the government, yet shielded those in power by allowing them to provide status updates about what was occurring rather than actual openness.

Conclusion

In 2014, CNN's Brian Stelter interviewed Obama's White House Press Secretary Josh Earnest about the topic of transparency. Earnest argued that the Obama

administration was the most transparent government in history. Stelter responded saying, "I'm surprised you still say that line, the most transparent president in history" (Stelter & Earnest, 2014). Earnest never backed down; instead, he maintained that Obama's record of transparency was better than any of his predecessors. As Obama intensified the war on terror from an external conflict into a fight against domestic radicalization, government openness became an integral component in detecting elements that threatened the public. To protect American citizens from the contagion of domestic radicalization, Obama used transparency as a rhetorical trope to encourage citizens to actively participate and become open to surveillance both horizontally and vertically.

As Virilio (2000) suggested, in the age of modern warfare, endo-colonization created the conditions for a permanent war that turned inward to oppress a nation's citizens. The differences between Bush and Obama's rhetoric about domestic terrorism highlighted this very problem. For the Bush administration, homegrown terrorists were a concern; however, the far greater fear was that of foreign agents attacking U.S targets. Thus, while the Bush administration certainly suppressed civil liberties with its expanded executive powers granted by the PATROIT Act and the 2001 Authorization for Use of Military Force, the risk of homegrown terrorism was not a high priority concern. For example, created by the Clinton administration in response to the 1995 Oklahoma City bombing, the first Justice Department domestic terrorism taskforce was scheduled to meet on September 11, 2001 and was cancelled due to the events of that day. However, the Bush administration never rescheduled or used the task force as its attention turned to fighting terrorism abroad (Johnson, 2014).

In comparison, President Obama recognized that Bush's Long War approach could not be sustained and sought to alter and intensify American exceptionalism in order to improve the nation's global reputation. However, in Obama's re-articulation of the war on terror, the war transformed into a biopolitical management of different performances of citizen subjectivity. Because radical ideology could be performed by anyone, the privileges and rights provided by citizenship were conditioned on a subject performing within the approved bounds of a liberal-democratic subjectivity. If a subject performed outside these boundaries, according to the logic of the Obama administration, it became a potential citizen-terrorist who could be eliminated in order to preserve the welfare of the population at large to maintain the homeostatic balance of the security state. In other words, the potentially contagious public needed to be suppressed and attacked in order to protect itself. Once performance as a citizen became the marker of who constituted a domestic terrorist threat, it was an easy step for the Administration to use advanced war techniques like "signature strikes" that select targets who engage in a range of behaviors that have been identified as likely terrorist activities rather identifying a specific person to target. Additionally, this discourse justified the targeted killing of American citizens, such as Abdulrahman, Anwar al-Awlaki, and Samir Kahn. As the Obama administration's drone strikes on citizen-terrorists demonstrated, endo-colonization became the rhetorical means by which the Administration made visible and marked for death all manner of bodies—citizen or non-citizen—through targeted decisions based either on algorithmic calculation of terrorist performance or from official government declaration.

While, Obama interpellated algorithmic citizens as interactive participants in the war on terror, the response by citizens, especially whistleblowers, demonstrate how citizens can identify with the subject formulation of algorithmic citizenship in a way formulates a radically democratic subjectivity. For instance, the ability for a few citizens to uncover classified information and leak it to the public was a logical extension of Obama's campaign promises of creating a transparent administration that released its policy documents so the public could openly debate the legislations' merits. The President's declaration of becoming the most transparent administration in history served as an invitation for citizens to communicate and connect with one another, to inform themselves about the process of government, openly debate, and mobilize together to take collective action. In other words, the same strategy of government 2.0 and transparency that Obama advocated and used to get elected contains within it a democratic potential for civic agency. This civic energy is not one that can be harnessed and controlled by the policy making elite but instead a radically democratic polity where citizens can directly contribute in the act of governing and being governed.

Chapter 5 takes up algorithmic citizenship's potential for democratic agency. Chapter 2 explored how Bush relied on the rhetoric of secrecy to squash dissent and govern the population. In response to this strategy of secrecy, Chapters 3 and 4 examine how both the private sector and the incumbent presidential administration appropriate transparency rhetoric alongside governmentality through government 2.0 discourse. The focus on the previous chapters mapped how government 2.0 operated to control and regulate citizens through the use of big data and surveillance. Altering the focus, Chapter

5 argues that algorithmic citizenship does not necessarily have to be a repressive mode of subjectivity but instead offers citizens political agency. Returning to the questions that guide the research, Chapter 5 demonstrates how algorithmic citizens use collaboration, openness, and transparency in order to inform themselves, interactively engage each other, and mobilize together to take political action.

CHAPTER 5: ALGORITHMIC CITIZENSHIP AND THE RHETORIC OF GOVERNMENT 2.0

Algorithmic citizenship articulated identity with digital data and, as such, it has the possibility to reorient citizenship away from traditional modes of *jus sanguinis* or *jus soli* towards more fluid and malleable mode based in communication. John Cheney-Lippold (2011) defined the new algorithmic identity as:

> …an identity formation that works through mathematical algorithms to infer categories of identity on otherwise anonymous beings. It uses statistical commonality models to determine one's gender, class, or race in an automatic manner at the same time as it defines the actual meaning of gender, class, or race themselves. Ultimately, it moves the practice of identification into an entire digital, and thus measureable, plane. (165)

Although the new algorithmic identity that Cheney-Lippold discussed was calculable, one's algorithmic citizenship was always in flux, constantly being modified and recalculated depending on the data that one produced. This is because every time someone went online or allowed their bank accounts to be tracked, data was produced based on one's personal activity. The data was used to determine: a person's geographic location, identity, language, and personal interests. Algorithms then sorted the data and used it to determine what advertisements a person should be given, in what language the homepage should be displayed, and whether or not a person was allowed to access specific content (Birdle, n.d.).

Government surveillance agencies could use algorithmic citizenship to determine a person's disposition without the person even being aware of it (Birdle, n.d.). As discussed in Chapter 2, even though government agencies such as the NSA were not allowed to spy on American citizens, they could collect and monitor data and assign a

percentage score to each user to determine if someone's algorithmic citizenship was located outside of the U.S. territory. Because data moves rapidly in an increasingly globalized fashion, it was possible for the government to monitor American citizens who were communicating within the U.S. but whose data moved outside of national territorial boundaries.

Even though algorithmic citizenship provided a loophole for government surveillance, it did not necessarily have to be a repressive system. There was room for agency and postmodern potential in regards to cultivating a citizenship based in difference as opposed to identity. In other words, the ability to negotiate and constantly rework one's digital subjectivity outside of rigid territorializing frameworks such as nationality provided algorithmic citizens new possibilities for agency. For example, the ability to be a global digital citizen meant that a person could occupy a particular physical location while inhabiting a digital profile that existed outside of that place and therefore circumvent a particular nation's laws and regulations. This digital status also allowed a person to constantly recreate their digital identity as they experimented with a process of continual becoming-other. One no longer was confined to a specific gender, race, sex, or national affiliation, as one could communicate and perform in ways that are traditionally foreclosed through metaphysical attachments reducing identity to physical bodily characteristics.

This study provides a materialist map tracing the constitution of algorithmic citizenship and how it was articulated through the rhetoric of collaboration, openness, and transparency. Beginning examining the discourse produced after the terrorist attacks on

September 11, 2001, this project followed the rhetoric of government 2.0 as it circulated through civic, economic, and government discourses. Chapter 1 began with the writings of Tim O'Reilly, noting that he advocated for and theorized about the importance of algorithmic regulation and using data to govern. Next, Chapter 2 analyzed President George W. Bush's counter-terrorism and surveillance discourse, demonstrating how good citizenship was articulated with openness and transparency because data collection had immense political value in the war on terror. Chapter 3 then mapped the economic logic of data as a natural resource and the rhetoric that private businesses employed to persuade consumers into adopting practices of algorithmic citizenship. Using IBM as a case study, Chapter 3 explored how private businesses used dual tropes of fear and fun to encourage the public into adopting communicative subjectivities that actively and willingly captured, disclosed, and shared data. Lastly, Chapter 4 examined President Obama's discourse as he campaigned on the promise to increase government transparency while intensifying government surveillance and warfighting. Obama was able to make these seemingly contradictory moves by applying the logic of algorithmic citizenship and government 2.0 towards the war on terror, incorporating increased reliance on weaponized drones and personalized targeted killings.

As I mapped the rhetoric of algorithmic citizenship in the post-9/11 era, I was guided by three main research questions: What form of citizenship was promoted under government 2.0? How did government 2.0 regulate citizens through the rhetoric of national security? How do citizens enact algorithmic citizenship and government 2.0? The following sections of this chapter take up these questions, highlighting how rhetoric

circulated throughout the logic of government 2.0 and constituted algorithmic citizenship. In answering the first question, I provide the theoretical foundation for how algorithmic citizenship was formulated through the logic of government 2.0. The response to the second question examines the role war on terror discourse played in the transition of government 2.0. Finally, the third answer explores the possibility for agency that exists within algorithmic citizenship.

What form of citizenship is promoted under government 2.0?

Government 2.0 promoted the logic of collaboration, interactivity, openness and transparency to articulate and constitute algorithmic citizenship. This project traced how the attacks on 9/11 helped bring about a transition towards algorithmic citizenship by intensifying surveillance that encouraged citizens to engage in transparent performances and open consumerism so that the data could be collected within a suspicion economy. Citizens were invited to participate in a series of designated affective monitored experiences that were used to construct a data profile of good citizens and potential terrorist subjectivities. By directing citizens to participate in a suspicion economy and provide the immaterial labor of monitoring and reporting on those around them, the post-9/11 world relied on an intensified form of biopolitical governance. Government 2.0 combined the intense surveillance of traditional biopolitics with neoliberal techniques such as outsourcing of labor which, in this case, was the responsibility of maintaining national security.

As Chapter 2 noted, the creation of the citizen-detective who was asked to be ever-vigilant began shortly after 9/11. Former President George W. Bush hailed citizens

to be active participants willing to assist the war on terror through their daily practices. By examining Bush's rhetoric through articulation theory allowed me to expose what actions, attributes, and values constituted a good citizen in the post-9/11 world. My analysis in Chapter 2 noted that the post-9/11 good citizen: accepted delays and inconveniences of tighter security; cooperated with members of law enforcement and intelligence agencies; displayed patience in what will be a long struggle; fought terrorism symbolically through daily practices; participated in and had confidence in the neoliberal economic order; possessed an altruistic and charitable spirit; prayed for and supported those in uniform; remained calm despite being in constant danger; and upheld liberal-democratic-capitalist values. In requesting that citizens perform these tasks and uphold these values, President Bush began to orient the public towards adopting the characteristics and techniques important for the implementation of government 2.0 and algorithmic citizenship.

Bush's constitution of citizenship made three important changes to the nature of the citizen-government relationship. First, the former President created a unified citizenry defined by Judeo-Christian values that stood opposed to an external Islamic enemy. Throughout a number of speeches, Bush drew upon Judeo-Christian values, invoked biblical scriptures, and requested prayer to implicitly conceptualized the war on terror as an ideological battle between external Islamic terrorists and domestic Judeo-Christian Americans. Although he noted on a number of occasions that the war on terror was not directly targeted as Muslims, Bush's rhetoric frequently described Islamic

extremists in ways that revealed who was going to be suspected and targeted as the enemy. For instance, Bush explained that:

> …the enemies of liberty come from different parts of the world, and they take inspiration from different sources. Some are radicalized followers of the Sunni tradition, who swear allegiance to terrorist organizations like al Qaeda. Others are radicalized followers of the Shia tradition, who join groups like Hezbollah and take guidance from state sponsors like Syria and Iran. Still others are "homegrown" terrorists -- fanatics who live quietly in free societies they dream to destroy. Despite their differences, these groups from -- form the outlines of a single movement, a worldwide network of radicals that use terror to kill those who stand in the way of their totalitarian ideology. And the unifying feature of this movement, the link that spans sectarian divisions and local grievances, is the rigid conviction that free societies are a threat to their twisted view of Islam. (WH, OPS 2006, August 31, para. 15)

Not only does this description of the enemy clearly demarcate Islamic groups as the "enemies of liberty," but it also re-inscribed the classic divide between external/internal security. In Bush's rhetoric, enemies existed outside the U.S. In comparison, U.S. citizens were uniformly cast as on the side of liberty.

Second, citizens were asked to provide immaterial labor for the new security state and to actively participate in the fight against terrorism. For example, citizens were called on to provide their immaterial labor to be suspicious and vigilant by reporting on other people and engage in performances of transparency within a culture of suspicion. But beyond simply remaining watchful, citizens were told by the Bush administration how they could directly participate in the fight against terrorism. Bush sets up the war on terror through a neoliberal framework, where citizens are asked to take it upon themselves to help in the relief efforts and the upcoming war on terror. For instance, citizens were encouraged to engage in acts of consumerism to both help the economy and offer data mined later to identify terrorist dispositions.

An additional rhetoric tactic used to actively deploy citizens in the fight against terrorism, Bush called for civic participation and volunteerism. The seemingly benign calls for citizens to continue their daily lives and participate in the economy carried with them provided immaterial labor for the state. According to Bush, "as government works to better secure our homeland, America will continue to depend on the eyes and ears of alert citizens" (WH, OPS, 2002, January 29, para. 32). To be ever alert, citizens were asked to join organizations such as the Freedom Corps and Neighborhood Watch and report to the TIPS programs. According to Bush, the attacks of 9/11 served as a reminder to the nation that citizenship was an obligation to each other, our country, and our history (WH, OPS, 2002, January 29). In this sense, good citizenship requires citizens to actively participate through joining the military, providing the immaterial labor through transparent performances and through reporting on suspected threats, volunteering in charitable organizations. Ultimately, this call for citizens to serve became a rhetorical strategy for interpellating good citizen-soldiers.

Third, citizens were called on to trust government surveillance and security programs. For instance, the Bush administration asked citizens to willingly submit to government surveillance programs and to be patient and accept increased security at airports and other institutions. In order to accept these programs, Bush invited citizens to adopt an emotional state such as patience so that they would accept surveillance without anger or dissent at the inconveniences that security might impose on daily life. However, if citizens dissented to increased surveillance or publicly challenge the war on terror, they were accused of being personally responsible for the loss of lives that could have been

prevented had they just trusted the government's national security efforts. This request for patient acceptance of surveillance and security extended the logic of government 2.0 because it operated according to an asymmetrical epistemic foundation where information was seen as a national asset. This resulted in a form of governance where Bush bypasses dissent and objective because his information about terrorist threats and the need for security came from sources that were more informed than the public's information. By collecting and controlling all security data, Bush was able to govern through a process of algorithmic regulation that mined data and used it to statistically construct terrorist profiles that needed to be identified from normal communication behaviors. The result was that the traditional values of democracy became inverted, where the government's work was secret and the daily lives of citizens became transparent.

President Bush was successful in using the fear of terrorism to garner citizens' energies into actively supporting government surveillance and participating in counter-terrorism programs. However, as Chapter 3 indicated, the public willingly participated in regimes of surveillance long before there was any controversy surrounding government surveillance. As government officials quickly noted, private companies had been collecting consumer data and selling it to advertising companies for quite some time. Yet, despite the severity of corporate surveillance, citizens were not up protesting this intrusion into their personal lives. Additionally, after the public learned about mass surveillance through the Snowden files and Wikileaks, companies like Facebook, Google, and Twitter did not face backlash from angry consumers deleting their accounts. So what

rhetorical strategies did private businesses use to gain public support in such ways and how did this then aid government surveillance?

