Individual Freedom versus Security:
An Unintended Casualty of the Battlefield

"Those who surrender freedom for security will not have,
nor do they deserve, either one." – Benjamin Franklin

The 21st century battlefield is truly unlike any other that we have witnessed. It is a time when the world has to contend not just with nation-state belligerents, but also with the proliferation of non-state, non-uniformed combatants.

We have named this current conflagration as the "War on Terror." However, that is a horrible misnomer if you comprehend exactly the essence of terrorism and its objective. Terrorism is a tactic for achieving a goal—a means to an end. A nation cannot embark upon a combat operation against a tactic. To use a parallel, World War II was not the "War on the Blitzkrieg" or the "War on the Kamikaze." Rather, a nation goes to war against an ideology that is antithetical to its fundamental principles and threatening to its existence. America gained its independence fighting against the governing philosophy of a monarchy. The major world wars in which our nation has participated since then were against German nationalism, Nazism, fascism, Japanese imperialism, and communism. At odds were always two competing ideals, value systems, and a quest for freedom against global domination.

Today America, and indeed the world, finds itself in the grips of an ideology that is not defined by borders or boundaries. It is a movement that transmits freely and masks itself well in order to infiltrate into nations and societies, in a cancerous manner, seeking to destroy its host. There are too many who, to their detriment, are afraid to identify this enemy, in the name of political correctness. For it was ancient military theorist Sun Tzu who stated in his seminal book *The Art of War*, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Our greatest issue on this new global battlefield is that we are reticent to call the enemy what they really are –Islamic jihadists. This is an enemy that purposefully targets civilians for death. This is an enemy that operates within civilian society and, against western nations, leverages our very principles and liberties against us. Our confusion in understanding this battlefield has led us to view the enemy in ambiguous euphemisms, rather than identifying them for precisely what they are.

We are intentionally failing to do the most basic thing in conducting a war – identifying and understanding the enemy. It is a very perplexing dilemma: we hold our individual freedoms in such high regard that, when confronted with an enemy who uses our liberties to mask their intentions and hide in plain sight, we recoil from confrontation. We are told to be tolerant of the intolerant, and policies are created that almost provide an advantage for our adversaries.

Sun Tzu's quote is so very applicable to where we are today, and nowhere is it more clear than in the classic struggle to balance liberty and security.

I was born in Atlanta in 1961. I remember taking school field trips to Atlanta Hartsfield Airport to watch the planes and have guided tours. Heck, even my Dad would take me out sometimes. That would be our bonding time, to sit and watch the planes take off and land. I remember the days where the entire family could go to the airport with their loved ones and sit at the gate, watching them board their flight. All of that changed in one day.

On September 11, 2001, I was a Major in the US Army stationed at Camp Lejeune, North Carolina, on an exchange assignment to the II Marine Expeditionary. I had finished morning physical training, showered, and was in my office putting on my camo uniform, when the phone rang. It was my Marine counterpart at US Marine Forces Atlantic headquarters in Virginia. He told me to get to the TV-- something very bad was happening. I finished donning my uniform and headed into the Operations Center in time to see the second plane strike the World Trade Center tower. Later we got the word about a plane striking the Pentagon – it hit the Army wing, and I had several friends who were there. Finally, we learned of the plane that crashed in the fields of Pennsylvania. That night was one of the most eerie nights ever: no flights taking off, no flittering lights of aircraft.

Now, some 14 years later, I would portend that something even more eerie is happening in America. In our refusal to identify the enemy, we have done exactly what the terrorists desired:

restrain American liberties in the name of security. We have created more government agencies and even, in some cases, turned the power of the federal government against the American people.

Rather than subjecting the entire citizen populace to constant government surveillance, we should consider using smart trend analysis. This means conducting extensive surveillance only on those individuals who present specific patterns of behavior and characteristics that are strongly associated with terrorist activity. We are not talking about monitoring all Muslims, or anyone who has recently flown to the Middle East, or anything so simplistic. Trend analysis is much more sophisticated than that. A person selected for surveillance would be someone who fits into a large number of high-risk data points. Academics, policymakers, and military and law enforcement experts have numerous tools for identifying individuals who pose a significant risk of violent behavior. Putting these techniques to work, we could cull down the pool of surveillance targets, preserving both civil liberties and our vital, finite anti-terror resources.

