

**The Surveillance State:
A Glance at the Structure, Constitutional and Societal Impacts, and
Solutions**

Contributing researchers:

Deeva Shah

Kirk Smith

J. Parker Gochenour

Margaret McCall

Carrie Filipetti

This report was created for The Rutherford Institute-Virginia Themis Society Research Program.

May 2009

Abstract

This paper is an in-depth study of the surveillance state in the United States after September 11th, 2001 and how it came into structure, the implications of it, and what solutions are available in order to restore privacy to American citizens. It also provides analysis on the constitutional basis for privacy and also provides a comparative examination of how American privacy rights compare to historical and foreign examples.

The first part of this paper addresses two major points: the structure of the surveillance state and also the structure of the surveillance itself. There is a breakdown of the federal government itself and what roles different branches and agencies have played and continue to play in the creation of the surveillance state. The second point considers the surveillance technologies and how they work and what they do exactly. Various surveillance technologies that are taken into account include wiretapping, biometrics, video-surveillance, infrared cameras, and satellites.

The second portion of this paper gives thought to the constitutionality of the surveillance state and what privacy rights have been given to citizens in the Constitution. This area addresses different court cases that have set the precedent for surveillance and searches in America and also how different surveillance technologies and the agencies that utilize them are violating the constitutional right to privacy. This leads into a comparison with South Africa and its use of surveillance during the apartheid.

Finally, the paper considers what solutions are available to increase individual privacy and what one must do as a citizen in order to change the government use of surveillance technologies. It addresses what capability America does have of becoming a surveillance state and what greater impacts this has on citizens and also on the national and international scale, looking both at long and short term effects.

Table of Contents

1. Abstract.....	.1
2. Table of Contents.....	2
3. Introduction.....	.3
4. Structure of the Surveillance State.....	3
5. Big Brother's Technologic Arsenal.....	16
6. The Surveillance State and Its Constitutionality.....	28
7. South Africa and The United States.....	39
8. Rights, Limits, and Education: What can we do as citizens?.....	60
9. Appendix.....	66

The Surveillance State:

A Glance at the Structure, Constitutional and Societal Impacts, and Solutions

Introduction

While America may not be a surveillance state quite yet, the dangers of becoming one are far too great for citizens to simply ignore them, especially with the warning signs that have become so visible since September 11th, 2001. With the Constitution in danger of losing the values our great founders embedded within it over 200 years ago, it is time that we look towards the surveillance state as not just a far off possibility, but a reality that is already a part of our every move. The questions one must ask are: What is the structure of the surveillance state and what technologies hold together these structures? When does our right to privacy trump the government's need for security? What judicial and historical precedents are there regarding privacy and its violations? How does this affect us on an international level? What are the implications of the surveillance state not just 50 years from now, but even 5 years from now? And most importantly, what can we do today in order to ensure our right to privacy and the protection of our Constitution? This may not provide all of the answers, but it is important to remember that the questions you find here are questions that we all must ask. While this paper does not ask you to believe or assume that America is already a full-fledged surveillance state, the aim is to show that with our civil liberties in danger, the only people who can truly step up are the citizens themselves.

Structure of the Surveillance State: The Evolutionary Process of Security

The power of the government within the United States has always been a question of constitutionality. Within the context of surveillance by the state on its citizens, the Founding Fathers addressed potential abuses as evident by the Fourth Amendment,

“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.”¹

The Fourth Amendment to the Constitution addresses the basic concept of protecting personal liberties and individual freedoms. Yet the Constitution was not constructed with surveillance practices at its forefront. In the modern world of the 20th and 21st Centuries, surveillance and its applicability to protecting the nation state evolved exponentially. The possibility has arisen where a security state could be possible under the current structure of the United States government. How could this have happened? Who are the chief principle perpetrators behind this shocking possibility? These questions and others regarding the perception of a “surveillance state” are answered through the analysis of legislation, executive orders, commissions, and the results of traumatic events in the United States, such as the terrorist attacks on September 11, 2001.

Conception and Development of the Intelligence Community: Then and Now

Regarding the history of domestic surveillance and intelligence gathering in the United States, the seminal date to begin an analysis of constitutionality and legality is July 26, 1947 with the passing of the National Security Act (PL 80-253)². This date is the beginning of the modern era of national security and intelligence in the United States as it established the Department of Defense and fundamentally changed the structure of how national security is executed. Also included in this act was the establishment of the Central Intelligence Agency (CIA) with the original intent to serve “as the nation’s primary organization for gathering, processing, analyzing, and disseminating foreign intelligence to policy makers.”³ Its role would eventually

¹ LII/ Legal Information Institute, “United States Constitution: Amendment IV,” Cornell University Law School, March 2009, <http://www.law.cornell.edu/constitution/constitution.billofrights.html>

² Proposals for Intelligence Reorganization and Dissolution

³ J. Ransom Clark, *Intelligence and National Security: A Reference Handbook*, 2007, 16.

expand with the escalating tensions between the USSR and the United States in the Cold War. Before moving on to the legislation and commissions that actively shaped security policy, there is one more important date that is important for the question of the surveillance state, 1952. In 1952, the National Security Agency was established to “[exploit] foreign signals intelligence and [make] the nation’s communications secure,”⁴ and is currently the largest agency in the IC. While other organizations such as the National Reconnaissance Office (NRO) and Defense Intelligence Agency (DIA) were also created in the Cold War, the CIA, NSA, and FBI are the agencies that most directly participate in domestic surveillance⁵.

The U.S. Intelligence Community is defined by the Fiscal Year 1996 Intelligence Authorization Act (P.L. 104-93) and includes the following agencies:

- Central Intelligence Agency
- Department of Defense
- Defense Intelligence Agency
- National Security Agency
- National Reconnaissance Office
- Departments of the Army, Navy, Air Force
- Department of State
- Department of the Treasury
- Department of Energy
- Federal Bureau of Investigation
- Drug Enforcement Administration

⁴ Ibid, 16.

⁵ Ibid. 17.

Central Imagery Office (currently the NGA)⁶

By 2007, two more agencies had joined the Intelligence Community (IC). The Department of Homeland Security was established in 2002 and incorporated the Coast Guard's division of Intelligence into the IC as well as its own office of Intelligence and Analysis. These two new agencies, when combined with the recently established Office of the Director of National Intelligence (2004), complete the 17 components of the current IC.⁷

As important as the present structure of the IC is for understanding the current status of the surveillance state, how the bureaucracies were formed over decades of investigations and world events is vital to comprehending the degree of the personal liberties in the United States. Their involvement in national security is the reason why they have been the constant targets for Congressional investigations since their conception

Commissions and Investigations: Congressional Influences on Structure

After the National Security Act of 1947, the roles and responsibilities of the agencies created under its auspices were constantly changed in response to particular situations. For example, the First Hoover Commission in 1949 established that the "CIA must be the central organization of the national intelligence system."⁸ There is a noticeable trend in commissions spearheaded by Congress at two points in time in the development of the IC. First, after its initial establishment in the late 1940's and into the 1950's, there were investigations and reports that attempted to cover and gaps left in the creation of the IC. The second era, and the most important for the impact that the IC has on civil liberties, is that of 1974-1981, "The Era of Public Investigations."⁹ During this time period, many reforms were imposed upon the IC by Congress and fundamentally changed the structure of the system. In particular, there was one

⁶ Proposals for Intelligence Reorganization and Dissolution 1949-1996, Congressional Research Services, 1996

⁷ J. Ransom Clark, 2007, pg. 21-22

⁸ Proposals...Congressional Research Services, 1996, pg. 6

⁹ Ibid, pg. 17

committee that brought to light the problems of the system and proposed the methods by which to correct them, the Church Committee.