To answer this question, Chapter 3 examined IBM as a case study to see how the company encouraged citizens to willingly participate in data sharing and surveillance. The analysis indicated that private companies supplemented public fear of issues related to crime and terrorism with the excitement, entertainment, and fun of connecting with others via social media. In other words, private companies created a sharing economy in which data was shared in an open and transparent manner because it was a fun method of connecting with others and establishing community. These acts with private companies served the discourse of government 2.0 well, as it invited citizens to identify and adopt the subjectivity of algorithmic citizens; members of an open and transparent data community who collaborated and shared information for the purposes of governing society and solving societal problems.

One of the most prominent displays of algorithmic citizenship and government 2.0 was IBM's THINK exhibit. To legitimize and normalize the use of data to regulate society, IBM created a 7500-square-foot interactive popup in the heart of New York City as part of the company's centennial celebration. Later, IBM opened an IBM THINK exhibit in Chicago's Museum of Science and Industry and Disney's Epcot Center. The exhibit exemplified how private businesses promoted algorithmic citizenship by encouraging people to interactively participate in public activities that turned data collection and sharing into entertainment. For example, educational and exciting activities, such as going to a community gathering, museum, or public exhibit became a

social site where people were educated about the importance of data in resolving society's problems while simultaneously internalizing and naturalizing systems of mass surveillance.

IBM's discursive strategy for promoting government 2.0 and its form of algorithmic citizenship was presented to several audiences. In its campaign to governments, IBM emphasized how globalization and technology were bringing the world's governments closer together. Because the world was shrinking due to new technologies, government 2.0 provided countries with the ability to communicate and share information in unprecedented ways. For instance, governments were encouraged to purchase IBM products and services that helped governments collaborate together. Further, IBM was able to provide services that allowed governments to directly communicate to their own citizens, providing the same type of 24-hour service that consumers expected from the private sector. Data sharing was marketed as helping governments connect to one another to address major issues such as climate change, disease pandemics, immigration, and terrorism. IBM also demonstrated the strategic value of openness and transparency. By contending that data was the next valuable resource, IBM worked to extract that value by persuading the public that it was in its best interest to share. Simultaneously, the company assisted government surveillance programs that were publicly contentious yet rationalized as essential to promote the values of government 2.0 and an interactive sharing culture.

When addressing citizens and customers, IBM stressed the importance of data as a natural phenomenon that is essential for human progress. For example, the Think

Exhibit allowed citizens to attend centennial public celebrations, stroll through a science museum, work on a school educational project, all while enjoying a fun and interactive process of participating in data collection that was used to govern their lives. Because some of the events were free and occurred in public spaces, the entertainment function of the campaign worked to encourage people to share their data and participate in transparent performances of citizenship. For instance, in New York, the Think Exhibit was just a temporary and free pop-up helped to normalize data collection as an entertaining process. Despite their entertainment value, the IBM exhibits and campaigns used the interactive nature of data sharing to legitimize and naturalize the process of intense surveillance that records communication and everyday activity. The same process of surveillance used to help individuals locate parking in one city was the same practice that private businesses used to personalize advertising and governments used for crime prevention and counter-terrorism. However, it was presented by companies like IBM as being part of the exciting and normal nature of human progress.

In Chapter 4, I note how President Obama's rhetoric combined his predecessor's culture of suspicion with the interactive fun of data collection to finalize the transition to government 2.0 and algorithmic citizenship. The President accomplished this in several ways. First, the Obama administration promoted the idea that citizens have political agency when they participate in interactive and transparent forms of government. For instance, according to Obama's arguments, the secretive nature of classifying information and the level of acquiescent rhetoric typically exemplified through citizen-government relations dissolve as citizens were provided a venue for analyzing government legislation

before it passed and having the ability to directly communicate grievances with government officials. Instead of having to write a letter to their representatives, citizens could send a quick email or communicate with an elected official through an interactive forum.

Second, the Obama administration argued that government 2.0 would create a better informed citizenry that was able to read legislation before it was passed and note any influence from special interest groups. While government 2.0 was supposed to resolve the problems of secrecy and excessive corporate and special interest influence, the implementation of these open and transparent policies dud not translate very well into practice. For example, the Patient Protection and Affordable Care Act (PPACA) and the Health Care and Education Reconciliation Act (HCERA) included 381,517 words. On top of that, the Obama administration published 11,588,500 words about final Obamacare regulations (Star, 2013). The amount of additional reading resulted in over 10,535 pages of text averaging 1100 words per page. Despite conservative criticism about the length of the healthcare bill, one thousand page bills are quite normal, especially with spending bills. For instance, in 2009, the stimulus bill was 1100 pages and the climate bill was 1200 pages (Beam, 2009). Thus, just to review these three large pieces of legislation, the public would be responsible for reading over a thousand pages to make an informed decision. Even if citizens had the ability, desire, and time to read through the entire text of these pieces of legislation, it would be impossible for them to wade through every single policy in the five-day grace period allotted on the government webpage.

More importantly, the problem with the President's transparency rhetoric is that it created an illusion that the government was open but made it highly unlikely that citizens will do so. This allowed Obama to claim that he was one of the most transparent presidents in history while, at the same time, he intensified government surveillance and warfighting techniques that used opaque decision making to determine what constituted suspicious activity or who were militants. These classified and closed decisions were enabled by presidential definitions that determined behaviors and dispositions that defined who was a threat and what counted as civilian or militant causalities.

The significant increase in weaponized drone strikes and the secretive nature in which they were carried out exposed the dangerous side of algorithmic citizenship. Whereas the Bush Administration would collect data on citizens to determine dispositions that were a threat to national security, the Obama administration used this data to determine whether a data profile constitutes a material threat that warranted execution. Therefore, President Obama's concentrated effort to apply the personalized logic of government 2.0 to the war on terror resulted in a shift in how government surveillance operated. Coupled with the concern about contagious ideologies and speech, terrorists were no longer seen as external enemies who could be contained or eliminated at a distance. Instead, government surveillance had shifted to define, predict, and eliminate homegrown extremists who were radicalized and presented significant threat to the country. The enemy construction resulted in the government increasing domestic surveillance in order to curtail terrorism and to best preserve national security.

Communication and rhetorical theorists have done excellent work pointing out the ways that consumerism is positioned alongside citizenship to either support the war or to identify with the trope of the citizen-soldier. Consumerism rhetoric is typically depicted as an asymmetrical force used by those in power to manipulate or pacify the common citizen. Krebs (2006) points to the citizen-soldier trope as a concept that contends that in order to be a good citizen that all military age males make the sacrifice of joining the military and fighting for their country. However, those where were rich enough would be able to make the sacrifice of paying someone else to take their place (Krebs, 2006). Rhetorical scholars such as Engels and Sass (2013) expose the way that consumerism is rhetorically deployed as a means to distract and pacify the public into acquiescing in support of war. McAlister (2010) demonstrates how popular media uses shows such as Extreme Home Makeover to persuade the public that acts of consumerism are a citizen's civic duty that can help show support for the war effort. Stahl (2010) labels the rhetorical articulation of the military/sports/entertainment complex militainment. While all of these theorists do very important work, they all depict consumerism as something that the masses are duped into or distracted by. Using rhetorical materialism allows for an alternative theorization that takes these criticisms into account while also examining the interactive way that consumerism operates under algorithmic citizenship.

Articulation theory allows for a mapping of the complex and contradictory relations between consumerism and citizenship. Grossberg (1992) explains that articulation links and de-links the construction of sets of relations. The connecting and

disconnecting of sets of relations and practices can be altered through the production of context. Context is conceptualized as a structured field or the set of practices and relations located in specific configurations (Grossberg, 1992). Rhetorical materialists work by mapping the articulations as they occur in any specific assemblage. The analysis takes into account the specific contexts and the articulations produced in order to analyze the effectivity in which articulations penetrate and affect reality (Grossberg, 1992). The effectivity is not something that operates through the logic of influence or causality, but rather is complex and works in different co-constitutive ways back and forth upon one another.

Sloop (2009) explains that rhetorical materialism conceptualizes rhetoric as "the energy or flow mediating between bodies, body prosthetics, and "semiotic conditions." This becomes a better conceptualization for rhetoric in that it side steps the debate between the relationship between rhetoric and materiality and instead approaches rhetorical materialism as an active project "which we understand that any time one attempts to talk about bodies and subjectivity, one is always already involved in the process of re-shaping the flow of mediation, the flow of meaning" (Sloop, 2009, p. 70). Using a slightly different vocabulary Johnson (2008) writes that "meaning and subjectivity both become articulated as contingent effects of discursive arrangement" (p. 32). The world is conceived of as a series of flows that constitute subjects and objects as they connect and disconnect in relation to speed. So a rhetorical critic maps how these flows constitute modes of subjectivity that positions elements in relation to one another. The rhetorical critic directly participates in materiality in the sense that they directly

engage the "macro-structures of power" that are distributed, activated and programmed by rhetorical practices for the purpose of policing a population (Greene, 1998).

Algorithmic citizenship is constituted through the material communicative practices that cannot simply be dismissed as mere consumerism. The personalized nature of government 2.0 and algorithmic regulation means that every time someone performs a web search they are providing data that calculates the information into an algorithm that determines normal from abnormal activity. With every product viewed on a website, a person is participating in the construction of a digital profile that is used to monitor activity and determine a person's preferences and dispositions. Each time someone posts a status on Facebook, Instagram, or Twitter they are both communicating with others, enacting citizenship, and constituting their subjectivity. By producing data, algorithmic citizens are working to constitute new interactive forms of public engagement and civic subjectivity that work to shape themselves but also to construct statistical models that are used to understand and preserve a state of homeostasis as well as predict future activity. Consumerism becomes an interactive process that on one level can serve to distract and pacify the population, yet on another level is an active process that works to shape subjectivity and provide an active process in the act of government. In regards to the latter, algorithmic citizenship becomes a means of monitoring the population's dispositions in order to detect abnormal communication that might pose a material and imminent threat to national security.

How does government 2.0 regulate citizens through the rhetoric of national security?

National security was a rhetorical trope that was commonly used in both corporate marketing and presidential addresses in an attempt to legitimize and rationalize the constitution of algorithmic citizenship. There was the initial claim that surveillance was necessary to maintain both economic and national security. As the American Express commercial analyzed in Chapter 1 indicated, surveillance was rhetorically framed as being essential to monitor and protect people from the threat of crime or harm. The analysis conducted in Chapters 2, 3, and 4 demonstrated the way that national security discourses directed towards external enemies, economic and financial security, and contagious domestic threats were used to legitimize and perpetuate data collection as necessary.

Chapter 2 mapped how the Bush administration used the rhetoric of national security to produce a culture of fear and suspicion. The Administration relied on ethos in cultivating rhetorical strategies that encourage people into adopting particular emotional states. For instance, Bush invoked fear by producing apocalyptic scenarios to scare members of the media or public into acquiescing to the administrations demands and national security policies such as increased surveillance and war. This was evidenced in Bush's post-9/11 State of the Union speech that depicted Saddam Hussein as an evil ruler who had to be stopped before he acquired and unleash weapons of mass destruction on the world. Further, Bush used the same apocalyptic scenarios to dissuade the *New York Times* from reporting on the increased surveillance programs implemented after 9/11, claiming that if the *Times* released the story, it would be responsible for the next terrorist attack.

National security discourses also worked to sow sentiments of distrust. By invoking an enemy that had no physical location—it was a war against a state of terror, not terrorism—and was capable of striking anywhere at any time, Bush was able to cultivate a culture of suspicion. Within this culture, citizens were asked to be vigilant and if they ever felt uneasy or witnessed something suspicious, then they were asked to communicate that threat to authorities. Thus, this logic of national security rationalized extreme forms of government intrusion into citizen's private lives under guise of national security. A secondary function of national security rhetoric was to outsource a great deal of the labor of maintaining security onto citizens. To this effect, citizens were encouraged to openly submit to government surveillance while taking it on themselves to actively surveil others.

Finally, while national security worked to render citizens transparent, this discourse became the rhetorical justification for the government to shroud the way that it conducted the war on terror from the public. As citizens became more open, national security made government information opaque. In order to best protect citizens, President Bush decided that he would not publicly announce how the US planned to conduct the war on terror so as not to alert the enemy. Much like the World War II logic that, "loose lips sink ships," the Bush administration argued that it was essential to conduct the war on terror in secrecy in order to protect the democratic values of openness and transparency. This allowed the government to conduct a largely secret war on terror that was not subjected to an open and democratic public debate.

Maybe because there was a lack of public debate regarding mass surveillance, it seems as though the American people have accepted and naturalized living in a world of constant surveillance. As the analysis of the American Express commercial from Chapter 1 indicated, surveillance worked to promote a feeling of security. These regimes of surveillance worked so well in fact that private businesses had to find new ways to persuade the public that they were insecure. This caused corporations to ask the question: while people's personal property and physical presence may be monitored by external surveillance through such means as security cameras and police officers, who should be watching the most valuable national resource of all: data? The answer is a combination of corporations and the government. Chapter 3 demonstrated the economic logic contained within national security rhetoric. Specifically, data was constituted as a national resource that must be collected, sorted, and monitored in order to most efficiently and securely govern.

IBM went to great lengths in advancing a rhetorical campaign that emphasized the importance of mapping and managing data in order to algorithmically regulate society and promote human progress. Algorithmic regulation intensified national security rhetoric by magnifying risk and using statistical analysis to attempt to predict and prevent threats before they occurred. For example, data could be used to analyze and predict crime patterns, terrorist activity, and enemy actions. The predictive nature of data collection worked alongside national security rhetoric to vindicate constant surveillance and data gathering in order to monitor the health and wellbeing of the population while preventing security threats from occurring.

To market data as a national resource, IBM relied on advancing government 2.0 and transparency rhetoric to promote national security. For instance, while IBM denounced the government's ability to coerce private businesses into releasing consumer data, the company very openly marketed itself as collaborating on data collecting technologies that were used by law enforcement and the military for national security matters. Part of IBM's strategy of building a smarter planet was to bring the advanced uses of predictive technologies seen in the 2002 Tom Cruz film *Minority Report* from fiction to reality. To this end, IBM worked to establish and market the practices of monitoring social media, predictive policing, and military programs such as the Human Terrain project. Each of these projects operated to monitor consumer data to detect aberrant communications in order to create a more secure world.

As the analysis in Chapter 4 noted, President Obama built on and intensified the national security rhetoric of his predecessor and IBM. In regards to President Bush, Obama extended the same sentiment that terrorism was the primary threat facing the U.S. However, Obama distanced himself from some of the Bush administration's more unpopular policies such as enhanced interrogation and the use of indefinite detention of prisoners at Guantanamo Bay. However, without the ability to capture and torture detainees in black sites or imprison new suspects in Guantanamo Bay, the Obama administration had to determine a new warfighting strategy that did not rely on these unpopular practices. The result was an increased reliance on drones and personalized warfighting.