For example, during my combat tour in Iraq, intelligence revealed that most IEDs in Iraq were placed at night by young men riding dirt bikes from certain rural areas. Therefore as we developed patrol tactics, techniques, and procedures in our designated area of operations, tasked with monitoring possible threats, we had some idea of what the indicators and warning signs were. We weren't going to worry too much about children or elderly people riding bikes, or families leaving the city, or even young men cruising around mid-day – unless there were multiple riders with their faces covered. However, when we observed a group of young men riding dirt bikes into

the darkness past 11pm, we were inclined to further investigate. This does not mean assuming all Iraqi young men with dirt bikes are terrorists, but rather identifying when numerous seemingly-unrelated factors line up to suggest a dangerous pattern.

To use the old "needle in a haystack" expression, current policy is as if someone decided that, instead of focusing on a small stack of needles (individuals likely to be terrorists), we needed to dump a big pile of hay (everyone else) on top, so as not to offend the needles. And with the impact of the hay falling upon them, the needles dispersed.

As the Benjamin Franklin quote in the introduction asserts, this discussion is not a new one. There is a careful balance needed, so that we don't put in chains that which defines our free society-- individual liberty-- in attempt to provide a more secure environment. Is it necessary to "dragnet" an entire nation for the sake of targeting a specific enemy? While we must learn from past discriminatory mistakes, such as internment of Japanese citizens during World War II, we also must not fret over conducting quality intelligence-gathering based upon trend analysis. Surveillance should be narrowly focused on the most likely offenders, not vacuuming up information on every American citizen. What I describe is not "profiling," it is smart allocation of resources.

This debate topic paper will analyze the history of intelligence-gathering and surveillance in America, and assess when and where this seminal domestic conflict between liberty and security has occurred. We will look at the affirmative and the negative arguments on surveillance in America as part of the new 21st-century battlefield. It is a critical issue, as reducing our individual liberties

and causing us to live in a state of fear represents a victory for the enemy. This, after all, is the primary goal of a terrorist: to cause terror.

A Brief History of Government Surveillance

"Enlightened rulers and good generals who are able to obtain intelligent agents as spies are certain for great achievements." – Sun Tzu, "The Art of War"

Government surveillance is as old as history itself. The ancient Israelites employed spies to gather intelligence on the people of Jericho before their attack. Historical leaders from Julius Caesar to Queen Elizabeth I used covert tactics to attempt to thwart their enemies. Intelligence, after all, offers a substantial strategic advantage.

During the French Revolution, Maximillien Robespierre and his cohort watched the population with a careful eye. In 1793, the revolutionary government established 12-member "committees of surveillance" throughout the country. They were authorized to identify, monitor, and arrest any suspicious former nobles, foreigners, and nationals who had recently returned from abroad, as well as suspended public officials, and many others.

It is quite apparent that this type of government surveillance was more political in nature than concerned with national security. Then again, perhaps this is the same argument we face today

in America – how to define national security, and how much intelligence is needed to protect it. Further, are surveillance programs instituted in wartime temporary in nature, or do they become permanently part of our "free society"?

It was not too long after Robespierre's committees of surveillance that the same issue reared its head in our very new Republic, America. Interestingly enough, American surveillance was to come as the nation prepared for a possible conflict with France – our allies during the Revolutionary War.

In 1798, the Congress of the United States passed what were to be known as the "Alien and Sedition Acts". This legislation was supported under the guise of controlling activities of foreigners at a time when Americans believed a war with France was impending. These new laws were broken down into four parts. The first was the Naturalization Act, which extended the residency requirement period for citizenship from five to fourteen years. The second was the Alien Act, which allowed for the expulsion of aliens deemed dangerous during peacetime. The third was the Alien Enemies Act, which allowed the expulsion or imprisonment of aliens deemed dangerous during wartime. The fourth and final law was the Sedition Act, which provided fines or imprisonment for individuals who criticized the government, Congress, or President in speech or print.