The Church Committee (The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities) published reports between 1975 and 1976 regarding the abuses of the intelligence agencies were published over seven volumes of public hearings and exhibits, six books of writings by the committee on particular topics addressed, and one interim report on foreign assassination attempts by the CIA.¹⁰¹¹ Of these extensive reports, there is a specific volume dedicated to Fourth Amendment Rights and the National Security Agency due to Project MINARET (a project designed to spy domestically on peace groups and African American rights groups).¹² In this portion of the investigations, the Committee directly questioned whether or not citizens had lost their right under the Fourth Amendment by having the NSA listen to conversations or communications. Also, the secretive nature of the NSA that had been established in 1952 under the Department of Defense, yet still had no definitive charter clarifying its roles or responsibilities (an issue later addressed in the Pike Committee of 1976), was pursued because of its growth to thousands of analysts in the 1970's.¹³ While the NSA and CIA were addressed specifically, the Church Committee addressed many abuses by agencies conducted over the course of the post-World War II and Cold War era.

Why the Church Committee findings were so crucial to the development of the IC can be found in four particular results. First, the House and Senate established permanent Select Committees on Intelligence to increase their oversight of the agencies involved. They believed that serious violations had occurred and that the potential for domestic spying and political blackmail had grown too high.¹⁴ Second, they proposed a restructuring of the IC to where the

¹⁰ "Church Committee Reports," The Assassination and Archives Research Center (AARC), 5 April 2009 http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm

¹¹ History Matters, "Church Committee," 5 April 2009, http://www.history-matters.com/archive/contents/contents_church.htm

¹² "The National Security Agency and Fourth Amendment Rights," AARC, 5 April 2009, http://www.aarclibrary.org/publib/contents/church/contents_church_reports_vol5.htm

¹³ Ibid, 5 April 2009.

¹⁴ "Church Committee," Espionage Information, 5 April 2009, <http://www.espionageinfo.com/Ch-Co/Church-Committee.html>

DCI (Director of Central Intelligence) would no longer be directly supervising the CIA. This marks a shift from prior commissions and investigations that established the CIA as the center for intelligence of the nation. The new alignment would place a deputy under the direct control of the CIA and would allow the DCI to become a managerial figure for the entire IC. Thirdly, the Church Committees findings eventually led to the enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978.¹⁵ This act “governs wiretapping agents of a foreign power inside the United States for the purpose of gathering foreign intelligence.”¹⁶ The important clarification that the FISA requires judicial review to obtain authorization of domestic surveillance generally hinders the role of the CIA in domestic matters. Finally, the “wall” in the intelligence community was created. As a result of the reforms and recommendations included in the Church Committee’s final report, the IC became cognizant of the potentiality of its abuses. This “wall” would become absolutely essential in the period leading up to and following the terrorist attacks on 9/11/01, as the IC blamed the Church Committees impositions as the reason why they were unable to prevent an attack.¹⁷ Hence, to prevent more attacks, the “wall” was dissolved with the enactment of the USA PATRIOT Act.

To comprehend the current structure of the IC, it is crucial that one views the IC as a slow development influenced by Congressional oversight. While there were points in time where the intelligence community has overstepped its authority in the protection of the country, there has consistently been an attempt by Congress to moderate their actions. Yet there are aspects of the IC that are still under the dark shroud of classified. Primarily, the intelligence budget, governed under the Intelligence Authorization Act, has been classified for the past ten years in the interest of national security. This is also an important topic to discuss, because the growth of money spent on intelligence has grown much like the size of the agencies, larger and larger over time.

¹⁵ “Foreign Intelligence Surveillance Act,” Federation of American Scientists, 5 April 2009, <http://www.fas.org/irp/agency/doj/fisa/>

¹⁶ Kate Martin, “Domestic Intelligence and Civil Liberties,” 2004

¹⁷ Kate Martin, “Domestic Intelligence and Civil Liberties,” SAIS Review, Vol. XXIV no. 1, Winter-Spring 2004

The Intelligence Authorization Act: Oversight and Growth

The budget for the IC is essential to understand the growth of the IC. Commissions and investigations have even questioned whether or not an intelligence capability, or separate agencies, was even needed after WWII.¹⁸ This possibility, however, is not likely considering the graph on intelligence spending from 1980-1996 (Figure 1).¹⁹ One instantly notices the degree to which intelligence spending has outpaced that of defense spending. Granted, this graphic emphasizes percentage change as opposed to actual dollar change. The Defense Budget surpasses that of the Intelligence Budget, \$543 Billion to not even \$50 Billion.²⁰ The reason why intelligence budgets are important because they show not only where the government is allocating its precious funds, but to what extent these funds are monitored. A brief summary of how the budget is created and the money is appropriated is needed before understanding the implications of the now classified intelligence budget.

Similar to the Defense Authorization Act that must be approved by Congress annually, the IC receives the Intelligence Authorization Act. Currently, there are three main parts to the Intelligence Budget and are as follows:

- National Foreign Intelligence Program (NFIP)- This section of the budget currently funds all foreign activities such as intelligence and counterintelligence while focusing on “national,” not departmental, needs²¹
- Joint Military Intelligence Program (JMIP)- This section is controlled by the Department of Defense and is used to address multiple service needs²²
- Tactical Intelligence and Related Agencies (TIARA)- This section is a “pooled” fund that services use to meet their own intelligence needs.²³

¹⁸ Proposals for Intelligence Reorganization and Dissolution 1949-1996, Congressional Research Services, 1996

¹⁹ “Tracing the Size of the Annual Intelligence Budget,” FAS, 1996, 5 April 2009, <http://www.fas.org/irp/budget/index.html>

²⁰ “FY 2009 Budget Request,” Office of the Secretary of Defense, 5 April 2009, http://www.defenselink.mil/comptroller/defbudget/fy2009/2009_Budget_Rollout_Release.pdf

²¹ “The U.S. Intelligence Budget: A Basic Overview,” CRS Report for Congress, 5 April 2009, <http://www.fas.org/irp/crs/RS21945.pdf>

²² Ibid, 2004

The NFIP typically funds agencies outside of the DoD such as the CIA, while JMIP and TIARA are derived from the DoD. The NSA, however, receives funds from both the JMIP and the NFIP due to its ability to apply cryptology to many different IC consumers. In 1996, the Commission on the Roles and Capabilities of the U.S. Intelligence Community partially disclosed the budget break down by stating that “about two thirds of the...budget at the time was for the NFIP and almost all of the NFIP budget was for the CIA and DoD, with three quarters [of it] went to the DoD.”²⁴ This summary allowed analysts and journalists to begin estimating the amount of funds allocated to the different portions of the budget.