To carry out the war on terror, Obama continued the mass surveillance programs implemented by the Bush administration, intensified kill lists, and increased the use of armed drones. Because capturing enemies was a politically contentious issue or difficult to battlefield geography, the Obama administration often resorted to lethal drone strikes to resolve this dilemma. Presidential definition played a vital role in normalizing drone strikes, especially in regards to legally justifying the program. When speaking to the public, Obama celebrated drones as being vital to the protection of national security in a manner that was ethical, legal, and, most importantly, consistent with American values. Yet, analysis of Obama's drone discourse demonstrated that the President drew upon national security rhetoric to strategically transition towards algorithmic warfare.

Another effect of national security rhetoric is that it positions the president and national security operators as exceptional compared to the public. This exceptional discourse is complex and often contradictory. On one level, the President and the national security operators are exceptional because they are average people, who dedicate their lives to keeping the general public secure. On another level, they are exceptional because their status makes them privy to information that the general public is not afforded. Then on a third level, they are exceptional in that they are the exception that proves the rule. In that they are clandestine operators that have little to no judicial or congressional oversight, in many cases answering only to the President. These workers are then assigned operations that potentially allow for them to operate outside of the law in order to preserve the security of the nation.

The use of presidential definition, especially in regards to national security, became a powerful rhetorical strategy that determined what bodies mattered, which could be marked for death, and how we discussed those deaths. The Obama administration formulated kill lists that relied on national security policies such as the AUMF and an expanded definition of immanence in order to provide the President with the authority to authorize which bodies could be killed. Further, President Obama expanded the definition of a militant to include any military age male. This definition provided the government with a legal cloak when carrying out signature strikes because those who were killed could be labelled militants and were thus considered enemy combatants. The ability to strategically and posthumously define the dead as militants rather than civilians or even unknown people demonstrated that the government had the power to declare what bodies mattered. For example, if people die and the headline in the paper the next day read, "15 Militants Dead," the public is led to believe that the U.S. launched a strike killing several enemy forces; the people that were killed do not matter because they were enemy forces who deserved to die. This is a completely different persuasive appeal than explaining the same type of drone strike as killing at least fifteen people, some or most of whom were civilians.

Using national security rhetoric to strategically define the enemy was shaped by the logic of endo-colonization and had serious implications in regards to the rights and privileges afforded by citizenship. After the Obama administration ordered the successful mission to kill bin Laden, the government had to find a new way of persuading the public that the war on terror was still important. To this extent, Obama began to

redefine the terrorism threat as operating at the level of ideology. This new conceptualization of terrorism reoriented the public away from a fear of external enemies and towards the domestic radical or homegrown extremists. As a result, the war on terror had to be fought not just on the military terrain but also on discursive, ideological, and performative levels.

The logic of endo-colonization produced two consequences. First, as the case of Anwar al-Awlaki demonstrated, citizens who engaged in aberrant speech, ideology, and performance had the privileges of citizenship revoked in the name of preserving national security. For instance, the legal memorandums regarding Awlaki indicated that a citizen's right to due process can be voided if the government decided that the person presented an imminent threat to the nation's security. While Awlaki might represent an extreme case, national security rhetoric still had implications beyond this one instance. It also operated as a legal rationalization for algorithmic monitoring and government surveillance of citizens' communications. If the government had reason to believe that an individual was communicating with a terrorist or even has social connections to someone in a terrorist network, those communications were monitored, sorted, and analyzed for the purposes of national security.

Second, as the analysis of the Bush administration, IBM, and the Obama administration indicated, national security rhetoric interpellated citizens by inviting them to adopt one or hybrid combinations of three specific subjectivities. As Chapter 2 noted, the Bush administration hailed citizens to become citizen-detectives and citizen-soldiers, as people were asked to be vigilant and on the lookout for suspicious behavior. If that

behavior was identified, the good citizen was asked to take action by either reporting it to proper authorities or, as was the case with the "underwear bomber" Umar Farouk Abdulmutallab or the passengers on Flight 93 in 2001, take direct action. Chapter 3 revealed how IBM used government 2.0 and transparency rhetoric to call forth a citizen-consumer subjectivity. The delineation between the two subjectivities was blurred as people were able to use banal communications and everyday consumer activity for the purposes of civic engagement and social mobilization. The Obama administration built upon the two previous interpellations, as Chapter 4 demonstrated, in developing a profile of the citizen-terrorist who was infected by a radical ideology and must be identified and eliminated for the purposes of national security. While the identification of the citizen-terrorist exposed the intensification and resurgence of repressive forms of control such as increased surveillance and disciplinary power, the interactive aspects of the citizen-consumer subjectivity provided potential agency for citizens to engage in and enable their own subjugation. Additionally, this interactive agency also gave people ineffective political access and input that was historically limited to representative control and submission to being governed.

National security discourse develops alongside the logic of government 2.0 in order to constitute an alternative conception of the citizen-soldier than is typically theorized in communication studies. Krebs (2009) contends that the citizen-soldier was a rhetorical trope that encompassed a form of citizenship where military age males were obligated by civic duty to join the armed forces. Stahl (2006) expands the a definition of the citizen-soldier to encompass the virtual aspects such as wiring oneself into a video-

game world that submerses the participant in fantasy war scenarios. Biesecker (2007) explores how national security discourse works to produce a dematerialized aesthetic, where citizens are asked to doubt their own beliefs, while adhering to a culture of suspicion that sees terror everywhere and thus marks everyone as suspicious. While all of these articulations of the citizen-soldier are accurate, they do not speak to the way that algorithmic citizenship operates on a global level to sort data into statistical profiles that demarcate bodies as good citizens or citizen-terrorists.

The development in the logic of government 2.0 explains some of the substantial differences between the war rhetoric of the George W. Bush and Obama Administrations. These dissimilarities lie in how each president constitutes the nature of citizenship and warfare. Few presidential scholars have studied Obama's war discourse and fewer yet have examined how his conceptions of citizenship intersect with his foreign policy in ways that justify the targeted killing of U.S. citizens. This dissertation argues that when one juxtaposes Obama's notions of citizenship with his war rhetoric, it reveals that his proscribed norms for the performance of citizenship are the cornerstone of his justifications for the targeted killing of American citizens. Thus, while some war discourse scholars such as Jeremy Engels and William Sass (2013) view Obama's foreign policy rhetoric as a mere extension of Bush's discourse, I contend that Obama's rhetoric may represent a fundamental shift in presidential war discourse that reshapes how we conceptualize citizenship and allows for the potential expansion of presidential war powers to include the targeting of American citizens without due process. Far from acquiescing to this war rhetoric, my contention is that U.S. citizens, through their

performances of citizenship, are interactive participants in an internal colonization or endocolonial production of citizen-soldiers and citizen-terrorist subjects.

While the majority of this dissertation has theorized that the rhetorical constitution of algorithmic citizenship is troubling, there remains the possibility for agency within the ideological hail of the surveillance state. The next section of this chapter examines how algorithmic citizenship and government 2.0 have transformative political potential capable of providing citizens with alternative modes of enacting citizenship. In examining agency, the next section will be divided into two parts: the first examines how citizens can apply articulation theory to the value of collaboration and interactivity to connect people in decentralized nonhierarchical networks; the second part follows the rhetorical tropes of openness and transparency as they pertain to algorithmic citizenship. More specifically, the second part explores how algorithmic citizenship destabilizes traditional understandings of identity and nationalism by promoting a constantly shifting global subjectivity. Taking seriously Jean-François Lyotard's writings on open information, I examine the democratic potential that exists within the values of openness and transparency through acts like whistleblowing.

How does the public enact algorithmic citizenship and participate in government 2.0?

Algorithmic citizenship and government 2.0 discourses constitute collaborative, interactive, tech-savvy, and transparent subjectivities. The majority of this project has examined the way that the government interpellated this form of subjectivity in order to govern the population. However, subjectivities within this ideological constitution were

not passively duped by governing forces. Rather, the algorithmic subjectivity is an interactive process in which citizens are afforded visibility and communicative possibility in new modes of public engagement. A review of the project's materialist mapping of collaboration, openness, and transparency rhetoric demonstrate how this agency was made possible.

Collaboration. One of the primary drivers of algorithmic citizenship was collaboration discourse. Algorithmic citizens were not restricted by physical boundaries or traditional forms of identity. A person could use digital technologies to connect with others while having a subjectivity that was in constant influx. The rhetorical force of collaboration was exemplified through articulation theory. As Lawrence Grossberg (1992) explains, articulation is the mapping of identity onto difference. Through articulation, rhetoric mobilizes and connects various elements, fragments, ideologies, tactics, and strategies into constituted subjectivities (DeLuca, 1999). Thus, articulation is a continuous struggle to reposition practices within a shifting field of forces. It constantly redefines the possibilities of life by reworking the field of relations in the context within a practice is located (Grossberg, 1992).

Because data profiles were used to determine material subjectivities, it was possible for citizens to use these profiles to circumvent geographic restrictions and regulations. For instance, citizens could use a Virtual Private Network to send data from a remote location without having to physically be in that country. This allowed people who were physically located in China to access the Internet without being restricted by China's firewall because their algorithmic citizenship was producing data from another

country. Because data was appearing at a particular place, the Internet treats people as if they were actually in that place (Birdle, n.d.). By performing these actions, algorithmic citizens could evade some of the rules and regulations that might apply to them.

Further, understanding algorithmic citizenship as articulation allows for collaboration and collective action among disparate groups. DeLuca (1999) discusses how new social movements can formulate alternative collectivities based upon re-articulations of various terms. Additionally, collectivity can occur as several individuals and groups come together by articulating linkages with groups that have been affected by surveillance or denied political access. Take for instance WikiLeaks, a non-state organization comprised of various individuals and groups such as citizens, journalists, NSA workers, and soldiers, all of whom can form alliances and build solidarity with legal groups such as the ACLU, privacy advocates, and other social movement groups who are fighting against globalization, imperialism, racial profiling, and war. These disparate groups can forge connections utilizing a vast array of rhetorical tactics that can transform their particular struggles into a broad-based challenge to the existing assemblage of power. Drawing upon Laclau and Mouffe's (1985) theory of articulation, Lindgren and Lundstrom (2011) conceptualize WikiLeaks as a networked public, "a participatory and collaborative environment where technology and tactics are used and developed, where interests are shared, where meanings are appropriated, re-made and re-distributed and where enthusiasts and volunteers create something together." Those who used the #WikiLeaks could be conceptualized as being part of a social movement even though they were disparate individuals who were participating on a social media sites (Lindgren

and Lundstrom, 2011). The use of the #WikiLeaks by users then became a bottom-up grassroots form of politics and resistance against corporate media. It exposed how social media has the potential to be a primary site of algorithmic resistance through tactics such as adbusting, culture jamming and hactivism that united various 'faceless" individuals (Lindgren and Lundstrom, 2011).

Digital technologies can also be appropriated for the purposes of collaborative protest. FireChat, for example, is a product that was designed for people to communicate without an Internet connection through their phones' Bluetooth and Wi-Fi signals to connect with other devices. The application's original purpose, however, was to allow festival goers to connect and communicate while at events such as Burning Man (Toor, 2014). Yet, protesters in Hong Kong and Taiwan used the application as a precaution against the threat that the government might shut off the Internet. Therefore, Firechat allowed protesters to communicate and collaborate, with each phone acting as an individual node that connected with other users. As more users connected with each other, the network's range expanded (Toor, 2014). Thus, the more people that collaborated, the more powerful the communication network became.

Overall, through algorithmic rhetoric and subjectivities and collaborative digital technologies, algorithmic citizens can use collaboration and interactivity to connect to, organize, and disperse from networks into anonymity if so desired. The ability for citizens to communicate and take collective action and protest demonstrates some of the civic power of collective digital engagement. The next subsection extends this discussion of agency by examining how openness and transparency rhetoric can be used by citizens

for the purposes of sousveillance and generating exposure and debate. The subsection begins with a brief review of Lyotard's writings about surveillance and the strategy of complete openness as a response to corporate privatization. Moving from Lyotard, I then map the rhetoric of openness and transparency in relation to modern whistleblowing in the cases of Edward Snowden and Wikileaks. These cases reveal an algorithmic strategy of sousveillance as a political response that reverses the traditional seer/seen binary on which government surveillance resides.

Openness and Transparency. In 1979, Jean-François Lyotard was proleptically writing about the information age, surveillance society, and their implications regarding who had access and control over information. Most importantly for this project, he noted that, "In the computer age, the question of knowledge is now more than ever a question of government" (Lyotard, 1984, p. 9). Lyotard theorized that the nation-state would be instrumental in employing science to promote knowledge of technological production. As was demonstrated in Chapters 3 and 4, Lyotard's predictions were quite accurate, especially in regards to government 2.0. Both Presidents Bush and Obama and officials for IBM highlighted the importance of using data and information to govern and regulate society. For instance, President Obama recently called for a partnership between the government and IBM to advance STEM education and technological production (WH, OPS, 2013, January 12).

Corporation partnerships that enabled the privatization of knowledge was what concerned Lyotard. One of his specific apprehensions was that corporations might have the potential to gain access to the Earth's orbital space which in turn could create the

possibility to privatize and control who can access that information (Lyotard, 1984). This concern has proven to be true as private businesses now claim ownership of satellites and surveillance technologies and offer services such as Google Earth or satellite radio and television. Moreover, a few major media corporations have purchased their competitors to consolidate control over information and means of communication.

Lyotard (1984) also worried that data would become a commercial and social commodity that could limit people's access to information. In order to get information, people must pay for access. For example, access to cellular networks and the Internet and much of their content requires people to purchase subscriptions. Even services like Google Earth, which advertises to consumers that it is free to download and use stipulates that the consumer must have access to an Internet connection and a device to use it. These access requirements in turn transforms knowledge into an informational commodity that provides its possessor with a stake in power. As Chapter 3 and 4 have noted, data has quickly become a national resource. As a commodity, there became a demand for analysis of patterns and trends that arise from large-scale data. Hence, the need for Big Data was born. However, the quantity of Big Data required substantial amount of automated data collection and storage. The question that Lyotard would pose is: who will have access to the stored information? His answer was that the ruling class comprised of technological experts will be the ones who have data access and are able to profit from it (Lyotard, 1984).

For Lyotard, the people who control the access to information are able to dictate the framework of reality. Reality is the evidence used as scientific argumentation proof

and ethical, juridical, and political prescriptions and promises (Lyotard, 1984). Through privatizing data, corporations can use algorithms, data collection, and surveillance to control the framing and representation of reality. For example, surveillance technologies reinforce what reality is by recording it into a knowable system of data accumulation. Once collected, the data is sorted and used to create an algorithm that provides a framework for the public's epistemological foundation. Lyotard (1984) argued that technology is reinforced more effectively if one has access to scientific knowledge and decision-making authority. If a private business or the state can record one's information in mass and use it to justify law or policy, then it becomes a way of legitimizing the scientific framework for understanding reality. The ultimate form of framing reality comes from the ability to actually record a version of events and play it back retrospectively and claim that it is reality. The illusion of perspective usually seen in movies is now applied to the political in an unquestioned technological mastery of reality (Lyotard, 1984).