The real goal, some would say, was completely political, in that it was aimed at hindering the Jeffersonian Republicans, the opposition political party of the Federalists, who controlled Congress at the time. The naturalization act did have an effect upon some Irish and French

immigrants, who leaned towards the Jefferson Republicans. As well, the alien enemies act was never actually enforced, but it did persuade some Frenchmen to return to France. The Sedition Act was enforced, in complete violation of the First Amendment right of freedom of the press. Some Jeffersonian Republican newspaper publishers were convicted under the terms of this law. The Sedition Acts advanced surveillance and punishment of foreigners, as well as critics of the policies of the Federalists. The Federalists justified this under the ruse of national security: the potential of war with France. The Sedition Act specifically targeted the individual freedoms of Americans by "prohibiting assembly with intent to oppose any measure…of the government," and made it illegal for a person to "print, utter, or publish…any false, scandalous, and malicious writing against the government." Therefore, early in our nation's existence, we saw the clash between individual freedom and security (or, perhaps, the ruse of security).

During the Civil War, we witnessed another episode in our history where civil liberties clashed with the imperative of national security. It was during those tumultuous years, when the future of the American Union was held in the balance, that President Abraham Lincoln declared martial law and authorized military tribunals to try individuals who could be deemed as "terrorists"-- non-uniformed belligerents. There are those who contend that the measures President Lincoln took during the Civil War were extraordinary and unconstitutional. There are also those who believe his actions were justified in order to preserve the Union in a time of war.

One of the most controversial acts during this period was Lincoln's suspension of the writ of

habeas corpus. This is defined as a "procedural method by which one who is imprisoned can be immediately released if their imprisonment is found not to conform to law." Now, the US Constitution states in Article I, Section 9, Clause 2, "The privilege of the writ of habeas corpus shall not be suspended, unless when in cases of rebellion or invasion the public safety may require it." This enumerated power is listed in Article I of the Constitution, which applies to the Legislative branch-- the Congress. So, did President Lincoln usurp the authority of the US Congress in suspending the writ of habeas corpus? Or should we acquiesce to the President at a time of rebellion?

In April 1861, Lincoln's actions were challenged by a Maryland citizen named John Merryman. Merryman spoke out vehemently against the Union, favoring the South, and made the decision to raise a contingent of troops for the Confederacy. On May 25th, Merryman was arrested by the military – not civilian authorities – and imprisoned at Ft. McHenry for the charge of acts of treason. Merryman's counsel sought to challenge his imprisonment and went to Supreme Court Chief Justice Roger B. Taney seeking a writ of habeas corpus. Justice Taney did issue said writ for the Ft. McHenry Commanding Officer George Cadwalader, who refused, citing Lincoln's suspension of said writ. Justice Taney issued a statement of contempt of court for Cadwalader, but the issuing Marshal was not allowed to enter Ft. McHenry.

The Constitution does not specify who has the power to suspend the writ of habeas corpus. It is, however, listed in Article I, which articulates the enumerated powers of the Congress. It does

not appear in Article II, dealing with the Executive branch. Are we left to believe that, in times of dire circumstance and situations that threaten the public safety, extraordinary measures that adversely affect individual civil liberties could be warranted?

Later, as communications capabilities developed in America, an interesting case came forward: the 1928 case of Olmstead v. United States. It was here that the Supreme Court decided that evidence from wiretaps placed by federal officials without judicial approval is permissible and did not violate the Fourth Amendment, since the case involved phone conversations, rather than physical artifacts, and no federal agent trespassed on the accused's property. This judicial precedent was later overturned in the 1967 case of Katz v. United States. This was America's first encounter with legal dilemmas surrounding mass communications, individual freedom, and surveillance.

Later, the consequences of two World Wars meant that the United States became increasingly engaged in the business of surveillance. Project Shamrock began the concept of collecting metadata; it encompassed the collecting and monitoring all telegraph information in and out of the country. And Project Minaret created a "watch list" of US citizens suspected of "subversive" activities and monitored their actions.