Guesstimation in the 21st Century: Current Estimates and Distribution of Funds

Unfortunately, the budget for the IC has been classified except for FY 1997 and FY 1998, where DCI George Tenet released that the total budget was \$26.6 billion and \$26.7 billion, respectively.²⁵ While this does protect foreign powers and terrorists from discerning as to where the money is being spent, it also restricts the public from interpreting where there money is being sent, and if it is being used illegally. The classified budget, however, was made less mysterious when Section 601 of the “Implementing Recommendations of the 9/11 Commission Act of 2007” (Public Law 110-53) required the Director of National Intelligence (DNI) to publicly disclose the total budget.²⁶ After this requirement came into effect, the next budget for FY 2007 revealed that the budget was approximately to \$43.5 billion. Many factors contributed to this startling jump in budget, but the primary reason would be the attacks on 9/11 that brought the IC to the forefront in terms of responsibility. Following the suggestions made by the 9/11 Commission for correcting errors in the system and elevating the Global War on Terror, intelligence budgets will cease to be irrelevant anywhere in the near future. Yet the detailed

²³ Ibid, 2004

²⁴ Ibid, 2004

²⁵ Ibid, 2004

²⁶ “Intelligence Budget,” GlobalSecurity.org, 5 April 2009, <http://www.globalsecurity.org/intell/library/budget/index.html>

budget is still classified and until it is declassified, the IC can operate beyond constitutional measures if they deem so necessary.

Figure 3 in the Appendix is a “Guesstimate” from GlobalSecurity.Org on the FY 2009 Intelligence based on the publicly disclosed figure of the \$66.5 billion total.²⁷ One of the most secret agencies, the NSA, receives almost 25% of the budget (\$15 billion), yet nobody truly knows how many people it employs or even what programs it uses within the domestic realms of the United States. The NRO also receives a similar amount under the NFIP, yet this could be due to the fact that its primary method of collection involves sophisticated technology such as satellites, which are almost prohibitively expensive. A final note on the FY 2009 Intelligence Budget is the almost 50% increase from the FY 2007 aggregate. This is an incredible amount of money that is for all intensive purposes, sunk into a black hole where only a handful of individuals know its final destination. There are representative measures in place, however, as the Senate Select Committee on Intelligence, and its House counterpart, bring a sliver of democracy to the intelligence budget appropriations process.

September 11, 2001: The Date that Changed Surveillance in the United States

Prior to the attacks on 9/11, the IC was operating as usual, with the primary agency for intelligence being the CIA. There are three agencies within the US government that pertain to domestic intelligence and 9/11: the CIA, FBI and NSA. These three are chosen due to their role in both foreign and domestic surveillance, as well as their cross IC customer base. Defense agencies involved in intelligence focus on operations and military intelligence, not intelligence within US borders. The following are the roles and responsibilities of the focal intelligence agencies before 9/11:

- CIA- The largest producer of all source national security intelligence to senior U.S. policy makers. Such intelligence includes HUMINT (intelligence pertaining to interactions between agents and contacts). Note, the CIA does not engage in the creation

²⁷ Ibid, 2008

of foreign policy and under the National Security Act of 1947, was prohibited from any “police subpoena, law-enforcement powers, or internal security functions.”²⁸²⁹

- FBI- As a part of the Department of Justice, the FBI is a responsive agency that combines domestic intelligence activities with criminal law enforcement, indicating that it has responsibilities for counterintelligence and counter-terrorism within the borders of the United States.³⁰³¹ Many of its authorities on intelligence were governed under FISA and Guidelines established by Attorney General Levi in 1976, and then modified under the Church Committee.
- NSA- The U.S.’s cryptology organization that is charged with the protection of US information systems and electronic infrastructure in addition to collecting, analyzing, and distributing foreign SIGINT (intelligence derived from electronic signals i.e. radio and telephone communications).³² It is an information assurance entity protecting US communications within and without the United States.

An important aspect to consider regarding these roles is that they are constantly changing as the threats of external states and actors fluctuate. Congressional investigations and hearings have drastically changed these responsibilities since the creation of the CIA under the National Security Act of 1947 to the time period prior to 9/11/01. The question remains, how did 9/11 occur? When the three terrorist, hijacked planes crashed on September 11, 2001, killing more than 3,000 individuals, answers were few and far between.

According to Attorney General Ashcroft, the attacks on the North and South towers of the World Trade Center occurred due to “the wall” described previously in the document.³³ The

²⁸ “Overview of the United States Intelligence Community by the 111th Congress,” Office of the Director of National Intelligence, 2009, pg 7

²⁹ Kate Martin, “Domestic Intelligence and Civil Liberties,” SAIS Review, Vol. XXIV no. 1, Winter-Spring 2004

³⁰ “Overview...,” ODNI, pg. 11, 2009

³¹ Ibid, pg 10, 2004

³² “Overview...,” ODNI, pg. 15, 2009

³³ “Flashback: Ashcroft Blamed Clinton Administration for “The Wall” between FBI and CIA,” September 11, 2001: United States and the World, 12 April 2009, 4 March 2009.

CIA and FBI were not communicating effectively and standard operating procedures prevented certain intelligence from being passed to the appropriate authorities. To quote Ashcroft, “government erected this wall...government buttressed this wall. And before 9/11, government was blinded by this wall.”³⁴ The CIA and FBI both knew of several terrorists, meetings between these terrorists, and of suspicious activities within the United States, yet “the wall” prevented sharing of information between the two in order to coordinate potential arrests on conspiracy for terrorism.³⁵ At this point in time, the NSA was not heavily concerned with terrorist attacks or non-state actors, but was focused on preventing a “virtual Pearl Harbor,” or an attack on the United States’ infrastructure via computer and digital access points.³⁶ As one can see, between the lack of coordination amongst the agencies and their focus on other problems, a possible result of no significant loss of life from foreign terrorist attacks prior to 9/11, the IC was inadequately prepared for 9/11.