In response to the computerization of society and privatization of information, Lyotard (1984) argued that there should be free public access to the data and storage banks of information. If this was made available, neither states nor private businesses would be able to form an epistemic consensus because everyone would have access to information and thus the dominant narrative would be disrupted through dissensus. This would be a politics of justice that does not seek consensus but rather respects the desire for the unknown (Lyotard, 1984). It must be stressed, that the data that becomes available for public consumption must be disruptive. Critics would be correct in pointing

out that the Internet already makes numerous competing narratives readily available. Further, the oversaturation of available information can also result in consumers either being so overloaded with information that they merely rely on the mainstream media to condense information for them or risk entering an informational echo chamber in which an algorithm only produces information that replicates the consumers' interests as opposed to a pluralist engagement with competing facts. It is through this framework, that I seek to advance the disruptive potential of surveillance whistleblowers such as Edward Snowden.

By advancing the figure of the whistleblowers as a potential site for dissensus, I do not mean to glamourize, make a hero out of, or romanticize people such as Edward Snowden or Glen Greenwald. Rather, Snowden's leaking of thousands of government files to *the Guardian* and *Washington Post* demonstrate a specific act in which a NSA employee provided mass information to a media outlet, which in turn, translated the mass amount of information into a series of easily consumable articles that exposed mass government surveillance programs that were otherwise classified for purposes of national security. In this act the media was essential in condensing what would have otherwise potentially been an overload of information to the public that would not have been easily digestible. For instance, if Snowden had just dumped all of the files onto a wiki, then the public would have to read through technical manuals, pages of data, or specialized jargon. Instead, *the Guardian* dedicated a section of their website to decoding the NSA files and explaining to the public in an understandable format what the NSA was doing.

In order to demonstrate how the rhetorical tropes of openness and transparency advocated by Lyotard might operate through algorithmic citizenship, let us examine how whistleblowers rhetorically resist status quo interactive, open, and transparent subjectivities by revealing secret information to the general public. Rather than reproduce the asymmetrical transparent citizens and opaque government relationship, whistleblowers have the ability to expose information in ways that leave the government more transparent and open to the citizenry. To examine how this might be possible, I explore briefly how whistleblowing in the cases of Wikileaks and Snowden's disclosures exposed the inherent contradictions behind the values of collaboration, openness, and transparency of corporate and governmental discourses. By revealing these paradoxes, perhaps it becomes possible for algorithmic citizens to articulate an alternative subjectivity that provides political agency and access to data through the adoption of government 2.0 practices.

Currently, the ability for the government and private businesses to collect consumers' bulk data creates an asymmetrical relationship that privileges elites with access to that information. In this sense, algorithmic citizens participate in the production of data that is used to govern and regulate the population without having equal access to the collected data. Through the act of whistleblowing about government drone policy, kill lists, mass surveillance, and military misconduct, algorithmic citizens are capable of altering the power relations towards a more democratic polity. For example, Snowden (2016, May 3) described the communicative significance of whistleblowing as providing citizens with the information necessary to be critical of government actions and

mobilize to challenge government policy. Put differently, whistleblowing operates to cultivate an empowered and informed citizenry capable of energizing the demos through engaged political debate. This level of informed political participation and dialogue allows for citizens to defend democracy in a way that would previously be foreclosed by the state's ability to classify information and keep it secret.

Additionally, whistleblowers re-appropriate the purpose for the materialization of algorithmic citizens by flipping the subject's vigilance and reporting towards government wrongdoing. As this project has noted, the government used government 2.0 logic and transparency rhetoric to interpellate citizens to identify with specific subjectivities that maintain government surveillance. Yet, the whistleblower subject demonstrates how citizens can identify with this interpellation in a way that inverts the power dynamics that privilege the dominant elite over the people. When citizens perform as transparent and vigilant subjects, they are also capable of using those performances to report abuses of those in positions of privilege and power. For instance, Snowden (2016, May 3) explained the considerable effect that a small number of whistleblowers had over those who govern, stating:

> …those who perform these actions now have to live with the fear that if they engage in activities contrary to the spirit of society — if even a single citizen is catalyzed to halt the machinery of that injustice — they might still be held to account. The thread by which good governance hangs is this equality before the law, for the only fear of the man who turns the gears is that he may find himself upon them. (para. 5)

This fear produced by whistleblowers is a product of government 2.0 logic, where citizens have open access to information, interact with those in power, and hold elite accountable for their actions. Snowden (2016, May 3) argued that his act of

whistleblowing was a form of political resistance, consistent with American values and the legacy of Paul Revere. Whereas President Obama evoked Revere as a testament to the importance of government surveillance, Snowden used the same allusion to note the importance of citizens raising the alarm against government forces that impede liberty.

In advancing this argument about whistleblowing, I do not want to suggest that whistleblowers are not at risk of government violence. The individuals who disclose government information take great risks in regards to their own lives and personal freedom. But as Snowden explained, "The insiders at the highest levels of government have extraordinary capability, extraordinary resources, tremendous access to influence, and a monopoly on violence, but in the final calculus there is but one figure that matters: the individual citizen" (para. 30). Thus, whistleblowing against government and corporate abuses of surveillance demonstrate the potential rhetorical power present in the act of applying the practices of government 2.0 to hold those in power accountable.

Additionally, I am aware that I might be romanticizing the act of whistleblowing in uncritical ways. I use the figure of the whistleblower as a useful heuristic for exploring the potential for transparency rhetoric to function in ways that provides the general public with a counter narrative that disrupts the hegemonic ability to classify information and thus control what narrative the public is given. It is important to adopt an ethic of permanent criticism when approaching whistleblowers and stories that come from the media establishment. While Snowden defends his decision to leak the information to *the Guardian* and *Washington Post* rather than the *New York Times* because the later had refused to print stories about government surveillance at the request

of the Bush Administration, it is not my intention to deny that both *the Guardian and Washington Post* are part of the mainstream and very powerful media elite. The ability to publish the Snowden leaks brought both attention and money to the news companies as well as Greenwald who went on to publish a book. Further, the very nature of these media companies is to provide the public with the news, an act that by its very nature creates a framework for reality that justifies itself under the guise of producing objective and non-biased information.

Overall, transparency rhetoric can articulate new modes of civic engagement and subjectivity through algorithmic citizenship. The ability to release classified information to the public can work as a counter-surveillance that frustrates the panoptic gaze and reverses the seer/seen binary. While the government collects data from citizens in order to control and regulate society, whistleblowing can re-appropriate and turn this panoptic gaze back onto those conducting surveillance. Through Snowden and WikiLeaks' disclosures, the general public was able to read and examine surveillance documents from the government. The critical act of the leaks was that they took information rendered classified by corporate and government corporate entities and shattered the power of the national security discourse used to conceal those documents. For instance, WikiLeaks turned the NSA's statist gaze back onto itself and forced the NSA to respond to the leaks and justify their policies. The revelations made public the very policies that the government denied were in existence. By rendering the state transparent, whistleblowers exposed how the classification of secret documents justified by "national interest" and security was largely an attempt to avoid criticism of the government's

legitimacy. Thus, while Snowden and WikiLeaks' disclosures may not have provided startling new information that exposed a pernicious government conspiracy, it did challenge the legitimacy that the government used to control access of information. Additionally, the leaks further exposed the state's contradictions and hypocrisy regarding its demands for transparent citizens.

It must also be noted that whistleblowers, such as Edward Snowden, possess unique access to information that the regular citizen is not privy. It is not the intention of this dissertation to claim that every citizen can engage in the same strategies of whistleblowing or that each action will have the same type of political force. Rather, citizens can adopt the logic of surveillance and whistleblowing in order to invert and re-appropriate the traditional democratic mantra of open and transparent government. While not every citizen has the same ability or potential to disclose secret government information, there are numerous other ways in which citizens can align themselves together, bear witness to abuses of authority, and render that information public. Some of these tactics challenge the private/public divide and create a politics of the commons. Other techniques allow citizens to engage in mutual surveillance or sousveillance, which allows people to expose state violence in law enforcement and military contexts through acts of citizen-journalism.

Transparent algorithmic citizenship as a politics of the commons. Algorithmic citizens are capable of formulating a collaborative, interactive, and open subjectivity that functions to facilitate free access to information by calling into question the private/public divide in favor of creating a politics of the commons. This mode of being

operates in the space that is neither private nor public while existing simultaneously within and against Empire (Springer et al., 2012). It is a form of positive biopolitical production that circulates information in a radical fashion. As Springer et al. (2012) contend: "WikiLeaks itself mobilizes the bottom-up, immaterial labor of the multitude who traverse authoritarian landscapes and deploy proliferating biopolitical tactics to transform privacy into public visibility" (p. 697). The communicative acts of algorithmic citizenship thus constitute a biopolitical project that formulates affective connections, intensities, and subjective formations through radical openness, social networks, and sousveillance. Further, it undermines conceptions of private property on which neoliberal capitalism rests. Springer et al. (2012) further explain, "Because it disrupts the (neo)liberal state's capacity to manage the public visibility of its regimes of privacy, property, militarized violence and law, WikiLeaks is an important site of contestation over the imaginaries through which contemporary democracy is struggled for" (Springer et al., 2012, p. 699). This is all made possible because citizens adopt transparent subjectivities to make data open and available to the public. Accessible and transparent information helps to inform and encourage debate and deliberation, which invites new voices to connect and be witnessed within such discussions.

Open algorithmic citizenship as sousveillance. Algorithmic citizens are also constituted through a rhetorical process that connects the camera, spectators, and surveilled (Cram, 2012). Surveillance constantly shapes and re-shapes subjectivity by positioning subjects, bringing forth their images and locking them in a specific space and time. However, transparent subjects are able to invert traditional surveillance through the

process of sousveillance, or watching from below. In other words, transparent and vigilant subjects are capable of either redirecting the panoptic gaze back onto those in power or interacting and participating directly with surveillance. Koskela (2006) explains the force of these acts by using the term "active agency" to describe the process of using sousveillance to transform the body from a passive object of surveillance into an active subject that should have a copyright over itself. Technology, specifically cameras, can aid the performative functions of active agency. For example, tactics such as use of sousveillance self-portraits or selfies operate by actively negotiating public perception and visibility by highlighting that surveillance is intruding into people's lives. Surveillance's power dynamic is reversed by these acts as people take pictures of themselves from the security or surveillance screens located in the space. Additionally, web cameras are empowering technologies. Unlike surveillance cameras that are elevated and record and frame through capture and intrusion, web cameras allow people to represent themselves visually in an interactive process in which they control their digital, material, and virtual presence.

The ability to adopt an interactive approach to surveillance can provide agency in cultivating a resistant subjectivity and the ability to self-identify and control the representation of one's body. Emily Cram (2012) provides an example of this kind of control of representation in examining how Angie, a trans woman who was murdered, was able to alter how trans bodies were perceived. It was believed that Angie was killed because of her trans identity. The defense however argued that because Angie was legally named "Justin" that she must have engaged in sexual deception which motivated

the violence against her. This was an act of gender surveillance that inspected Angie to determine what normal or abnormal behavior was. In response to the defense's attempt to control Angie's public image, supporters engaged in a rhetorical performance by wearing clothing displaying Angie's portrait inside the courtroom. This allowed images of Angie as a trans woman to circulate, moving public perception away from the sexual deception depiction. Instead, the self-portrait transformed into a public witnessing, in which Angie was made public and a dialogue about what that meant began (Cram, 2012). In other words, Angie was, in many ways, an algorithmic citizen whose supporters were able to use her image to generate publicity and public discussion that works to shape and renegotiate subjectivity in a manner that promoted agency over representation, even posthumously.

Sousveillance as mutual gaze. The ability to observe and communicate with those who are watching shifts the ways in which the gaze operates. Koskela (2006), for instance, argues that webcams transform surveillance into an active spectacle, a rhetorical act that transforms bodies and the visual into sites of resistance. As a result, webcams open up the user's life to radically new subjectivities. With cameras, surveillance no longer operates only as a technology of control but also as a technology of agency and resistance. In particular, web cameras alters the gaze from an asymmetrical and unilateral manner into one a mutual gaze (Koskela, 2006). Thus, algorithmic citizenship provides the opportunity for subjects to rhetorically constitute a post-cyborg subjectivity, where the camera is no longer merely a recording device but is an integral aspect of the subject's lives. It produces a shared governance, or a way of perceiving and being in the

world differently that "enables a form of 'embodied witnessing' that transforms the relations between disgust, ways of seeing, and our bodies' relationship to the state" (Cram, 2012). Thus, surveillance is transformed from a register of criminality towards an alternative conception of responding to others when governmentality intersects with violence.

Further, algorithmic citizenship can re-appropriate transparency rhetoric for the purposes of exposing violent transgressions committed by those in power. By adopting a culture of reporting and surveillance, citizens can record and make public injustices that are typically relegated to private sphere and rendered invisible. For instance, the ability for ordinary citizens to use their digital devices to record acts of police or state violence committed against other citizens brings to public attention issues that people may not know about or might be inclined to disbelieve without visual proof. For example, citizens recorded state violence and made it public rose global awareness about state violence that was occurring in Egypt, Syria, and Tunisia (Markam, 2014).

In the U.S., the ability for citizens to enact algorithmic citizenship through sousveillance has brought national attention to police brutality against minorities. For instance, sousveillance is credited for exposing the police brutality against Rodney King (Blodgett, 2012). In this example, George Holliday filmed the severe beating an unarmed and black King received at the hands of Los Angeles police. Because the violence was captured on video by a civilian, the public was allowed to see video evidence that might otherwise have been denied or explained away (Blodgett, 2012). The ability to capture the acts on video was essential in verifying King's claims of abuse (Blodgett, 2012).

Therefore, the ability to produce evidence is essential for challenging the perceptual gap in credibility between police officers and civilians. If one merely attempts to report abuse and violence without video proof, they often are outmatched by police resources or risk having their voices discredited (Mann, 1998).

Sousveillance is a technique that algorithmic citizens can use to enact a politics of transparency (Scholz, 2008). For instance, there is a digital application called Mobile Justice, designed for people to record their interactions with police officers (Hackman, 2015). The app allows recorded video to be sent to the local American Civil Liberties Union (ACLU) chapter to be reviewed by lawyers. The direct transmission of the recording prevents police from either confiscating or destroying the video evidence. Lawyer then review the videos to help protect citizens from be incriminated in the recording (Hackman, 2015). Further, the app also notifies users if they are close to another person who is either experiencing or witnessing a public encounter between the citizen and police (Hackman, 2015). Thus, algorithmic citizenship technologies and tactics are capable of connecting users, bringing them together to publicly witness citizen-police interactions while encouraging and promoting more ethically transparent communications.

Sousveillance as citizen-journalism. Citizen-journalists are capable of providing firsthand accounts that produce an affective investment and emotional appeal that cannot simply be captured by mainstream news (Scholz, 2008). There is a level of care, cooperation, and intimacy that is embodied through alternative approaches to surveillance. For example, websites such as IraqBodyCount.org and

livingunderdrone.org report on the death tolls caused by U.S. military action. In doing so, they provide information and visibility to deaths that are rendered outside the purview of the state-centric surveillance narratives. Wikileaks, for instance, released the video *Collateral Murder*, which showed U.S. soldiers firing down upon civilians, including reporters for the Reuters news organization (Mortenson, 2014). The shooting happened because a helicopter pilot mistook a camera telephoto lens for a rocket propelled grenade. The video's audio recorded one of the pilots saying, "Come on, let us shoot!" The excitement about shooting was accompanied by the aerial footage that provides the perspective of the soldier. From the vantage point of the helicopter, the soldier's spatial relationship to the people they were shooting at was so vast that the people appear as nothing more than a blip on a screen, not unlike a perspective in a video game. The use of aerial surveillance seen in *Collateral Murder* produced what Donna Haraway (1988) refers to as the "god-trick," the ability to gaze from nowhere while simultaneously being everywhere (Graham, Shaw, & Akhter, 2012). However, by leaking this video, Wikileaks was able to criticize the view from nowhere by humanizing the dead and inviting the viewing audience to identify with the victims.