It is clear that the issue we are now debating is nothing new. The question we must seek to answer is whether widespread suspension of individual rights and the proliferation of government surveillance is both constitutional and necessary. Who defines what is considered "subversive?" As

history has taught us, such power can be wielded for political purposes.

As the Cold War emerged, America realized that intelligence gathering in a mass communications global environment became a national security priority. To respond to this imperative, the federal government did as government nearly always does: it created a new agency.

The Emergence of the National Security Agency

If we are to understand any government agency or program, it is always best to trace its beginning and original mission. Therefore, it is relevant to consider the creation of the American National Security Agency (NSA). The NSA that we know today officially earned its name by way of National Security Council Intelligence Directive No. 9, dated 24 October 1952. This directive was executed by the Secretary of Defense on specific instructions from the President. So, what we first need to understand is that the NSA was not an agency developed by way of the legislative process, but by executive branch directive. There was a perceived need for an agency that could gather intelligence though new mass communications services. The United States was now fully invested in the business of not just simple cryptologic activities, but would expand beyond to the ideas of ELINT (Electronic Intelligence) and COMINT (Communications Intelligence) to what would become known as SIGINT (Signals Intelligence), a term adopted in 1958-1959.

In order to understand the development of the NSA, we must trace the organizations that precipitated its founding. In 1917, the US Army created a Cipher Bureau in its Military Intelligence Division in order to assist the radio intelligence units of the American Expeditionary Force deployed in France. The advent of radio communications made it necessary to develop a means by which enemy communications could be monitored. After the end of World War I, the bureau was used to extract intelligence from foreign diplomatic communications, and the expenses were shared by the Departments of State and War. In 1929, the State Department withdrew its financial support, and the Cipher Bureau ran its course and was eventually terminated. However, soon to come was World War II, so surveillance again became a priority. The US Army Signal Corps began training officers in the area of cryptology. This resulted in the creation of the Army's Signal Security Agency. Not to be outdone, the US Navy developed the first COMINT producing cryptographic unit, the Code and Signal Section (OP-20-G) in the Office of Naval Communications. COMINT was of tremendous importance during World War II, and its value continued to be recognized as the war ended and America entered into a post-war environment where the capabilities put in place during conflict are always reviewed and questioned.

As a result, it was decided to establish the Army-Navy Communications Intelligence Board with a subordinate committee. But post- World War II, it quickly became evident that the Soviet Union would not be an ally. So, it was President Harry Truman who authorized by executive order the Secretaries of War and Navy to collaborate with the British, as well as with other American government departments and agencies. The result was STANCIB (State-Army-Navy

Communications Intelligence Board) as the purveyor of COMINT activities. However, in government, agencies tend to grow in size. In June 1946, STANCIB was temporarily joined to the FBI and was renamed USCIB (United States Communications Intelligence Board). This name was retained even after the FBI dropped out of the program.

The following year, in 1947, a major change occurred in the executive branch: the President acquired what is known today as the NSC (National Security Council). By this time, we no longer had a War Department-- it has been renamed the Department of Defense, and subordinate Departments of the Army, Navy, and Air Force were created. The JCS (Joint Chiefs of Staff), previously only a wartime entity, was designated by statute as a standing military advisory body. Another new entity created at this time was the Central Intelligence Agency, whose precursors were the OSS (Office of Strategic Services) and the Central Intelligence Group.

In the coming years, SecDef (Secretary of Defense) James V. Forrestal "considered creating a one unified national cryptologic agency to obtain the desired results at the least cost. He appointed a special board under the leadership of US Navy RADM (Rear Admiral) Earl E. Stone, Director of Naval Communications, to formulate a plan for merging all military COMINT and COMSEC functions and resources in a single agency." As a result, on 20 May 1949, SecDef Forrestal directed the JCS to "establish the AFCIA (Armed Forces Communications Intelligence Agency) with accompanying advisory council." But, as with all acronyms in the military, there was a change, and the final agency was named AFSA (Armed Forces Security Agency). On 15 July 1949, RADM Stone became its first

director. AFSA was originally located in Washington DC and Virginia and was directed to relocate to a safer, less vulnerable site. So, on 1 February 1952, AFSA moved from its two locations and combined itself at Ft. George G. Meade in Maryland.