The USA PATRIOT Act: Constitutional Lightning in a Bottle

The series of events that led to H.R. 1362, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act; the Act) were overwhelmingly rapid, and some may argue, reckless with little regard for civil liberties. Consider the timeline of events following 9/11:^{37,38}

- September 14, 2001- Congress grants extensive executive authority to President Bush to “use appropriate force” against those that planned and executed the attacks, and any nations that may harbor them
- October 2, 2001- The initial form of the USA PATRIOT Act is introduced to congress

³⁴ Ibid

³⁵ “Complete 911 Timeline: Key Warnings,” Historycommons.org, 12 April 2009, 17 Oct. 2002, www.historycommons.org

³⁶ Shane Harris, “NSA Sought Data before 9/11/01,” National Journal, 12 April 2009, 2 Nov. 07

³⁷ “Flashpoints USA. America at War. In Focus. Post 9/11 Timeline- PBS,” Bryant Gumbel and Gwen Ifill, 12 April 2009, 29 June 2004.

³⁸ “H.R. 3162,” THOMAS (The Library of Congress), 12 April 2009, 24 Oct. 2001.

- October 24, 2001- The final version of the USA PATRIOT Act is passed by the House

Within two months of the terrorist attacks, new legislation had been passed that addressed perceived intelligence failures that led to the attacks, but the consequences of the new legislation could also lead to civil liberty violations if used improperly.

There were several perceived barriers that led to the IC's inability to prevent the attacks on 9/11, but only several were addressed in the USA PATRIOT Act. Of these, arguably the most important was the change to the FISA's application with regard to intelligence gathering capabilities. Prior to 9/11, the primary purpose of the FISA was to protect the rights of individuals within the US by requiring FISA Court approval of wiretapping activities on foreign powers. The Bush Administration, however, requested that this provision be repealed and that the FISA be applied to anybody suspected of criminal activities.³⁹ Instead of addressing bureaucratic idiosyncrasies that probably created "the wall," the Congress acceded to the Administration's request and granted extensive authority to intelligence agencies to gather intelligence on persons within the US. Due to the fact that FISA already needed a lower burden of proof for approval of authorized intelligence, the application to a broader proportion of the population, foreign and domestic, indicated an increased role of different agencies in the IC. Specifically, the CIA gained more responsibilities in the domestic realm of intelligence. The provision that causes the most ire for civil liberties group is that of the requirement of the Attorney General, and the Justice Department, to relinquish all information regarding foreign intelligence, contacts with foreign governments or organizations, with essentially no safeguard for the information may be distributed. Further, the Attorney General further revised FBI criminal investigations in May 2002 to permit FBI agents to collect information regardless of whether or not a crime or planning for a future crime may have occurred.⁴⁰ After 9/11, many provisions in the USA PATRIOT Act were addressed at improving the effectiveness of the IC while allowing agencies broader range of movement in their surveillance actions.

Despite the limitations imposed by Congress under legislation, and their apparent repeal in the USA PATRIOT Act, the IC did not continue to garner power in the post-9/11 atmosphere.

³⁹ Martin, 2004, pg 14.

⁴⁰ Ibid, pg. 15

While debating the USA PATRIOT Act, members of Congress believed that the extensive powers they had granted in the Act may need to be reviewed at a later point in time to deem their legality and constitutionality. These provisions, termed “sunset” provisions, expired on December 31, 2005.⁴¹ Those provisions believed to be the most controversial by many civil liberty groups, and those that grant the most authority to agencies within the IC, were reviewed in 2005 prior to the “sunsets” applying to the laws. Cases that were being processed prior to, or criminal actions committed before, the sunset date were still to be treated under the old sunset laws in the USA PATRIOT Act.⁴² Intense debate followed these sunset provisions, as several senators considered the changes those provisions granted permitted violations of rights granted under the Constitution. Most significantly, the provisions under Title II and Title III of the USA PATRIOT Act relating to foreign intelligence gathering as well as surveillance authorities were strongly debated. Under strong pressure from President Bush, the House passed the renewal for the Act, including its provisions, on July 22, 2005, even though the debate lasted until late December.⁴³

Big Brother’s Technologic Arsenal: Unveiling the Private Lives of the Public

Since the catastrophic attacks on September 11, 2001, various politicians such as Chris Van Hollen, Democratic member of the United States House of Representatives, representing Maryland’s 8th congressional district espouse the important need for mass surveillance stating,

⁴¹ “USA PATRIOT Act Sunset,” Electronic Privacy Information Center, 14 April 2009, 15 Nov. 2008, www.epic.org/privacy/terrorism/patriotact/sunset.html

⁴² Ibid, 2005

⁴³ Ted Barrett, “House Approves Renewal of Patriot Act,” CNN.com/politics, 14 April 2009, 22 July 2005 www.cnn.com

“As we have all said, we understand that electronic surveillance is a vital tool in the war on terror. We all want to know when Osama bin Laden is calling: when he is calling, who he is calling, and what he is saying”.⁴⁴ According to a November Newsweek article in 2007 there are approximately 30 million surveillance cameras located throughout the United States while the average American is caught on film more than 200 times a day.⁴⁵ With Americans seeing cameras on the streets, at the ATM, at convenient stores, and even in public restrooms they have grown accustomed to various forms of surveillance that pervades their lives. This “Big Brother” notion provides implications dealing with the ultimately controversial issue of eroding one’s privacy in a democratic society. A few technologies that constitute mass surveillance are electronic eavesdropping devices, traffic cameras, biometrics, radio-frequency identification cards, and satellites, all of which persistently monitor the behaviors and actions of the public, intruding one’s privacy.

Eavesdropping Devices: Who’s On the Other line?

Wiretapping, one of the most notable and effective forms of surveillance of the law enforcement is defined as “Eavesdropping on private conversations by connecting listening equipment to a telephone line, often by covert means”.⁴⁶ In order for such action to be legal, eavesdropping must be authorized by a search warrant or court order, although 2007 legislation and the Protect America Act allow the President of the United States to conduct wiretapping without warrants for intelligence purposes. Before Alexander Graham Bell’s invention of the telephone in 1876, wiretapping was initially used on telegraph communication. Since then, wiretapping has had a long history in which it has been used on telephones, dating back as far as the early 1920s with its involvement in the Warren G. Harding administration and the Teapot

⁴⁴ "View Appearance | C-SPAN Congressional Chronicle, Created by Cable. Offered as a Public Service." C-SPAN Video Library | Created by Cable. Offered as a Public Service, 28 Sept. 2006. 12 Mar. 2009 <<http://www.c-spanarchives.org/congress/?q=node/77531&id=7508847>>.

⁴⁵ Bennett, Jessica. "Smile! You're on Hidden Camera | Print Article | Newsweek.com." Newsweek - National News, World News, Health, Technology, Entertainment and more... | Newsweek.com. 20 Nov. 2007. 14 Mar. 2009 <<http://www.newsweek.com/id/71506/output/print>>.

⁴⁶ "Wiretapping - legal definition." Nolo: Law Books, Legal Forms and Legal Software. 15 Mar. 2009. 15 Mar. 2009 <<http://www.nolo.com/definition.cfm/Term/6597D764-0245-42D1-A2850A504D49F01A/alpha/W/>>.