WikiLeaks also has a website collateralmurder.com which provides numerous camera angles and audio of soldiers massacring civilians juxtaposed with images of children grieving over their dead parents' bodies. The website also showed images from the funerals of dead children and the Reuters journalists who were killed in the attack. Other websites such as Iraqbodycount.org made visible the amount of death and destruction waged during the second Gulf War. Additionally, livingunderdrones.org

engaged in similar humanizing strategies by providing the names and stories of those whose lives were affected by the increased use of drone strikes as a method of conducting the war on terror. These websites operate rhetorically by humanizing and making visible the violence that is done to otherwise abstract and dehumanized bodies. Further, offer a counter-narrative against the hegemonic state-sanctioned national security discourse that denies that the U.S. kills civilians.

Ian Shaw (2013) exposes the need to publicize and render visible the stories of those who are asymmetrically targeted by surveillance technologies which, in many instances, meant being marked for death. His argument is that the state-sanctioned surveillance narrative is one that strategically focuses its gaze in a way that renders invisible and silent the material violence it is committing. Take for example the numerous drone strikes that are happening in the region that the public is told is Pakistan. Rather than happening in Pakistan, the drone strikes are predominately taking place in an area known as the Federally Administered Tribal Areas (FATA). This space was carved out of a history of colonialism and was originally created as a buffer zone between imperialist British and Russian forces (Graham, Shaw, & Akhter, 2012). In the war on terror, the FATA becomes an exceptional space, in that it is and is not Pakistan. Moreover, the space that is not accessible to journalists and other researchers and therefore activity there does not register in public consciousness. Because it is a space rendered largely invisible and lawless, it becomes a site where he majority of U.S. drone strikes occur. In response to this problem, websites such as livingunderdrones.org provide visibility to the area by sharing the story of the individuals who live in this space

and face the exceptionalist violence on a daily basis. Publicizing their stories works to disrupt and disturb the hegemonic gaze that renders life in the FATA as a statistical dehumanized algorithmic calculation. In exposing people's stories, the algorithmic calculation is challenged by this humanizing discourse that is not found in the disposition matrix. Therefore, the sousveillance strategies used by WikiLeaks and similar websites situate the surveillance footage as specific events that are occurring at specific spaces and during specific times. It is capable of transforming the abstracted footage gathered from surveillance cameras and turning them into embodied events (Mortenson, 2014). While traditional news footage might provide abstract coverage of a drone strike occurring in the FATA or Pakistan, sousveillance strategies instead report on specific material events that are a scene of violence.

In addition to revealing that which is intended to be kept invisible or silent, the spectacle produced through algorithmic citizenship is an important rhetorical process. For example, Cram (2012) argues that public witnessing can provide opportunities for publics to come together to mourn. These public grieving gatherings thus rhetorically constitute political communities through emotional identification and solidarity through calls for dignity of others (Cram, 2012). Overall, spectatorship operates as a critical site of civic judgment and invention. The act of witnessing through sousveillance opens the possible for forming counter-hegemonic articulations that expose the radical instability of legal language, institutions, and cultures (Cram, 2012). Algorithmic citizenship does not require that citizens become docile or passive subjects; rather, it provides the tools of

collaboration, interactivity, and transparency capable of articulating alternate subjectivities that produce political agency.

Limitations and future directions of study

This project provides a map of the rhetorical constitution of algorithmic citizenship as it emerged from counter-terrorism and government 2.0 discourse. To this end, the dissertations followed an algorithmic trail of presidential address and corporate marketing strategies in order to map how these discourses interpellate citizens. In following this trail, there three primary issues that were beyond the scope of research and analysis of this project.

First, the counter-terrorism discourse that was analyzed was primarily concerned with al Qaeda and, as a result, it does not fully analyze the rhetoric used by organizations like ISIS. Because of a need to limit the scope of the dissertation, I primarily focused on a timeline ranging from September 11, 2001-January 27, 2014. While Chapter 4 examined how Obama's comments and speeches were directed at domestic radicalization, the analysis concluded without much focus on the rise of ISIS. In limiting out ISIS, there are several issues that are relevant to this research but beyond the scope of study. For instance, the research was concluded before ISIS claimed responsibility for the San Bernardino mass shooting, which has rekindled public arguments about the need for more surveillance. Additionally, this event raised issues about the ability of citizens to use technology to network, radicalize, and carry out domestic acts of terrorism. Future research should consider how the domestic terrorist threat posed by terrorist organization such as ISIS has extended or reconfigured U.S. counterterrorism and surveillance

discourses. Since the analysis of this project was completed, major attacks linked in some way to ISIS has occurred in places such as Bangladesh, Belgium, Iraq, Orlando, Paris, San Bernardino, Syria, and Turkey. While an anti-ISIS coalition has scored a number of military victories against ISIS, its ability to radicalize subjects in several countries through internet videos and social media seems to be increasing. As a result, there is even more surveilling and policing of online behavior.

Second, this dissertation was also limited primarily to U.S. counterterrorism discourse and it did not analyze the rhetoric used by organizations for the purpose of recruiting, networking, and committing acts of terrorism. Chapter Four did provide a brief analysis of al Qaeda's magazine *Inspire*. However, future research should explore the radicalization and recruiting strategies of terrorist organizations. For instance, future studies might consider analyzing the public speeches of key al-Qaeda figures like Anwar al-Awlaki or Osama bin Laden to better understand how they interpellate followers. In regards to studying ISIS, future research should analyze Abu Bakr al-Baghdadi's sermon in the Mosul mosque where he declares himself Caliphate. Further, ISIS has released several recruitment videos to the public as well as an English magazine called *Dabiq* that might be rhetorically significant in helping to understand how people are persuaded to join. Finally, others studies might consider analyzing the public executions committed by ISIS against American citizens and others and how this affects both recruitment and Western responses.

This dissertation also exclusively examined U.S. counterterrorism discourse in response to terrorist attacks made on American soil. While, these attacks are important

for tracing how government 2.0, security, and surveillance discourses work together to constitute algorithmic citizenship, analyzing major global terrorist attacks would greatly contribute to the intellectual discussion. There is no denying that al Qaeda attacks in Istanbul, Jakarta, or Madrid all contributed to the counterterrorism discourse that informs U.S. counter-terrorism policy. Additionally, attacks against *Charlie Hebdo* demonstrated the material impact that art, composition, and speech have in regards to soliciting acts of violence. Lastly, the late-2015 and current 2016 ISIS attacks further demonstrate the global and interconnected aspects of terrorism and would provide useful information in regards to how algorithmic citizenship operates on a global level in different legal and political systems.

Third, the economic analysis of this dissertation was limited to the discourse of a single company, IBM, and did not explore instances where private businesses engage in legal disputes with government agencies to prevent data collection. While, IBM was an important artifact for analyzing the corporate justification for government 2.0, it was not the intention of this study to suggest that all private businesses sought to comply with the government's demand to turn over consumer data. For instance, Microsoft sued the Department of Justice over secret data requests. Additionally, Apple was engaged in a legal dispute with the FBI and refused to write a code to allow hacking into iPhones after the San Bernardino shooting. Future studies should analyze these economic discourses as they pit individual privacy against national security rhetoric.

Conclusion

Despite these limitations, scholarly research about algorithmic citizenship becomes essential as data collection is increasingly used to help governments regulate populations and discipline individual subjectivities. With both private companies and government organizations claiming that data is a national resource, citizens must learn about these practices in order to effectively participate in the process of democratic governance. It is with this understanding in mind that this project utilizes a rhetorical materialism method of analysis to map algorithmic citizenship as it is discursively constituted through government 2.0 and war on terror discourse. Tracing the rhetorical constitution of algorithmic citizenship supplements the many contributions currently being made to this field of research within such fields as communication and cultural studies, political science, and security studies. Understanding algorithmic citizenship is especially important for scholars who examine issues of citizenship, surveillance, and war.

First, studying algorithmic citizenship demonstrates consumerism's potential for civic and democratic engagement. Traditionally, scholars have separated the concepts of consumerism and citizenship as being largely unrelated. For instance, Mark Crispen (2004) claims that citizens are different than consumers because they are equals in government processes but manipulated like sheep in commercial transactions. Additionally, Bob Garfield (2004) expresses a similar view, contending that citizens participate in the collectivity in a democracy whereas consumers are only interested in individual choices. My analysis of algorithmic citizenship and government 2.0 demonstrates that the two concepts cannot be easily separated. If data is being used to

determine a person's material identity, then the ability for a consumer to produce data is a form of enacting citizenship and participating in the governing process through public engagement. Furthermore, the interactive logic of government 2.0 indicates that consumerism is no longer a passive activity; rather, it creates new modes for communicating and participating with others. As a results, scholars can build upon this understanding to theorize and develop new possibilities for the democratic processes of governing and being governed.

Second, studies of algorithmic citizenship are capable of contributing to the intellectual discussion regarding the surveillance rhetoric. Rhetorical tropes associated with surveillance such as openness and transparency must be problematized. Too often, scholars studying surveillance adopt a totalizing viewpoint in which surveillance is either an oppressive force that must be resisted entirely or transparency is celebrated unreflexively as resistant act in an open society. Scholars interested in surveillance rhetoric should continue to analyze how the interpellative call to be open and transparent can have the normalizing and legitimizing effects of rendering the population visible to those in power. At the same time, the ability to be made visible through surveillance can also provide people with a level of political agency to communicate and connect with others as well as the ability to expose and interact with the governing process.

Finally, studies of algorithmic citizenship provide useful theoretical tools to understand war rhetoric and how it is modified and intensified through counterterrorism discourses. In a few months, the war on terror will be transferred to a third president and it is important to trace how the discourse and policies have evolved during this time. It is

easy to dismiss President Obama's war on terror policies as a mere continuation of the Bush administration's policies. Instead, this study demonstrates the rhetorical shifts in the logic and implementation of the war on terror. As this project argues, it is important to note how President Obama operated by publicly denouncing the unpopular Bush-era polices such as enhanced interrogation, indefinite detention of prisoners in Guantanamo Bay, and mass surveillance. In response to these controversial measures, Obama began to modify the surveillance programs by connecting them with increased use of lethal drone strikes and an implementation of the presidential kill list. Additionally, whereas former President Bush approached the war on terror through the traditional logic of external enemy nation-states, President Obama operated through an endo-colonizing logic where the enemy is a particular ideology that can exist both inside and outside the country. Because the enemy was an ideology, governmentality operated through monitoring the transparent performances of algorithmic citizens. Thus, scholars interested in exploring war rhetoric would be remiss to not consider algorithmic citizenship as a future site of study.

REFERENCES

Al-Awlaki, A. (2010). Shaykh Anwar's Message to the American People and Muslims in the West. *Inspire.* Summer 1431 (1) retrieved from s3.amazonaws.com/s3.documentclo ud.org/documents/1392935/aqap-inspire-magazine-volume-1.pdf

Allabaugh, D. (2012). Computer skills become essential tool for job seekers. *Times Tribune*. Retrieved from http://thetimes-tribune.com/news/business/computer-skills-become-essential-tool-for-job-seekers-1.1293372

American Anthropological Association (2007, October 31). *American Anthropological Association Executive Board Statement on the Human Terrain System Project*.. Retrieved from http://www.aaanet.org/about/policies/statements/human-terrain-system-statement.cfm

American Civil Liberties Union of Massachusetts (2010). *Know Your Options at the Airport*. Retrieved from the American Civil Liberties Union website: http://www.aclum.org/sites/all/files/education/aclu_know_your_options_at_airport_nov2010.pdf

Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University Press of Kansas.

Asen, R. (2004). A Discourse Theory of Citizenship. *Quarterly Journal of Speech*. 90(2) 189-211.

AQ Chef. (2010). How to make a bomb in the kitchen of your Mom. *Inspire*. Summer

1431(1).Retrievedfroms3.amazonaws.com/s3.documentcloud.org/documents/1392935/aqap-inspire-magazine-volume-1.pdf

Authorization for Use of Military Force of 2001, S.J. Res. 23, Public Law 107-40. (2001). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm

Backstrom, L., Boldi, P., Rosa, M., Ugander, J., & Vigna, S. (2012). Four Degrees of Separation. *Websci 2012*. p. 33-42. doi 10.1145/2380718.2380723

Ball, J. (2013). NSA's Prism surveillance program: how it works and what it can do. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/08/nsa-prism- server-collection-facebook-google

Beam, C. (2009). Paper Weight: The health care bill is more than 1,000 pages. Is that a lot? *Slate*. Retrievedfromwww.slate.com/articles/news_and_politics/explainer/2009/08/paper_weight.html

Becker, J., & Shane, S. (2012). Secret 'Kill List' Proves a Test of Obama's Principles and Will. *The New York Times*. Retrieved from:www.nytimes.com/2012/05/29/world/obamas-leadership-in-w ar-on-al-qaeda.html

Benjamin, W. (2003). *Selected Writings Volume 4 1938-1940*. (E. Jephcott, Trans). Cambridge, MA: The Belknap Press of Harvard University Press.

Beasley, V. (2001) The rhetoric of ideological consensus in the United States: American principles and American pose in presidential inaugurals, *Communication Monographs*, 68:2, 169-183 .doi.org/10.1080/03637750128055.

Biesecker, B. (2007). No Time for Mourning: The Rhetorical Production of the

Melancholic Citizen-Subject in the War on Terror, *Philosophy and Rhetoric*. 40(1) 147-169.

Blodgett, L. (2012). LA Riots Video Footage: Community Recording, or 'Sousveillance', In Los Angeles Since the LA Riots. *The Huffington Post*. Retrieved from www.huffingtonpost.com/2012/04/28/la-riots-sousveillance_n_1460347.html

Bloomfield, A. (2013). GCHQ: The British Are Spying On Us More Than the NSA Is. *Policy.Mic*. Retrieved from http://mic.com/articles/50333/gchq-the-british-are-spying-on-us-more-than-the-nsa-is

Bridle J. (ND). Algorithmic Citizenship. *Citizen EX*. Retrieved from http://citizen-ex.com/citizenship

Bush, G. (2002, Febuary 7). *White Memo from President Bush to Vice President and Others re: Humane Treatment of al Qaeda and Taliban Detainees*. [Memorandum]. Washington DC: ACLU FOIA Request. Retrieved from www.thetorturedatabase.org/document/white-memo-president-bush-vice-president-and-others-re-humane-treatment-al-qaeda-and?search_url=search/apachesolr_search/Bush%20memo

Butler, J. (1997). *The Psychic Life of Power: Theories in Subjection*. Stanford, CA: Stanford University Press.

Butler, J., & Athanasiou, A. (2013). *Dispossession: The Performative in the Political*. Cambridge UK: Polity Press.