In its early days, AFSA was coming together at a time when the United States learned of the Soviet Union's ability to produce a nuclear bomb. There can be no debate that the Soviet threat was a primary impetus in the US assessment that COMINT collection was a necessary security tool. AFSA was also challenged early on with the advent of the Korean War – beginning in June 1950 -- and the issues of collaboration and coordination with SCAs (Service Cryptologic Agencies). At this time, there was a determined drop-off in the quality of COMINT information that had been garnered during World War II. AFSA was the fourth military cryptologic agency, and its controversies with SCAs were also felt by others such as the CIA and the State Department.

In December 1951, President Truman ordered another special committee to create a unified COMINT agency with greater powers. The "Brownell Committee," led by Mr. George A. Brownell, "proposed a unified agency controlled in policy matters by a reconstituted USCIB, under the chairmanship of the Director of the CIA, in which the representation of military and non-military intelligence assets would be evenly balanced." On 24 October 1952, the President and NSC adopted the Brownell Committee's recommendation. The ensuing result was that the "SecDef was ordered to delegate their COMINT responsibilities to the Director, NSA and entrust him with operational and technical control of all US COMINT resources." The NSA thus became subordinate to the SecDef.

We then saw the consolidation of what would become SIGINT gathering and collection activities under the one agency. What had begun as radio listening is now a mega government agency with the capability to gather huge swaths of information. Today's NSA has grown to keep pace with communications methods and global actors. The NSA "gathers intelligence by conducting surveillance on its adversaries through the collection of phone-call, emails, and internet data." The agency has two primary missions: preventing foreign adversaries from stealing sensitive or classified national security information from the United States (COMSEC responsibility) and collecting, processing, and disseminating information from foreign signals for counter-intelligence purposes (SIGINT responsibility).

The key question that emerges against this historical backdrop is, as this surveillance agency and the threats it monitors have grown, have our individual liberties and freedoms lessened? And should such a lessening be considered acceptable? Are we, the American citizenry, to be considered "adversaries"?

Should we Decrease and Limit Government Surveillance?

During my time in Congress, the Patriot Act came up for full reauthorization. I voted for a three-month extension to provide me an opportunity to study and understand the provisions better

and ascertain their effectiveness. I sent letters to the Head of the FBI, Director Mueller, as well as met with Congressional committee staff to gain information regarding my inquiries. When it came time for the full five year reauthorization vote, mine was a "No." I had not been convinced that these implemented protocols have been instrumental in deterring terrorist attacks in the homeland. There were two things that appeared evident to me: first, typical of all things government, we created a new agency. Second, following previous precedents, the civil liberties of the American people were offered upon the altar of security in response to a crisis event. The seminal question is whether or not we truly need to have this increased level of surveillance due to increasing terrorism.

Neil M. Richards, Law Professor at Washington University, writes in the Harvard Law Review, "First, surveillance is harmful because it can chill the exercise of our civil liberties…consider surveillance of other people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas". Of course, we know that the assessment of what is controversial and/or deviant is subjective – it could be based upon who is in political power at the time. Professor Richards continues, "A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms such as discrimination, coercion, and the threat of selective enforcement where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the

purpose of the surveillance." This premise was seen during the introduction, with the implementation of the Alien and Sedition Acts. As we established, these acts were begun under the guise of "security."

If surveillance efforts are begun with the intent of national security, perhaps the people can understand and accept. However, it seems that, while the original intent may be honorable – and yes, we can even question that –in the long term, the unintended consequences become great. This summer, we watched the horrific incident in which one 24-year-old Muslim man by the name of Youssef Muhammad Abdulazeez gunned down four US Marines and one US Sailor at a Navy Reserve Support Center in Chattanooga, Tennessee. We later learned that his own father had actually once been on the terrorist watch list. Why did surveillance fail to prevent this attack?