Dome Scandal. Wiretapping was used by Federal Bureau of Investigations Director William Burns on Montana Senator, Burton Wheeler because of the suspicion regarding his initiation of the investigation on the Harding Administration, especially the Attorney General, Harry Daugherty.⁴⁷ “Even a federal investigation led by Senator Frank Church from Idaho in the late 1970s revealed that past Presidents and the Federal Bureau of Investigations had wiretapped phone conversations with other political leaders, activists, politicians, civil rights leaders, and even their wives. This list of dignitaries whose phones had been wiretapped included people such as Martin Luther King Jr. and Eleanor Roosevelt”.⁴⁸ Federal Bureau of Investigations Director J. Edgar Hoover filed a request with Attorney General Robert Kennedy to tap King's and his associates' phones and to bug their homes and offices in July 1963, a month before the March on Washington”.⁴⁹ This request led to the civil right leader’s residency to be installed with “bugs” in a failing attempt to determine if communists were influencing the civil rights leader.

Wiretapping continues to remain a very powerful tool used by law enforcement today, and since its creation the technology’s applications and properties have remained the same. While telephone carries a circuit of energy, it also carries a circuit of information between the two telephones. The average wiretapping technology operates by simply connecting a listening device to the circuit carrying information between two telephones. The information is “fluctuated” sound wave patterns, which can be interpreted by wiretap technology.⁵⁰ In certain situations, the vibrations of sound waves can be extracted off of the glass windows surrounding a conversation. People often believe that experiencing static and obscure noise on their phone lines means that they are being listened to by a third party; however, most wiretaps emanate no perceptible sounds.⁵¹ The sound waves can be interpreted from techniques involving the tapping of outside lines, the planting of sound devices such as bugs in the room or in the phone wall socket or headset, and with the utilization of bugs, wireless communication can be monitored

⁴⁷ Sanchez, Julian. "Wiretapping's true danger - Los Angeles Times." Today's Headlines - Los Angeles Times. 16 Mar. 2008. 16 Mar. 2009 <<http://articles.latimes.com/2008/mar/16/opinion/op-sanchez16>>.

⁴⁸ *Ibid*.

⁴⁹ Christensen, Jen. "FBI tracked King's every move - CNN.com." CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News. 17 Mar. 2009. 17 Mar. 2009 <<http://www.cnn.com/2008/US/03/31/mlk.fbi.conspiracy/index.html>>.

⁵⁰ Harris, Tom. "HowStuffWorks "Basic Wiretapping Techniques"" Howstuffworks "People Channel" 30 Oct. 2008. 15 Mar. 2009 <<http://people.howstuffworks.com/wiretapping1.htm>>.

⁵¹ "Wiretapping and Eavesdropping on Telephone Conversations." Privacy Rights Clearinghouse--privacyrights.org. 01 Aug. 2007. 14 Mar. 2009 <<http://www.privacyrights.org/fs/fs9-wrtp.htm#w1>>.

from afar, often in a nearby parking lot or such close to the destination.⁵² The above techniques can be categorized as “passive” tapping or eavesdropping, in which one can observed the flow of information and messages without any actual alterations being done to the information. “Active” wiretapping, also known as tampering, has a negative connotation because it deals with the illegal activity of deliberately modifying the flow of information. Most of the time “active” wiretapping is used to insert falsified information or delete particular information. Active wiretappings most common use is to alter information on bank accounts and transaction information.⁵³ Between the two forms of wiretapping “passive” serves as the most common for its legal and frequent use by the Federal Bureau of Investigations.

In result to 9/11, telecommunications companies cooperating with the U.S. government have more apprehension regarding the interception of international phone calls and e-mail of American citizens suspected of espionage or terrorism rather than domestic crimes. Pre-9/11 wiretapping was used to track and alleviate certain domestic crimes such as gambling and drug use. For example, in 1968, wiretapping’s main use was to target gambling, the main source of income for organized crime, until the early 1980s when President Reagan authorized the national “War on Drugs”.⁵⁴ In 1968 64% of wiretapping cases corresponded to gambling while only 27% of the cases involved narcotic use, while in 1994 the surveillance cases involving narcotics was 77% and gambling only made up less than 8% of the cases.⁵⁵ The following statistics reflects how through time the U.S. government concentration is regarding domestic issues changes, and now the government’s primary interest for wiretap use is to safeguard our nation from terrorism.

As society has evolved over time, so have various eavesdropping technologies. Now wiretapping technologies can be used without occupying an agent full-time. This is possible through the use of recent speech recognition technology. This technique uses speech to text software that enables audio (sound waves) to be converted to actual words, which are then stored on a computer database. Once the data has been deciphered and transported to a computer

⁵² Harris, Tom. "HowStuffWorks "Basic Wiretapping Techniques"" Howstuffworks "People Channel" 30 Oct. 2008. 15 Mar. 2009 <<http://people.howstuffworks.com/wiretapping1.htm>>.

⁵³ "Data Security." The ACM Portal. 20 Mar. 2009. 20 Mar. 2009 <http://delivery.acm.org/10.1145/540000/539308/p1robling_denning.pdf?key1=539308&key2=2662757321&coll=portal&dl=ACM&CFID=15151515&CFTOKEN=6184618>.

⁵⁴ Diffie, Whitfield, and Susan Landau. Privacy on the Line The Politics of Wiretapping and Encryption, Updated and Expanded Edition. New York: The MIT P, 2007.

⁵⁵ *Ibid.*

database, words that present a threat can be detected, where then an agent is appointed to the phone call. Notable telecommunication corporations such as Teleserv Technologies, Nuance-Dragon Speaking Technologies and Verint (“The Global Leader In Actionable Intelligence Solutions”) produce automated call-analysis programs and speech to text software. In addition to the telecommunication companies and the Federal Bureau of Investigations, the Information Awareness Office at DARPA assist in creating surveillance and biometric technologies that would permit the people to have security. Dr. John Poindexter, Director, Information Awareness Office of DARPA, at DARPATech declared, “I really believe that we don't have to make a trade-off between security and privacy. I think technology gives us the ability to have both”.⁵⁶ Although, wiretapping technologies like the ones produced at DARPA may assist in safeguarding the citizenry from terrorism, the people must also realize the ramifications brought forth by these technologies as they may erode one’s privacy.

Traffic Cameras: Speed and License Plate Surveillance

Traffic camera surveillance is a major component of the intelligent transportation system, a system that acquires details related to the transport infrastructure and the automobiles it supports. The major aspect of traffic cameras is that they operate in real time, meaning they provide information to the authorities without any latency. Traffic cameras can be seen on traffic lights, alongside highways and roads, on bridges, and on expressways. Traffic cameras are used to monitor traffic conditions but also are utilized to catch drivers who break the law by speeding or perhaps running a red light. Governor Martin O'Malley of Maryland plans to ask lawmakers to approve the use of cameras to catch speeders for the state of Maryland.⁵⁷ Camera locations can be realized by the presence of a sign stating “Photo Enforced” under the speed limit sign. Although, a camera is present, acknowledgment of the technology’s presence must be given. These specific traffic cameras would operate by taking photographs of license plates when a car

⁵⁶ "John Poindexter Quotes." Famous Quotes and Quotations at BrainyQuote. 18 Mar. 2009. 18 Mar. 2009 <<http://www.brainyquote.com/quotes/quotes/j/johnpoinde234849.html>>.