Carafano, J., Bucci, S., & Zuckerman, J. (2012). *Fifty Terror Plots Foiled Since 9/11:*

The Homegrown Threat and the Long War on Terrorism. Retrieved from the Heritage Foundation Website: http://www.heritage.org/research/reports/2012/04/fifty-terror-plots-foiled-since-9-11-the-homegrown-threat-and-the-long-war-on-terrorism

Carson, E. (2014). Prisoners in 2013. *Bureau of Justice Statistics*. Retrieved from http://www.bjs.gov/content/pub/pdf/p13.pdf

Cauley, L. (2006, May 11). NSA has massive database of Americans' phone calls. *USA Today*. Retrieved from http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm

Chapman, S. (2014, October 22). Even terrorists have a right to citizenship. *Chicago Tribune*, retrieved online at http://www.chicagotribune.com/news/opinion/chapman/ct-government-terrorist-citizenship-strip-ted-cruz-20141022-column.html.

CBS News. (2009). Bush's Final Approval Rating: 22 Percent. Retrieved from http://www.cbsnews.com/news/bushs-final-approval-rating-22-percent/

Chaput, C. (2010). Rhetorical circulation in late capitalism: Neoliberalism and the overdetermination of affective energy. *Philosophy and Rhetoric*, 43(1), 1-25.

CNN. (2006). Plane plot involved 'explosive cocktail,' official says. Retrieved from http://www.cnn.com/2006/US/08/10/us.security.1642/index.html

Coll, S. (2004). Legal Disputes Over Hunt Paralyzed Clinton's Aides. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/articles/A59781-2004Feb21.html

Communication Arts (2013). *IBM THINK Exhibit*. Retrieved from http://www.commarts.com/interactive/cai13/ibmthinkexhibit.html

Cortada, J., Gupta, A., & Le Noir, M. (2007). How nations thrive in the Information Age: leveraging information and communications technologies for national economic development, *IBM Institute for Business Value*. Retrieved from http://www-935.ibm.com/services/us/gbs/bus/pdf/g510-6575-01-infoage.pdf

Cortada, J., Dijstra, S., Mooney, G., & Ramsey T. (2008). Government 2020 and the perpetual collaboration mandate. *IBM Global business services*. located online: http://www-01.ibm.com/industries/government/ieg/pdf/govt_2020_report.pdf

Cram, E. (2012). "Angie was Our Sister:" Witnessing the Trans-Formation of Disgust in the Citizenry of Photography. *Quarterly Journal of Speech*. 98(4) 411-438.

Crispen, M. (2004). Persuading the Consumer and the Citizen/Interviewer: Frontline [transcript]. Retrieved fromwww.pbs.org/wgbh/pages/frontline/shows/persuaders/themes/citizen.html

Cruz, A. (2011). The robot general: Implications of Watson on military operations. Armed Forces Journal. Retrieved from http://www.armedforcesjournal.com/the-robot-general/

Daugherty, R. (2003). President Bush broadens classifications rules. *The News Media & The Law*. 27(2), 16.

De Vogue, A. (2008). Classified Detainee Memos at Center of Legal War. *ABC News*. Retrieved From http://abcnews.go.com/TheLaw/LawPolitics/story?id=4620002

Deleuze, G. & Guattari, F. (2009). *Anti-Oedipus: Capitalism and Schizophrenia*. (R.

Hurley, M. Seem, and H. Lane, Trans). NY, New York: Viking Press (originally published 1977).

DeLuca, K. (1999) Articulation Theory: A Discursive Grounding for Rhetorical Practice. *Philosophy and Rhetoric*. 32 (4) 334-348.

Demers, J. & Ross, S. (2008). Bush secrecy policies have Transformed U.S. Government From "Open" to "Closed". Global Research. Retrieved from www.globalresearch.ca/bush-secrecy-policies-have-transformed-u-s-government-from-open-to-closed/8763

Department of Homeland Security. (2014, September 5). *National Terrorism Advisory System*. Retrieved from the Official website of the Department of Homeland Security: http://www.dhs.gov/national-terrorism-advisory-system

Department of Homeland Security (2015, September 22*). Chronology of Changes to the Homeland Security Advisory System*. Retrieved from http://www.dhs.gov/homeland-security-advisory-system

Department of Justice. (ND) *The USA Patriot Act: Preserving Life and Liberty*. http://www.justice.gov/archive/ll/highlights.htm

Department of Justice. (2006, Jan 19*). Legal Authorities Supporting the Activities of the National Security Agency Described By the President*. Retrieved from http://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pdf

Department of Justice White Paper (2011). *Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qa'ida or An*

Associated Force. Retrieved from http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/dept-white-paper.pdf

Earnest, J. [Interviewee], & Stelter, B. [Interviewer]. (2014). Josh Earnest's First Sunday Interview. *Reliable Sources*. Retrieved from: cnnpressroom.blogs.cnn.com/2014/07/13/wh-press-secy-josh-earnests-first-sunday-interview/

Elsea, J. (2005). Detention of American Citizens as Enemy Combatants. *Congressional Research Service Report for Congress*. Retrieved from https://www.fas.org/sgp/crs/misc/RL31724.pdf

Engels, J., & Saas, W. (2013). On Acquiescence and Ends-Less War: An Inquiry into the New War Rhetoric. *Quarterly Journal of Speech*. 99(2), 225-232.

Executive Office of the President. Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 26, 2009) retrieved from https://www.federalregister.gov/articles/2009/01/26/E9-1777/transparency-and-open-government

ezkl2230 (2013). Amex Secure World [video file]. Retrieved from https://www.youtube.com/watch?v=4vQoBTnnc44

Federal Bureau of Investigation. (2004, Apr. 30). *The Terrorist Threat Integration Center: One Year Later*. Retrieved from http://www.fbi.gov/news/stories/2004/april/threat_043004

FBI National Press Office (2013). *2011 Request for Information on Tamerlan Tsarnaev*

From Foreign Government. Retrieved from: https://www.fbi.gov/news/pressrel/press- releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government

Federal News Service. (2013, March 6*). Hearing of the Senate Judiciary Committee Subject: "Oversight of the Justice Department" Chaired by: Senator Patrick Leahy (D-VT) Witness: Attorney General Eric Holder*. Retrieved from http://www.lexisnexis.com.proxy.lib.wayne.edu/hottopics/lnacademic/?verb=sf&sfi=AC00NBEasySrch

Figg, E. (2014). The legacy of Blue CRUSH. *High Ground*. Retrieved from http://www.highgroundnews.com/features/BlueCrush031214.aspx

Fine, G., Heddell, G., Lewis, P, Ellard, G., C& Mazer, R. (2009). *Unclassified Report on the President's Surveillance Program*. (Prepared by the Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence No. 2009-0013-AS). Washington, DC: U.S. Government Printing Office

Foucault, M. (1978) *The History of Sexuality. Volume 1: An Introduction*. (R. Hurley, Trans.). New York, NY: Random House (Original work published 1976).

Foucault, M. (1988) *Technologies of the Self: A Seminar with Michael Foucault*. (Eds. Martin, L., Gutman, H., & Hutton, P.) Amherst, MA: The University of Massachusetts Press.

Foucault, M. (2000). Governmentality. In P. Rabinow (ed) (Vol. 3), *Power* (201-222). (Robert Hurley, Trans). New York, NY: The New Press.

Foucault, M. (2003). *"Society Must Be Defended": Lectures at the College de France, 1975-1976*. (D. Macey, Trans.). New York, NY: Picador (Original work published in 1997).

Friedman, L., & Lanspery, L. (2011). *IBM Centennial THINK Exhibit Fact Sheet*. Retrieved from: IBM%20CENTENNIAL%20THINK%20EXHIBIT%20(4).pdf

Garamone, J. (2002). Leaks Put Americans in Danger, Rumsfeld Says. *DoD News*. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=43656

Garfield, B. (2004). Persuading the Consumer and the Citizen/Interviewer: Frontline [transcript]. Retrieved from www.pbs.org/wgbh/pages/frontline /shows/persuaders/themes/citizen.html

Gates, K. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York, NY: NYU Press.

Gellman, B. & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, B., & Soltani, A. (2013, October 14). NSA collects millions of e-mail address Books globally. *Washington Post*. Retrieved from http://www.washingtonpost.com/world/natio nal-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

Gellman, B., & Soltani, A. (2013, Oct. 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Genck, D. (2013). *The Charges and Affidavit of Special Agent Daniel R. Genk. AO 91 (Rev. 11/11) criminal complaint*. United States District Court for the District of Massachusetts, Case No. 13-2103-MAB.

Gezari, V. (2013, Aug 10). How to Read Afghanistan, New York Times. Retrieved from http://www.nytimes.com/2013/08/11/opinion/sunday/how-to-read-afghanistan.html?_r=0

Gorman, S. (2006, May 18). NSA rejected system that sifted phone data legally. *The Baltimore Sun*. Retrieved from http://articles.baltimoresun.com/2006-05-18/news/06051800941surveillance-national-security-agency-well-informed

Gonyea, D. (Reporter) & Bush, G. W. (Responder). (2003, February 18). Analysis: President Bush Discounts Impact of Anti-War Protest Marches Around the World. All Things Considered [NPR Transcript]. Retrieved from www.npr.org/programs/atc/transcripts/2003/feb/030218.gonyea.html

Gonzalez, A. (2004). *Remarks by Alberto R. Gonzales Counsel to the President, Before the American Bar Association Standing Committee on Law and National Security*. Retrieved from www.pegc.us/archive/White_House/gonzales_remarks_to_ABA_20040224.pdf

Gonzalez, R. (2007). Towards mercenary anthropology? The new US Army Counterinsurgency manual FM 3-24 and the military-anthropology complex. *Anthropology Today*. 23(3), 14-19.

Graham, I., Shaw, R., & Akhter, M. (2012). The Unbearable Humanness of Drone Warfare in FATA, Pakistan. *Antipode*. 44(4), 1490-1509, doi: 10.1111/j.1467-8330.2011.00940.x.

Greenberg, A. (2014) Wired, August 20, *Researchers Easily Slipped Weapons Past TSA's X-Ray Body Scanners*. Retrieved from the Wired website: www.wired.com/2014/08/study-shows-how-easily-weapons-can-be-smuggled-past-tsas-x-ray-body-scanners/

Greene, R. (1998). Another Materialist Rhetoric, *Critical Studies in Mass Communication*. 15(1), 21-41.

Greene, R. (2001). Citizenship in a global Context: Towards a Future Beginning For a Cultural Studies Inspired Argumentation Theory. *Arguing Communication & Culture*. 1(1), 97.

Greene, R. (2003) John Dewey's Eloquent Citizen: Communication, Judgment, and Postmodern Capitalism. *Argumentation and Advocacy*. 39(Winter), 189-206.

Greene, R. (2004) Rhetoric and Capitalism: Rhetorical Agency as Communicative Labor. *Philosophy and Rhetoric*. 37(3)188-206.

Greene, R. (2004). The Rhetorical Subject and the General Intellect. In B. Biesecker & Lucaites, J. (Eds), *Rhetoric, Materiality, and Politics* (43-66). New York, NY: Peter Lang.

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data Of Apple, Google and others. *The Guardian*. Retrieved from www.theguardian.com/world/2 013/jun/06/us-tech-giants-nsa-data

Grossberg, L. (1992). *We gotta get outta of this place: Popular Conservatism and Postmodern Culture*. London: Routledge.

Goudreau, J. (2013). IBM CEO Predicts Three Ways Technology Will Transform the Future of Business. *Forbes*. Retrieved from www.forbes.com/sites/jennagoudreau/2013/03/08/ibm-ceo-predicts-three-ways-technology-will-transform-the-future-of-business/

Hackens, R. (2015). New app aims to help citizens record police brutality using cellphones. *The Guardian.* Retrieved from http://www.theguardian.com/us-news/2015/may/07/new-app-citizens-record-police-brutality-cellphones

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies*, 14(3), 575-599.

Harper, D. (2008) The Politics of Paranoia: Paranoid Positioning and Conspiratorial Narratives in the Surveillance Society. *Surveillance and Society*. 5(1) 1-32

Hay, J. (2007). The many responsibilities of the new citizen-soldier. *Communication and Critical/Cultural Studies*. 4(2) 216-220.

Heath, B. (2015, Apr. 8). U.S. secretly tracked billions of calls for decades. *USA Today*. Retrieved from www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

Hickey, W. (2012). Meet the Biggest Political Donors in Silicon Valley. *Business Insider*. Retrieved from http://www.businessinsider.com/donations-obama-romney-tech-yahoo-google-facebook-2012-9?op=1

Holder, Attorney General, Et Al. v. Humanitarian Law Project Et Al. No. 08–1498 (2010).

Hopkins, N., & Borger, J. (2013). Exclusive: NSA pays £100m in secret funding for GCHQ. *The Guardian*. Retrieved from www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

House of Representatives Committee on Oversight and Government Reform (2007). Memorandum: Additional Information about Blackwater USA. Retrieved from http://graphics8.nytimes.com/packages/pdf/national/20071001121609.pdf

Huntington, S. (1993). The Clash of Civilizations? *Foreign Affairs*, 72 (3), 22-49.

IBM (N.D.) *THINK exhibit: An Exploration into Making the World Work Better*. Retrieved from http://www-03.ibm.com/ibm/history/ibm100/us/en/thinkexhibit/

IBM Social Media (2010, January 20). *Smarter Public Safety*. [Video File]. Retrieved from https://www.youtube.com/watch?v=pErVnX9mrVY

IBM (2011, October 4). *THINK: A film about making the world work better* [Video file]. Retrieved from https://www.youtube.com/watch?v=UtEIafP9h7Y

IBM (2011, March 17). *Predictive Crime Fighting*. Retrieved from http://www-

03.ibm.com/ibm/history/ibm100/us/en/icons/crimefighting/

IBM. (2011, March 11). *A Culture of Think*. Retrieved From www-03.ibm.com/ibm/history/ibm100/us/en/icons/think_culture/

IBM (2011). *Memphis PD: Keeping ahead of Criminals by finding the "hot spots"*. Retrieved from http://www.ibm.com/smarterplanet/us/en/leadership/memphispd/assets/pdf/IBM_MemphisPD.pdf

IBM. (2012, May 1). *IBM i2 Intelligence Analysis portfolio available from Passport Advantage.* Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS212-110

IBM. (2013, December 27). *A military team turns complex human terrain data into Intelligence*. Retrieved from www03.ibm.com/software/businesscasestudies/us/en/corp?synkey=L164373D99437L43

IBM. (2014, May 28). *State intelligence agency prevents crime by monitoring social media*. Retrieved from www-03.ibm.com/software/businesscasestudies/us/en/corp?synkey=J853688V51468P02

Insider Surveillance. (2014*). Palantir: Visualizing the Future of Crime and Terrorism*. Retrieved from https://www.insidersurveillance.com/palantir-visualizing-the-future-of-crime-and-terrorism/

Inspire (2013). We Are All Usama: America you have passed on the message of Sheikh Usama that you are truly the enemy of Islam. *Inspire.* Spring 1434(10). Retrieved from info.publicintelligence .net/InspireWinter2013.pdf

Isikoff, M. (2013). Justice Department memo reveals legal case for drone strikes on Americans. *NBC News*. Retrieved from investigations.nbcnews.com/_news/2013/02/04/16843014-justice-department-memo-reveals-legal-case-for-drone-strikes-on-americans

Issenberg, S. (2012). A More Perfect Union: How President Obama's campaign used big data to rally individual voters. *MIT Technology Review*. Retrieved from www.technologyreview .com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters/

Ivie, R. (2005). *Democracy and America's War on Terror*. Tuscaloosa, AL: The University of Alabama Press.