Or we can go back to June 2009, when a convert to Islam named Carlos Bledsoe shot two soldiers at a Little Rock, Arkansas recruiting station. In the same year, a man named Nidal Hasan gunned down thirteen soldiers and Army civilians and wounded another 31 – where were the surveillance resources in these cases? As a matter of fact, we came to learn that it was well known that Hasan had been communicating with Anwar al Awlaki, a known al-Qaeda recruiter who was later killed in a drone strike in Yemen. It was also known that Hasan was proselytizing about his militancy to soldiers entrusted to his care as patients.

The surveillance state also did not save a woman in Moore, Oklahoma from being beheaded by a coworker—in an act the government called "workplace violence."

It appears the government has instituted a policy of mass surveillance, but we still have major breaches of security – and that's before we even delve into cybersecurity. With so much surveillance, how is it that we still experience so many attacks?

A relevant question we need to ask is, who else is benefitting from the surveillance state? As Richards states, "Private industry is also marketing new surveillance technologies to the state. Since September 11th attacks, governments have been eager to acquire massive consumer and Internet-activity databases that private businesses have compiled for security and other purposes, either by subpoena or outright purchase." One has to laugh at this derivative of the free market's basic premise of supply and demand – it seems that the government surveillance state is demanding more access to our personal data and the private sector, which has been collecting it, is either willingly providing or being forced to supply the information.

But there are also costs to the private sector resulting from the surveillance state. Danielle Kehl is a policy analyst at New America's Open Technology Institute (OTI), and she, along with several colleagues, offer some insights. She writes, "American companies have reported declining sales overseas and lost business opportunities, especially as foreign companies turn claims of products that can protect users from NSA spying into a competitive advantage. The cloud computing industry is particularly vulnerable and could lose billions of dollars in the next three to five years as a result of NSA surveillance."

As well, there is a cost to our US foreign policy. Kehl continues, "Loss of credibility for the US

Internet Freedom agenda, as well as damage to broader bilateral and multilateral relations, threaten US foreign policy interests." Of course nations conduct surveillance activities against each other, but these seem to be a dramatic increase in surveillance, conducted even against even our own allies. If there is wholehearted concern about internet freedom because of NSA surveillance actions – mass date collection efforts – it could damage the free exchange of ideas not just in America, but indeed throughout the world.

Stopping illegal surveillance programs is also difficult. One of the great challenges for the individual is to present "standing" in any case confronting the government surveillance program. As Richards says, "Challenges to the NSA's wiretapping program have foundered because plaintiffs have failed to convince federal courts that secret surveillance has cause them legally cognizable injury. In ACLU v. NCA, the Sixth Circuit Court dismissed any suggestion that the First Amendment values were threatened when the government listened to private conversations. The court concluded that the plaintiffs has no standing to assert the First or Fourth Amendment violations, as they could not prove that the secret government program had targeted them."

Have we moved into an era where the individual American citizen can be classified as an "adversary" by their own government? There can be no doubt that we are truly living in a time of grave security concerns, but is increased government surveillance actually the answer to how we contend with this new environment? We have always had foreign agents operating in our country, since the day of the nation's inception. Today, however, the proliferation of the internet and social

media does present a new challenge to America's intelligence collection apparatus. But mass information data collection against the American people is not the answer.

Intelligence and information collection has to be focused – and reasonable. Requirements such as taking off shoes at the airport have grown from the sublime to the ridiculous. It only represents a deceptive façade of security – and the same may be true for the massive growth of the American surveillance state.

The Necessity of Government Surveillance

If we lived in a perfect world and man was angelic, we would not need security policy and surveillance. Since this is not the case, the new 21st century battlefield presents us with an incredible dilemma: how do we balance individual liberties against the collective security of the American people? Here on our own soil, we face an enemy that does not wear uniforms. They do not openly declare and carry their weapons. Because of the advanced communications technologies that we all enjoy, this enemy now has the ability to communicate, coordinate activities, and issue guidance, direction, and orders from across the globe. Government surveillance has always existed, but the new issue pertains to the level and extent it has an effect upon the everyday citizen.