⁵⁷ "Lawmakers to Consider Traffic Cams." WTTG FOX 5 myfoxdc Washington, DC Region News, Weather, Sports and Entertainment. 04 Mar. 2009. 10 Mar. 2009 <http://www.myfoxdc.com/dpp/news/maryland/Lawmakers_to_Consider_Traffic_Cams>.

would exceed the speed limit, capturing the date, time and speed of the violating vehicle. A violation ticket is then mailed to the speeder's residence days later. Similar cameras have actually been placed in 35 mph zones or less or school zones in order to increase safety. According to a *My Fox News* report, of the 26 camera sights in Montgomery County, Maryland for 7 months, 111,000 tickets were given for speeding violations, an approximately 4.5 million dollar revenue.⁵⁸ Traffic cameras located throughout the United States all serve the purpose to replace law enforcement officers, decrease speed violations, increase safety, and even create revenue for the state. Some people contest that the traffic camera companies are benefiting more than anyone and that cameras located at both traffic lights and maximum speed signs actually cause more rear end collisions.⁵⁹ Like all mass surveillance technologies however, people must consider whether or not the warrantless intrusion of privacy and decreased number of police officers on the road is worth some amount of compromisable safety.

The Biometric Database

A *New York Times* article titled *A Watchful State* discusses the aftermath of 9/11 on Wall Street by reflecting on the fact that all stocks plunged a week after the event except for some technological businesses such as the New Jersey company, Visionics, whose price per share more than tripled.⁶⁰ The company's primary concentration is in the field of biometrics, which is defined as the statistical study of biological phenomena.⁶¹ Companies in the field of biometrics study and create technology that analyzes humans using both behavioral and physiological traits. The term biometrics was not seriously mentioned or referred to until after the tragic attacks on 9-11 when President Bush noted in his State of The Union address on January 29, 2002 "we will...use technology to track the arrivals and departures of visitors in the

⁵⁸ "Lawmakers to Consider Traffic Cams." WTTG FOX 5 myfoxdc Washington, DC Region News, Weather, Sports and Entertainment. 04 Mar. 2009. 10 Mar. 2009

<http://www.myfoxdc.com/dpp/news/maryland/Lawmakers_to_Consider_Traffic_Cams>.

⁵⁹ *Ibid*.

⁶⁰ Rosen, Jeffrey. "A Watchful State - The New York Times." The New York Times - Breaking News, World News & Multimedia. 7 Oct. 2001. 12 Mar. 2009

<<http://query.nytimes.com/gst/fullpage.html?res=9505E4DE123DF934A35753C1A9679C8B63&scp=1&sq=biometric%20surveillance&st=cse>>.

⁶¹ *Ibid*.

United States.”⁶² It was not actually until May 14, 2002 that he said the word “biometrics” when he signed the Enhanced Border Security and Visa Entry Reform Act.⁶³

Biometric technology can observe both voice and behavior patterns of humans while also using methods to recognize unique physical traits such as their facial structures, retinal patterns, fingerprints, hair and eye color, and even body odor. Similar technologies were featured in the 1997 film *Gattaca*. In the “not-too-distant future” film, the biometric database was used in order to classify different genetic characteristics and selecting a desired genetic makeup and relating it to ones role in society.⁶⁴ Here, the question that must be answered is, “Is our society moving toward a Gattaca-age?” For now, there is no conclusive evidence showing our society is evolving to those extreme and science fiction conditions, although biometrics does exist across the United States. Technologies in the biometric market including smart cameras that can identify people based off of the biometric database. *The New York Times* article mentioned before also discusses the success of a facial recognition technology known as FaceIt. “FaceIt develops identification codes for individuals based on 80 unique aspects of their facial structures, like the width of the nose and the location of the temples”.⁶⁵ The technology can uses a database of faces including terrorists or wanted criminals when comparing a scanned image of a person’s face; however, one must consider the need for protection of the person's stored biometric information, so it is not misused and released to the public. Patricia Hewitt, former Secretary of State for Health and British politician stated in a 2003 interview, “I have very real concerns about the civil liberties implications of ultimately requiring every resident to submit themselves for compulsory fingerprinting or some other biometric test”.⁶⁶ The decision whether or not to use biometrics in mass surveillance continues to challenge both the U.K. and the U.S. because of the contentious issue to exchange privacy for security.

⁶² Jr., Woodward, John D. *Biometrics*. New York: McGraw-Hill/Osborne, 2003.

⁶³ *Ibid*.

⁶⁴ "Gattaca (1997) - Plot summary." *The Internet Movie Database (IMDb)*. 18 Mar. 2009. 18 Mar. 2009
<<http://www.imdb.com/title/tt0119177/plotsummary>>.

⁶⁵ Rosen, Jeffrey. "A Watchful State - The New York Times." *The New York Times - Breaking News, World News & Multimedia*. 7 Oct. 2001. 12 Mar. 2009
<<http://query.nytimes.com/gst/fullpage.html?res=9505E4DE123DF934A35753C1A9679C8B63&scp=1&sq=biometric%20surveillance&st=cse>>.

⁶⁶ Ashley, Jackie. "Jackie Ashley meets Patricia Hewitt | Politics | The Guardian." *Latest news, sport, business, comment and reviews from the Guardian | guardian.co.uk*. 29 Sept. 2003. 18 Mar. 2009
<<http://www.guardian.co.uk/politics/2003/sep/29/uk.women>>.

Biometric information may even be applied to individual use rather than being stored on one mega-database. The national ID card would store biometric information and would enable people to have access to everything from airplanes to national parks and some courthouses.⁶⁷ In the *New York Times* article, titled, *Why Fear National ID Cards?*, by Alan M. Dershowitz, a law professor at Harvard, claims the national ID card could help avoid toll booths, by the device sending a radio signal that records their passage. The driver would then be billed later while the toll-takers know more about you as you entered and left the tollbooth.⁶⁸ Essentially, the card would provide convenience, efficiency, and time for the American citizen.