Immigration, Asylum and Nationality Act 2006, Revised Statutes of United Kingdom (2006, c.13). Retrieved from http://www.legislation.gov.uk/ukpga/2006/13/contents

Jameson, F. (1991). *Postmodernism or, the Cultural Logic of Late Capitalism*. Durham, NC: Duke University Press.

Janssen, K. (2014, July 23). Alleged bin Laden associate should lose citizenship, U.S. says. *Chicago Sun Times*. Located online at http://chicago.suntimes.com/?p=162233

Johnson, C. (2014). Justice Department Renews Focus On Homegrown Terrorists, *NPR*,

Retrieved from http://www.npr.org/2014/06/03/318414889/justice-department-renews-focus-on-homegrown-terrorists.

Johnson, D. (2007). Mapping the Meme: A Geographical Approach to Materialist Rhetorical Criticism. *Communication and Critical/Cultural Studies*. 4(1) 27-50.

Kaminer, W. (2010, June 21). 'Material Support' Bans and the Criminalization of Political Advocacy. *The Atlantic*, located at www.theatlantic.com/national/archive/2010/06/materi al-support-bans-and-the-criminalization-of-political-advocacy/58469/

Katersky, A., & McPhee, M. (2015). What Boston Marathon Bombing Suspect Dzhokhar Tsarneav Wrote in Blood-Stained Boat. *ABC News*. Retrieved from http://abcnews.go.com/US/boston-marathon-bombing-suspect-dzhokhar-tsarnaev-wrote-blood/story?id=29534415

King, J. [Interviewer] & Pressler, P. [Interviewee] (2001, October 6). CNN Saturday Morning News [Interview Transcript]. Retrieved from CNN website: http://transcripts.cnn.com/TRANSCRIPTS/0110/06/smn.26.html

Kirk, M, Gilmore, J., & Wiser, M. (2014). United States of Secrets: The Program, United States, *Public Broadcasting Service*, Retrieved from PBS website: www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/transcript-61/

Klien, S. (2005) Public Character and the Simulacrum: The Construction of the Soldier Patriot and Citizen Agency in Black Hawk Down, *Critical Studies in Media Communication*, 22:5, 427-449, doi: 10.1080/07393180500342993.

Koebler, J. (2013). Boston Bombing Changes Lawmakers' Views on Drone Killings of Americans on U.S. Soil. *US News & World Report*. Retrieved from http://www.usnews.com/news/articles/2013/04/23/boston-bombing-changes-lawmakers-views-on-drone-killings-of-americans-on-us-soil

Kosar, K. (2009). Security Classification Policy and Procedure: E.O. 12958, as Amended. *Congressional Research Service*. Retrieved from http://www.fas.org/sgp/crs/secrecy/97-771.pdf

Koskela, H. (2006). 'The Other side of Surveillance': webcams, power and agency. In *Theorizing Surveillance: The Panopticon and Beyond*. (Ed. David Lyon). Portland, OR: Willan Publishing.

Krebs, R. (2009). The Citizen-Soldier Tradition in the United States: Has its demise been greatly exaggerated? *Armed Forces & Society*. 36, 153-174, doi: 10.1177/0095327X09337370

Kun, J. (2015). Big data algorithms can discriminate and it's not clear what to do about it. *The Conversation*. Retrieved from http://theconversation.com/big-data-algorithms-can-discriminate-and-its-not-clear-what-to-do-about-it-45849

Kundnani, A. (2014*). The Muslims Are Coming!: Islamophobia, Extremism, and the Domestic War on Terror*. Brooklyn, NY: Verso.

Laclau, E. and Mouffe, C. (1985). *Hegemony and socialist strategy.* London: Verso.

Lafer, G. (2004). Neoliberalism by Other Means: The "War on Terror" At Home and Abroad. *workSite.* Retrieved from http://worksite.econ.usyd.edu.au/lafer.html

Lee, J. (2009). Transparency and Open Government. Retrieved from

https://www.whitehouse.gov/blog/2009/05/21/transparency-and-open-government

Lee, T. (2013, June 6). Everything you need to know about the NSA's phone records scandal. *The Washington Post*. Retrieved from www.washingtonpost.com/blogs/wonkblog/wp/2013/06/06/everything-you-need-to-know-about-the-nsa-scandal/

Lee, T. (2013, June 12). Here's everything we know about PRISM to date. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

Leonard, T. (2010). Barack Obama orders killing of US cleric Anwar al-Awlaki. *Telegraph*. Retrieved from www.telegraph.co.uk/news/worldnews/barackobama/7564581/Barack-Obama-orders-killing-of-US-cleric-Anwar-al-Awlaki.html

Lever, R. (2012). 'Predictive policing' takes bite out of crime. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/technology/sci-tech/predictive-policing-takes-bite-out-of-crime-20120730-23bg6.html#ixzz26JDKv6XX

Lindgren, S. &, Lundstrom, R. (2011) Pirate Culture and Hactivist Mobilization: The Cultural and Social Protocols of #WikiLeaks on Twitter. *New Media & Society*. 13(6) 999-1018.

Lockton, D. (2012). Persuasive Technology and Digital Design for Behavior Change. Working Paper, Paper ID: 2125957, Aug 2012.

Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance*. Malden, Ma: Polity

Press

Lyotard, J. F. (1984). The Postmodern Condition. (G. Bennington & B. Massumi trans). Manchester, UK: University Press.

MacAskill, E. (2013, Aug 23). NSA paid millions to cover Prism compliance costs for tech companies. *The Guardian*. Retrieved from www.theguardian.com/world/2013/aug/23/nsa -prism-costs-tech-companies-paid

MacAskill, E. & Dance, G. (2013). NSA Files: Decoded What the revelations mean for you. *The Guardian*. Retrieved from www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Mann, C. (2011, December 20). Smoke Screening. *Vanity Fair*. Retrieved from: http://www.vanityfair.com/culture/features/2011/12/tsa-insanity-201112

Mann, S. (1998). Reflectionism and Diffusionism. *Leonardo*. 31(2) 93-102.

Marcos, C. (2015, January 16). Bill would end birthright citizenship. *The Hill*. Retrieved from:http://thehill.com/blogs/floor-action/house/229778-bill-would-end-birthright-citizenship

Markham, T. (2014). Social Media, Protest Cultures and Political Subjectivities of the Arab Spring, *Media, Culture & Society*. 36(1) 89-104.

Mayer, J. (2007). The Black Sites. *The New Yorker*. Retrieved from http://www.newyorker.com/magazine/2007/08/13/the-black-sites

McAlister, J. F. (2010) Domesticating Citizenship: The Kairotopics of America's Post-9/11 Home Makeover, *Critical Studies in Media Communication*, 27:1, 84-104,

DOI:10.1080/15295030903554391.

Memphis Police Department (2014). *Memphis PD Initiatives*. Retrieved from http://www.memphispolice.org/initiatives.asp

Mercieca, J. (2010). *Founding Fictions*. Tuscaloosa, AL: The University of Alabama Press

Military Commissions Act of 2006, 10 42 U.S.C. § 948-949 (2006). Retrieved from https://www.gpo.gov/fdsys/pkg/BILLS-109s3930enr/pdf/BILLS-109s3930enr.pdf

Miller, G. (2010). Muslim cleric Aulaqi is 1st U.C. citizen on list of those CIA is allowed to kill. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040604121.html

Miller, G. (2012, October 23). Plan for hunting terrorists signals U.S. intends to keep adding names to kill lists. *The Washington Post*. Retrieved from the Washington Post website: http://www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signals-us-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html

Miller, T. (1993). *The Well-Tempered Self: Citizenship, Culture, and the Postmodern Subject*. Baltimore, MD: John Hopkins University Press.

Morozov, E. (2014). The Rise of Data and the Death of Politics. *The Observer*, Retrieved From http://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics- evgeny-morozov-algorithmic-regulation

Mortensen, M. (2014). Who is Surveilling Whom? Negotiations of surveillance and

sousveillance in relation to WikiLeaks' release of the gun camera tape Collateral Murder, *Photographies*, 7:1, 23-37, DOI: 10.1080/17540763.2014.896144.

Mueller, J. E. (2006). *Overblown: How politicians and the terrorism industry inflate national security threats, and why we believe them*. New York, NY: Free Press.

Nealon, J. (2012). *Post-Postmodernism or, the Cultural Logic of Just-in-Time Capitalism*. Stanford, CA: Stanford University Press.

New York Science (2012). *THINK: The Process of Innovation*. Retrieved from http://teacherstryscience.org/units/think-process-innovation

O'Reilly, T. (2008, October 29). *Why I Support Barack Obama*. Retrieved from: http://radar.oreilly.com/2008/10/why-i-support-barack-obama.html

O'Reilly, T. (2008, November 3). *Is a Political Endorsement Appropriate for a Technical Site?* Retrieved from: http://radar.oreilly.com/2008/11/political-endorsement-appropriate-tech-sites.html

O'Reilly, T. (2010) Government as a Platform. *Innovations*. 6(1).

O'Reilly, T. (2013) *Open Data and Algorithmic Regulation, in Beyond Transparency: Open Data and the Future of Civic Innovation*, (Ed. Goldstein, B. & Dyson, L.) San Francisco, CA: Code for America Press

Obama, B. (2007, June 22). Remarks of Senator Barack Obama: Taking Our Government Back. *Obama '08 Campaign* [website]. Retrieved from web.archive.org/web/20080731232126/http://www.barackobama.com/2007/06/22/remarks_of_senator_barack_obam_17.php

Obama, B. (2008, May 13). *Obama Economic Town Hall*. [Video]. Retrieved from

http://www.c-span.org/video/?205351-1/obama-economic-town-hall

Obama, B. (2008, Sept. 22). *The Change We Need in Washington*. Remarks of Senator Barack Obama. Retrieved from http://speeches.demconwatchblog.com/2008/09/barack-obama-speech-from-green-bay-wi.html#jumpto

Obama for America (2008). *The Blueprint For Change: Barack Obama and Biden's Plan for America*. Retrieved from www.barackobama.com

Office of the Attorney General. (2013, March 4). *Attorney General's Letter to Rand Paul*. Retrieved from http://www.paul.senate.gov/files/documents/BrennanHolderResponse.pdf

Office of the President-Elect (ND). The Obama-Biden Plan. Retrieved from http://change.gov/agenda/ethics_agenda/

Packer, J. (2006) Becoming Bombs: Mobilizing Mobility in the War on Terror, *Cultural Studies*, 20(4), 378-399.

Packer, J. (2007). Homeland Subjectivity: The Algorithmic Identity of Security. *Communication and Critical/Cultural Studies*. 4(2) 211-215.

Packer, J. (2013) Screens in the Sky: SAGE, Surveillance, and the Automation of Perceptual, Mnemonic, and Epistemological Labor. *Social Semiotics*. 23(2), 173-195.

Parry-Giles, S., & Parry-Giles, T. (2000). Collective memory, political nostalgia, and the

rhetorical presidency: Bill Clinton's commemoration of the March on Washington August 28, 1998, *Quarterly Journal of Speech*, 86:4, 417-437, DOI: 10.1080/00335630009384308.

Phillips, M. (2011, May 2). Osama Bin Laden Dead. *Remarks by the President on Osama Bin Laden*. Retrieved from https://www.whitehouse.gov/blog/2011/05/02/osama-bin-laden-dead

Pieterse, N. (2012). Leaking Superpower: WikiLeaks and the Contradictions of Democracy, *World Quarterly,* 33(10), 1909-1924, doi 10.1080/01436597.2012.728324.

Priest, D. (2013, July 21). NSA growth fueled by need to target terrorists. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed b9b6fe264871_story.html

prism. 2016. In *Merriam-Webster.com*. Retrieved February 16, 2016 from http://www.merriam-webster.com/dictionary/prism

prism. 2016. In *Oxford Dictionaries*. Retrieved February 16, 2016 from http://www.oxforddictionaries.com/us/definition/american_english/prism

Providing material support or resources to designated foreign terrorist organizations, 2006, 18 U.S.C. §2339B p.542-545.

Purdy, M. & Bergman, L. (2003). WHERE THE TRAIL LED: Between Evidence and

Suspicion; Unclear Danger: Inside the Lackawanna Terror Case. *New York Times*. Retrieved from http://www.nytimes.com/2003/10/12/nyregion/where-trail-led-between-evidence-suspicion-unclear-danger-inside-lackawanna.html?pagewanted=1

Risen, J., & Johnston, D. (2002). Bush Has Widened Authority of C.I.A. To Kill Terrorists. *New York Times*. Retrieved from www.nytimes.com/2002/12/15/international/15INTE.html

Risen, J., & Lictblau, E. (2005, Dec. 16). Bush Lets U.S. Spy on Callers Without Courts. *New York Times*. Retrieved from www.nytimes.com/2005/12/16/politics/16program.html?pagewanted =all&_r=0

Rodriquez, G. (2013). Edward Snowden Interview Transcript. *MIC*. Retrieved From: http://mic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism

Rotella, S. (2013). Boston Bombing Suspects Echo Home-Grown Terrorists in Madrid, London Attacks. *ProPublica*. Retrieved from http://www.propublica.org/article/boston-bombing-suspects-echo-home-grown-terrorists-in-madrid-london-att#tsarnaev-spelling

Scahill, J., & Greenwald, G. (2014, February 9). The NSA's Secret Role in the U.S. Assassination Program. *The Intercept*. Retrieved from theintercept.com/2014/02/10/the-nsas-secret-role/

Schneier, B. (2009). Is aviation security mostly for show? *CNN*. Retrieved from: http://edition.cnn.com/2009/OPINION/12/29/schneier.air.travel.security.theater/

Scholz, T. (2008) *Where the Activism Is. In Digital Media and Democracy: Tactics in Hard Times*, (Ed. Megan Boler). Cambridge, MA: MIT Press.

Shamsi, H, & Harwood, M. (2014, November 6). How Surveillance Turns Ordinary People into Terrorism Suspects. *Mother Jones.* Retrieved from http://www.motherjones.com/politics /2014/11/ how-surveillance-turns-ordinary-people-terrorism-suspects

Shane. S. (2015). Homegrown Extremists Tied to Deadlier Toll than Jihadists in U.S. Since 9/11. *New York Times*. Retrieved from http://www.nytimes.com/2015/06/25/us/tally-of-attacks-in-us-challenges-perceptions-of-top-terror-threat.html?mabReward=A4&_r=3

Shane, S. (2015). Drone Strikes Reveal Uncomfortable Truth: U.S. Is Unsure About Who Will Die. *New York Times*. April 23, Retrieved from www.nytimes.com/2015/04/24/world /asia/drone-strikes-reveal-uncomfortable-truth-us-is-often-unsure-about-who-will-die.html?_r=0

Shaw, I. (2013). Predator Empire: The Geopolitics of US Drone Warfare. *Geopolitics*. 00, 1-24, doi:10.1080/14650045.2012.749241.

Said, E. (2001, October 22). The Clash of Ignorance. The Nation. Retried from http://www.thenation.com/article/clash-ignorance/

Sloop, J. (2009). People Shopping. In B. Biesecker & Lucaites, J. (Eds), *Rhetoric, Materiality, and Politics* (43-66). New York, NY: Peter Lang.