John Yoo writes in the Harvard Journal of Law and Public Policy, "The Constitution vests the

President with the executive power and designates him as Commander-in-Chief. The Framers understood these powers to invest the executive with the duty to protect the nation from foreign attack and the right to control the conduct of military hostilities. To exercise those powers effectively, the President must have the ability to engage in electronic surveillance that gathers intelligence on the enemy. Regular military intelligence need not follow standards of probable cause for a warrant or reasonableness for a search…A warrant requirement for national security searches would reduce the flexibility of the executive branch, which possesses unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance."

The problem with the above statement is how to define the conflagration with militant Islamic terrorism in which America currently finds itself. We say "War on Terror," but, since a nation cannot fight a tactic, that is a misnomer. We damage our own efforts when we straddle the fence by treating counter-terror operations as akin to police action, and giving enemy combatants the rights of Americans. It appears that, due to the lack of a clear comprehension of this current battlefield, which has no borders or boundaries, we are playing a dangerous game of ad hockery when it comes to individual rights.

Yes, we have an enemy that resides amongst us. The best way to rectify this pressing dilemma is to cease the belief that "political correctness" should rule. We must have a government that conducts some form surveillance – from the standpoint of national security, that much cannot be debated. Should a terrorist attack be successful, the American people will demand: who was

responsible, what system failed? The people deserve a transparent response.

In a CNN article, former Head of the NSA Lieutenant General Keith Alexander stated, "information gathered from these programs provided government with critical leads to prevent over 50 potential terrorist events in more than 20 countries around the world". In the same article, Sean Joyce, the deputy Director of the FBI, addressed "how email surveillance of foreigners under one program helped authorities discover two New York City plots." In the fall of 2009, Joyce said, the NSA intercepted an e-mail from a suspected terrorist in Pakistan. That person was talking with someone in the United States about perfecting a recipe for explosives. Authorities identified Afghan-born Najibullah Zazi of Denver. The FBI followed Zazi to New York and eventually broke up his plan to attack the city's subway system. Zazi pleaded guilty and is currently in prison.

Here is a proof-positive example of a time when the government surveillance system worked and staved off a terrorist attack. The questions that remains: is it necessary to collect all metadata on all citizens in order to catch the Najibullah Zazi's that live here amongst us? Do we need to create additional procedures, such as the Patriot Act, or should we just ensure that the NSA is properly executing its duties within the established parameters?

Have we come to a time when we no longer have a right to privacy over communications? My position is that we should not subject law-abiding American citizens to the same status as our domestic and foreign enemy – unless there is significant cause to do so. We should, as a nation, stop operating on the basis that the enemy somehow possesses the right to privacy. We need not drop a

haystack over needles in order to give the needles a "fair chance" to hide. Through our refusal to conduct targeted surveillance, we in essence create our own difficulty. The solution I allude to is not "profiling"-- it is trend analysis. This should be the aim of our government surveillance program – not a massive infringement on the individual rights of everyone in order to avoid causing some offense to any group. In my assessment, that is the difference between a wide net and laser focus.

Let's face it, as long as there is an enemy, government surveillance is here to stay. The issue is to what level of disruption and impact upon the citizenry we should tolerate.

Conclusion

The first amendment of the US Constitution states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." The fourth amendment of the US Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Both of these grew out of the early experiences of the Founding

Fathers and their experience with the tyrannical rule of the British. They are consistent with the belief established in the Declaration of Independence regarding the absolute preeminence of individual rights.

Of those unalienable rights, the first is life, followed by liberty. The modern challenge we face, which the Founders did not, is the existence of massive communications networks and a vile, barbaric enemy that does not separate civilians from combat operations. America has always conducted surveillance on its perceived enemies and their accomplices, including fellow citizens – history shows this. But today's bulk surveillance is a very new experience for not just our country, but for the free world as a whole. We cannot eliminate the need for some degree of government surveillance. However, we also cannot become such alarmists that we suspend our prized individual rights in acquiescence to the false gods of political correctness.

The preeminent responsibility of the government is to protect its citizens and safeguard their individual liberties. The purpose of this research paper was not to provide a prescriptive, definitive policy answer, but rather to ask the reader to consider the history and contending sides of the issue. The ultimate recommendation is that we focus our surveillance assets on the enemy, using trend analysis techniques, and monitor American citizens only if there is probable cause.