The Department of Transportation has in the past pushed for an advanced driver's license, which will contain biometric information similar to the national ID cards. The advanced driver's license is very useful in a situation where a police officer would pull an out-of-state driver over for speeding or by violating the law the officer can refer to the card and see that the driver has a valid driver's license rather than a look-alike.⁶⁹ Ron Paul, Republican House Representative from Texas's 14th district stated when campaigning for President, "I am absolutely opposed to a national ID card. This is a total contradiction of what a free society is all about. The purpose of government is to protect the secrecy and the privacy of all individuals, not the secrecy of the government. We don't need a national ID card."⁷⁰ Paul, among other politicians, claims that legislation promoting the ID card such as the Real ID Act would only give authority to the Department of Homeland Security to design such forms of identification, further stripping individuals of biometric information that is considered to be private. The nation ID card would contain a vast amount of information regarding physiological traits safeguarding a person from crimes such as identity theft, but it could also invite more racial profiling throughout the country. The card would then serve as an even greater civil liberties problem by both

⁶⁷ McCullagh, Declan. "National ID cards on the way? - CNET News." *Technology News - CNET News*. 14 Feb. 2005. 17 Mar. 2009 <http://news.cnet.com/National-ID-cards-on-the-way/2100-1028_3-5573414.html>.

⁶⁸ Dershowitz, Alana M. "Why Fear National ID Cards? - The New York Times." *The New York Times - Breaking News, World News & Multimedia*. 13 Oct. 2001. 13 Mar. 2009 <<http://query.nytimes.com/gst/fullpage.html?res=9800E2D6123FF930A25753C1A9679C8B63&scp=1&sq=national%20id%20card&st=cse>>.

⁶⁹ Pellegrini, Frank. "The National ID Card That Isn't, Yet - TIME." *Breaking News, Analysis, Politics, Blogs, News Photos, Video, Tech Reviews - TIME.com*. 08 Jan. 2002. 16 Mar. 2009 <<http://www.time.com/time/nation/article/0,8599,191857,00.html>>.

⁷⁰ "Ron Paul Revolution." *Ron Paul for President 2008*. 20 Mar. 2009. 20 Mar. 2009 <<http://www.fight4truth.com/ronpaul.htm>>.

intruding on the privacy of individuals and magnifying the existing racial profiling issue. The national ID card remains to tear the political spectrum apart even more, as it remains a very contentious issue on both the campaign trail and on Senate votes. National ID cards are truly the exchange of privacy for time and convenience, similar to the (RFID).

The Mark: Radio-Frequency Identification (RFID)

Radio-Frequency Identification technology includes a reader which communicates with a tag (microchip), through the signals of radio waves.⁷¹ “The tag contains digital information in a microchip. There are also forms of RFID tags without a microchip that use material to reflect back a portion of the radio waves beamed at them”.⁷² (RFID) tags are currently used throughout the United States to help keep record of inventory and as of 2005, 50 people in the United States had them planted under their skin to transmit their medical conditions along with biometric data, in case of an emergency.⁷³ Similar technologies have been used in livestock and pets to trace them and to reflect the animal’s owner. Although the technology may seem useful, it is argued by many that it will lead to an increased power of the government over people and the civil liberties of humans may be at stake if one would be required to have such technology inserted under the skin.

In a 2006 *New York Times* article titled, *High Tech, Under the Skin*, an Ontario piercing and tattoo parlor is known to insert specific technologies under the skin. The long-grain rice size silicone microchip technology is inserted into the webbing between one’s thumb and forefinger by a needle.⁷⁴ The desired patient requested the (RFID) tag in order to log on to his computer, open doors and unlock his car all of which can be read by a scanner two to four inches away.⁷⁵ The Florida (RFID) producing company Verichip implanted 2,000 people worldwide, 60 people

⁷¹ "RFID Journal — Glossary of Terms - What is RFID, Definition, Radio Frequency Identification Systems." RFID Journal - RFID (Radio Frequency Identification) Technology News & Features. 18 Mar. 2009. 18 Mar. 2009 <<http://www.rfidjournal.com/article/glossary/3#125>>.

⁷² *Ibid.*

⁷³ "The State Of Surveillance." BusinessWeek - Business News, Stock Market & Financial Advice. 8 Aug. 2005. 11 Mar. 2009 <http://www.businessweek.com/magazine/content/05_32/b3946001_mz001.htm>.

⁷⁴ Bahney, Anna. "The New York Times Log In." The New York Times - Breaking News, World News & Multimedia. 2 Feb. 2006. 13 Mar. 2009

<<http://www.nytimes.com/2006/02/02/fashion/thursdaystyles/02tags.html?scp=9&sq=RFID%20human&st=cse>>.

⁷⁵ *Ibid.*

in United States of America, mostly for people to store medical information in case of an emergency.⁷⁶ As society evolves, the (RFID) chip will also enable people not only to store medical information but also biometric data, and possibly even “the history of their lives”.

“The U.S. State Department is now considering even to issue passports with radio frequency identification, or (RFID), chips embedded in them, and Virginia may become the first state to include (RFID) tags into all its driver's licenses.”⁷⁷ The (RFID) tag presents a science fiction yet frightening theme to the world if one perceives the technology as a symbol like some evangelicals as a sign of “The end times”. The Bible states in Revelation 13:16-17, “And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: and that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name”. The Bible further mentions that those who take this mark will serve under torment for all of eternity.⁷⁸ Even when the religious aspect is not taken into account, the constitutional applications still prevail when addressing the chips. Having the history of a person on record violated their right to privacy and to have information that the government is not privileged to hold. The (RFID) chip continues to be one of the most debatable amongst surveillance technologies as it provides both religious and constitutional implications.

The Eye in the Sky: Satellites and Sensor Technology

Since the first satellite launch of Sputnik by the Soviet Union on October 4, 1957, satellites have been placed into orbit by human endeavor in order to provide services including (GPS) navigation, mapping, weather, radio, telephone, television, military, and most importantly, surveillance. According to NASA's Goddard Flight Center, as of 1997 (40 years since the launch of Sputnik) there are about 3,000 useful satellites and 6,000 pieces of space junk orbiting Earth.⁷⁹ Satellites have become a form of mass surveillance the public has grown used to due to

⁷⁶ *Ibid.*

⁷⁷ McCullagh, Declan. "National ID cards on the way? - CNET News." Technology News - CNET News. 14 Feb. 2005. 17 Mar. 2009 <http://news.cnet.com/National-ID-cards-on-the-way/2100-1028_3-5573414.html>.