Soltani, A., Peterson, A., & Gellman, B. (2013). NSA uses Google cookies to pinpoint

targets for hacking. *Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the- switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/

Springer, S., Chi, H., Crampton, J., McConnell, F., Cupples, J., Glynn, K., Warf, B., & Attewell, W. (2012) Leaky Geopolitcs: The Ruptures and Transgressions of WikiLeaks, *Geopolitics*, 17(3) 681-711, doi:10.1080/14650045.2012.698401.

Snowden, E. (2016, May 3). Inside the Assassination Complex: Whistleblowing Is Not Just Leaking — It's an Act of Political Resistance. *The Intercept*. Retrieved from https://theintercept.com/2016/05/03/edward-snowden-whistleblowing-is-not-just-leaking-its-an-act-of-political-resistance/

Stahl, R. (2006). Have You Played the War on Terror? *Critical Studies in Media Communication*. 23(2) 112-130.

Stahl, R. (2010). *Militainment, INC. War, Media, and Popular Culture*. New York, NY: Routledge.

Star, P. (2013). 11,588,500 Words: Obamacare Regs 30x as Long as Law. *CNSNews*. Retrieved from http://cnsnews.com/news/article/penny-starr/11588500-words-obamacare-regs-30x-long-law

Sweet, L. (2007). Sweet blog special: Obama transparency speech. *Chicago Sun-Times*. Retrieved from blogs.suntimes.com/sweet/2007/09/sweet_blog_special_obama_ trans .html

Talks at Google. (2007, November 14). *Barack Obama / Candidates at Google* [Video File]. Retrieved from https://www.youtube.com/watch?v=m4yVlPqeZwo

Tau, B. (2015, January 11). White House to Convene Summit on Violent Extremism To Highlight Efforts to Stop Extremists from 'Radicalizing, Recruiting, or Inspiring Individuals'. *Wall Street Journal*, Located at http://www.wsj.com/articles/white-house-to-convene-summit-on-violent-extremism-1420991097

Tay, G. (2009) *Exceptional Web Experience with Government Services*. Retrieved from ftp://public.dhe.ibm.com/software/ph/pdf/3.Govt_Gavin_Tay_Experience_with_Government_Web_Services.pdf

Tewksbury, D. (2012). Crowdsourcing Homeland Security: The Texas Virtual Border Watch and Participatory Citizenship. *Surveillance & Society*. 10(3/4): 249-262.

Toor, A. (2014).Why a messaging app meant for festivals became massively popular during Hong Kong protests. *The Verge*. Retrieved from: www.theverge.com/2014/10/16/698112 7/firechat-messaging-app-accidental-protest-app-hong-kong

Transportation Security Administration. (2014, November 13). *How to Get Through the Line Faster*. Retrieved from the Official Website of the Department of Homeland Security: http://www.tsa.gov/traveler-information/how-get-through-line-faster

Transportation Security Administration. (2014, September 3). *Advanced Imaging Technology*. Retrieved from the official website of the Department of Homeland Security: http://www.tsa.gov/traveler-information/advanced-imaging-technology

Transportation Security Administration. (2014, July 28). *If You See Something, Say Something™*. Retrieved from the Official website of the Department of Homeland

Security: http://www.tsa.gov/if-you-see-something-say-something

Transportation Security Administration (2014, July 16). *Pat-Downs*. Retrieved from the Official website of the Department of Homeland Security: http://www.tsa.gov/traveler-information/pat-downs

U.S. Department of Justice, Office of legal Counsel, Office of the Assistant Attorny General. (2010, July 16). *Memorandum for the Attorney General. Re: Applicability of Federal Criminal Laws and the Constitution to Contemplated Lethal Operations Against Shaykh Anwar al-Aulaqi.* Retrieved from www.aclu.org/sites/default/files/field_document/2014-06-23_barron-memorandum.pdf

U.S. Department of Justice. (2006, January 19). *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*. Retrieved from:www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pdf

U.S. Department of Justice. (2015). *Investigation of the Ferguson Police Department*. Retrieved from http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf.

U.S. National Commission on Terrorist Attacks upon the United States (2004). *9/11 Commission Report: The Official Report of the 9/11 Commission and Related Publications.* Prepared by Thomas H. Kean and Lee Hamilton. Y 3.2:T 27/2/FINAL. Washington, D.C.: GPO.

U.S. Senate. Committee on Foreign Relations. (2009). *Tora Bora Revisited:: How We*

Failed To Get Bin Laden and why it Matters Today. (S. Rpt. 111-35). Washington: Government Printing Office, 2009. Retrieved from http://www.gpo.gov/fdsys/pkg/CPRT-111SPRT53709/html/CPRT-111SPRT53709.htm

U.S. Senate. Rand Paul (R-KY). (2013). *Brennan Nomination*. (S. Rec. S1150). Washington: Government Printing Office, 2013. Retrieved http://thomas.loc.gov/cgi-bin/query/C?r113:./temp/~r113c84yn7

Virilio, P. (2007). *Strategy of Deception*. (Trans. Chris Turner). New York, NY: Verso.

Virilio, P. & Lotringer, S. (1997). *Pure War*. Los Angeles, CA: Semiotext(e).

Volz, D. (2014) British Spies Allowed to Access U.S. Data Without a Warrant. *National Journal*. Retrieved from http://www.nationaljournal.com/tech/british-spies-allowed-to- access-u-s-data-without-a-warrant-20141028

Washington Post. (2013, June 6). Monitoring a target's communication. Retrieved from http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

WeAreChange. (2012). *Obama's Top Adviser Robert Gibbs Justifies Murder of 16 Year Old American Citizen*. [Video File]. Retrieved from www.youtube.com/watch?v=7MwB2zn BZ1g

Weber, R. (2014, March 14). A Letter to Our Clients About Government Access to Data. *IBM* Retrieved from http://asmarterplanet.com/blog/2014/03/open-letter-data.html

White House, Office of the Press Secretary. (2001, September 11). *Statement by the President in His Address to the Nation.* Retrieved from http://georgewbush-

whitehouse.archives.gov/news/releases/2001/09/20010911-16.html

White House, Office of the Press Secretary. (2001, Sept 14). *President's Remarks at National Day of Prayer and Remembrance*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010914-2.html

White House, Office of the Press Secretary. (2001, September 15). *President Urges Readiness and Patience: Remarks by the President, Secretary of State Collin Powell and Attorney General John Ashcroft.* Retrieved from georgewbushwhitehouse.archives.gov/news/releases/2001/09/20010915-4.html

White House, Office of the Press Secretary. (2001, September 15). *Radio Address of the President to the Nation*. Retrieved from georgewbush-whitehouse.archives.gov/news/ releases/2001/09/20010915.html

White House, Office of the Press Secretary (2001, Sept. 17). *Guard and Reserves "Define Spirit of America"* Retrieved from georgewbush-whitehouse.archives.gov/news/releases /2001/09/20010917-3.html

White House, Office of the Press Secretary. (2001, Sept. 18). *President Signs Authorization for use of Military Force bill. Statement by the President.* Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010918-10.html

White House, Office of the Press Secretary, (2001, Sept. 20). *Address to a Joint Session of Congress and the American People*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html

White House, Office of the Press Secretary. (2001, September 27). *At O'Hare, President*

Says "Get On Board" Remarks by the president to Airline Employees. Retrieved from: georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010927-1.html

White House, Office of the Press Secretary. (2001, Oct. 26). *President Signs Anti-Terrorism Bill. Remarks by the President at Signing of the Patriot Act, Anti-Terrorism Legislation.* Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2001 /10/200 11026-5.html

White House, Office of the Press Secretary. (2001, December 11*). President Speaks on War Effort to Citadel Cadets*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2001/12/20011211-6.html

White House, Office of the Press Secretary (2002, January 29). *The President Delivers State of the Union Address*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/ releases/2002/01/20020129-11.html

White House, Office of the Press Secretary (2002, March 12). *Gov. Ridge Announces Homeland Security Advisory System*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2002/03/20020312-1.html

White House, Office of the Press Secretary (2006, May 15). *President Bush Addresses the Nation on Immigration Reform*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2006/05/20060515-8.html

White House, Office of the Press Secretary. (2002, July 3). Expedited Naturalization Executive Order. *The White House Archives*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2002/07/20020703-24.html

White House, Office of the Press Secretary. (2003, Jan 28). *President Delivers "State of the Union"*. Retrieved from http://georgewbush whitehouse.archives.gov/news/releases/2003/01/20 030128-19.html

White House, Office of the Press Secretary. (2003, Feb 14). *Fact Sheet: Strengthening Intelligence to Better Protect America.* Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2003/02/20030214-1.html

The White House President George Bush. (2003, Feb 14). *President Speaks at FBI on New Terrorist Threat Integration Center*. Retrieved from georgewbush-whitehouse.archives.gov/news/releases/2003/02/20030214-5.html

White House, Office of the Press Secretary. (2005, July 9) *President's Radio Address*. White House Radio. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2005/07/20050709.html

White House, Office of the Press Secretary. (2005, August 13*) President's Radio Address*. White House Radio. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases /2005/08/20050813.html

White House, Office of the Press Secretary. (2005, August 20) *President's Radio Address*. White House Radio. Retrieved from http://georgewbush-whitehouse.archives.gov/newsreleases/2005/08/20050813.html)

White House, Office of the Press Secretary (2005, Dec. 17). *President's Radio Address*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/200 51217.html

White House, Office of the Press Secretary (2006, Jan. 22). *Setting the Record Straight: Democrats Continue to Attack Terrorist Surveillance Program*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2006/01/20060122.html

White House, Office of the Press Secretary (2006, January 23). *President Discusses Global War on Terror at Kansas State University*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2006/01/20060123-4.html

White House, Office of the Press Secretary. (2006, Jan. 31). *President Bush Delivers State of the Union Address*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2006/01/20060131-10.html

White House, Office of the Press Secretary. (2006, March 25). *Executive Order 13292*. Retrieved from http://www.fas.org/sgp/bush/eoamend.html

White House, Office of the Press Secretary. (August 31, 2006). *President Bush Addresses American Legion National Convention*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2006/08/20060831-1.html

White House, Office of the Press Secretary. (2006, Sept. 5). *President Discusses Global War on Terror*. Retrieved from georgewbush-whitehouse.archives.gov/news/releases/2006/09 /20060905-4.html

White House, Office of the Press Secretary (2006, Sept. 6). *President Discusses Creation*

of Military Commissions to Try Suspected Terrorists. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2006/09/20060906-3.html

White House, Office of the Press Secretary. (2007, January 21*). Vice President's Remarks at a Rally for the Troops*. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2007/02/text/20070221-5.html

White House, Office of the Press Secretary (2009, Jan 21). *Remarks of the President in Welcoming Senior Staff and Cabinet Secretaries to the White House*. Retrieved from https://www.whitehouse.gov/the-press-office/remarks-president-welcoming-senior-staff-and-cabinet-secretaries-white-house

White House, Office of the Press Secretary. (2010, July 27). *Remarks by the President After bipartisan Leadership Meeting*. Retrieved from https://www.whitehouse.gov/the-press-office/remarks-president-after-bipartisan-leadership-meeting

White House, Office of the Press Secretary. (2010, July 25). *Statement of National Security Advisor General James Jones on Wikileaks*. Retrieved from https://www.whitehouse.gov/the-press-office/statement-national-security-advisor-general-james-jones-wikileaks

White House, Office of the Press Secretary. (2011, May 2). *Press Briefing by Senior Administration Officials on the Killing of Osama bin Laden. Press Release*. Retrieved from https://www.whitehouse.gov/the-press-office/2011/05/02/press-briefing-senior-administration-officials-killing-osama-bin-laden

White House, Office of the Press Secretary. (2011, Aug 3). *Empowering Local Partners to Prevent Violent Extremism in the United States*. Retrieved from www.whitehouse.gov/ the-press-office/2011/08/03/empowering-local-partners-prevent-violent-extremism-united-states

White House, Office of the Press Secretary. (2011 Sept. 30). *Remarks by the President at the "Changes of Office" Chairman of the Joint Chiefs of Staff Ceremony*. Retrieved from https://www.whitehouse.gov/the-press-office/2011/09/30/remarks-president-change-office-chairman-joint-chiefs-staff-ceremony

White House, Office of the Press Secretary. (2013, Aug. 9). *Remarks by the President in a Press Conference*. Retrieved from https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference

The White House, Office of the Press Secretary. (2013, Aug. 9). *Background on the President's Statement on Reforms to NSA Programs*. Retrieved from https://www.whitehouse.gov/the-press-office/2013/08/09/background-president-s-statement-reforms-nsa-programs

White House, Office of the Press Secretary. (2014, January 17). *Remarks by the President on Review of Signals Intelligence*. Retrieved from www.whitehouse.gov/the-press- office/2014/01/17/remarks-president-review-signals-intelligence

White House, Office of the Press Secretary. (2014, August 1). *Press Conference by the*

President. Retrieved from https://www.whitehouse.gov/the-press-office/2014/08/01/press-conference-president

White House, Office of the Press Secretary (2015, Apr. 23). *Statement by the President on the Deaths of Warren Weinstein and Giovanni Lo Porto*. Retrieved from https://www.whitehouse.gov/the-press-office/2015/04/23/statement-president-deaths-warren-weinstein-and-giovanni-lo-porto

Woodward, B. (2001). CIA Told to Do 'Whatever Necessary' to Kill Bin Laden. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/11/18/AR2007111800655.html

Yoo, J. (2011/12). Assignation or Targeted Killings After 9/11. *New York Law School Law Review*. 56, p.57-79.

Zarefskey, D. (2004). Presidential Rhetoric and the Power of Definition. *Presidential Studies Quarterly*. 34(3) 607-619.

ABSTRACT

INTERACTIVE SECURITY: THE RHETORICAL CONSTITUTION OF ALGORITHMIC CITIZENSHIP IN WAR ON TERROR DISCOURSE

by

AVERY J. HENRY

August 2016

Advisor: Dr. Kelly Young

Major: Communication

Degree: Doctor of Philosophy

This dissertation traces algorithmic citizenship as it is constituted through war on terror discourse. Utilizing Ron Greene's rhetorical materialism, this project analyzes corporate discourse along with presidential address and policy to map how they interpellate citizens' subjectivity. Specifically, the dissertation follows George Bush's presidential rhetoric as he defines the war on terror and invites the public to participate. Then the dissertation examines how the political discourse associated with government 2.0 is also an economic discourse that works to articulate citizenship alongside consumerism. The next chapter follows the presidential rhetoric of Barack Obama as he intensifies the surveillance and war fighting rhetoric identified with George Bush and IBM. Finally, the dissertation maps the communicative function and role played by whistleblowers and theorizes how the interactive values of government 2.0 and algorithmic citizenship offer the potential for rhetorical agency.

AUTOBIOGRAPHICAL STATEMENT

Avery Henry was born on October 7, 1984. He grew up in Guymon, Oklahoma where he graduated high school. Afterwards, Henry attended the University of Central Oklahoma, where he received a Bachelor of Arts Degree in Sociology. Henry then attended the University of Louisiana-Lafayette and earned a Master of Science degree in Communication Studies. Avery then worked on his doctoral degree at Wayne State University. Currently, he is an Assistant Professor of Public Address/Debate in the Communication Studies department at Southeast Missouri State University.