⁷⁸ *Ibid.*

⁷⁹ "NASA - Artificial Satellites." NASA - Home. 20 Mar. 2009. 20 Mar. 2009 <http://www.nasa.gov/worldbook/artificial_satellites_worldbook.html>.

their common use. The United States' military frequently uses satellites to monitor bases, aircraft carriers, military operations, facilities, and occurrences throughout the world. In the early to mid 1990s, satellite surveillance was used to image locations such as airdropped aid bundles in Bosnia, presidential palaces and scud bunkers in Iraq, patriot missile batters in Israel, and nuclear facilities in North Korea.⁸⁰ Satellites have even been used to produce infrared images, which show the amount of heat coming from Earth and the clouds, while also tracing the heat emitted from human beings. Certain infrared satellites are then able to track suspects on foot or traveling in vehicles. Over the past five decades satellites have developed a resolution farther than ever imagined. The third-generation satellite GeoEye-2 created by ITT Corporation is now the world highest resolution satellite. GeoEye-2, currently expected to launch in 2011 is capable of perceiving objects on the Earth's exterior as little as 0.25-meter (9.75 inch) in size.⁸¹ Similar satellites located at least 12,000 miles above the Earth are communication satellites that are part of the Global Positioning System. About 24 of the (GPS) satellites are currently operational at any time operate in relation to cellular telephones, vehicles, and navigators to help position people, always knowing where these people are located and where they are heading. "The GPS constellation is controlled by the United States (NOAA and NASA) for operations of the U.S. Department of Defense, but is free for anyone to use, with the exception of (GPS) navigational receivers commonly found for both the vehicle and cell phone".⁸² Some receivers that are used to monitor plate motions have an accuracy to map locations on Earth with millimeter accuracy, while the average receiver has an accuracy of up to 10-15 meters when using up to 12 (GPS) satellites.⁸³ The 24 satellites all at one time interact with one another along with ground-based stations and other (GPS) satellites in order to achieve the location mechanism.⁸⁴

Whether it is a human behind the wheel of a car or a geologist tracking plate tectonics, (GPS) has served as a very useful tool for the lost and the ones searching for knowledge; however, the law enforcement have also shown desire to use (GPS) on criminals. In a newspaper

⁸⁰ Richelson, Jeffrey. U.S. intelligence community. Boulder, Colo: Westview P, 1999.

⁸¹ Merten, Dave. "Macsimum News - GeoEye-2, the world highest resolution satellite in development." Macsimum News - For your digital life(style). 04 Jan. 2009. 15 Mar. 2009
<http://www.macsimumnews.com/index.php/archive/geoeye_2_the_world_highest_resolution_satellite_in_development/>.

⁸² AGI/, NAGT, Edward M. Tarbuck, and Richard M. Busch. Laboratory Manual in Physical Geology (8th Edition). Upper Saddle River: Prentice Hall, 2008.

⁸³ *Ibid.*

⁸⁴ *Ibid.*

article named *Putting Parolees on a Tighter Leash*, (GPS) satellites and remote tracking technology are used to track sex offenders and criminals in real time in order to constantly monitor their locations. In 2002, 1,200 offenders were tracked by remote tracking technology, with 27 states utilizing the device, and Florida having 600 offenders under surveillance.⁸⁵ Satellites have become a huge part of human lives. They may be great eyes in the sky but as useful as they may be, people must also understand that these concealed devices will always be peering down on humanity knowing one's every move, especially as the resolution of the satellites continues to advance.

Arcane Technologies for an Evolving Society

Various forms of surveillance, whether they are the satellite in the sky or the cameras on the road, continue to pervade the lives of the citizenry. The chief of police in Washington D.C. told a CBS reporter in 2002 that he potentially has access to an unlimited number of cameras.⁸⁶ This statement, like many others made by high-ranking officials have revealed evidence that America is slowly being succumbed to a "Big Brother" surveillance society. However, America does not stand alone in being bombarded constantly by mass surveillance; Great Britain has resembled police state behavior in their usage of technologies. In order to prevent terrorism from the Irish Republican Army, as of 2005, Great Britain had 4 million video cameras monitoring streets, parks, and government buildings.⁸⁷ In 2005, London alone was reported as having 500,000 cameras watching for signs of criminal actions.⁸⁸ High ranking government officials in the United States feels that as a nation fighting a war on terror we too should implement pervasive forms of surveillance technologies. In a 1994 interview, the 10th Director of the

⁸⁵ Lee, Jennifer. "Putting Parolees on a Tighter Leash - The New York Times." The New York Times - Breaking News, World News & Multimedia. 31 Jan. 2002. 15 Mar. 2009 <<http://query.nytimes.com/gst/fullpage.html?res=9501E2DA1E3AF932A05752C0A9649C8B63&sec=&spon=&sc=1&sq=satellite%20surveillance&st=cse>>.

⁸⁶ Crean, Ellen. "Close Watch - CBS News." CBS News - Breaking News Headlines: Business, Entertainment & World News. 21 Apr. 2002. 13 Mar. 2009 <<http://www.cbsnews.com/stories/2002/04/19/sunday/main506739.shtml>>.

⁸⁷ "The State Of Surveillance." BusinessWeek - Business News, Stock Market & Financial Advice. 8 Aug. 2005. 11 Mar. 2009 <http://www.businessweek.com/magazine/content/05_32/b3946001_mz001.htm>.

⁸⁸ *Ibid.*

Federal Bureau of Investigation, Louis Freeh, stated, "The American people must be willing to give up a degree of personal privacy in exchange for safety and security".⁸⁹ Though this alternative Freeh proposes might safeguard the citizenry from terrorism, it will not protect them from the present and future unwarranted invasion of one's privacy. With the constant bombardment of surveillance technologies on the public, privacy will continue to remain elusive in our modern society, especially until the general public is ready to accept their constitutional right to privacy and more importantly, the significance of it.

The Surveillance State and Its Constitutionality

Due to the advance of technology's capabilities to monitor people in various ways, the U.S. Government has become a nation treading on the fine lines of constitutionality. Being one of the most important American documents, great debates arise concerning whether the

⁸⁹ Markoff, John. "A Push for Surveillance Software - The New York Times." The New York Times - Breaking News, World News & Multimedia. 28 Feb. 1994. 16 Mar. 2009
<<http://query.nytimes.com/gst/fullpage.html?res=940DE5DD143AF93BA15751C0A962958260&sec=technology&spon=&pagewanted=all>>.

government has overstepped its boundaries or if the developments after 9/11 appear far-reaching but still within the scope of the Constitution and the Bill of Rights. The 4th Amendment, in particular, has played a crucial role in the limiting of the surveillance state, but the government has found several ways to bypass this standard in order to achieve its own personal goals. This section of the paper will serve as an evaluation of the original intent of privacy in the 4th Amendment, survey the standard presented by the Supreme Court with respect to privacy, investigate if the government is violating the right to privacy, evaluate how the presidency has developed beyond the intention of the Constitution, and review the National Security Administration's behavior under the same standard.

The Fourth Amendment: Using History to Understand its Purpose

To understand the intent of the Founders in writing the Fourth Amendment, it is important to review two English cases that served as guides for creating the American standard of privacy. A case decided in 1603, *Semayne's Case*, established the well-known maxim of "Every man's house is his castle" as a result of the ruling that declared the right of a man to defend against unlawful entry to his home even by the King's agents.⁹⁰ At the same time, this case also affirmed that if the King's agents have the appropriate authority to break and enter upon notice, thereby establishing a standard for the entry into a man's home.⁹¹ One further case that the U.S. Supreme Court called a "great judgment" is *Entick v. Carrington*. The English court ruled that the use of a general warrant (one which permitted officers to enter into a house and seize whatever documents they found- it was not specific for any crime) was a violation of a man's privacy.⁹² This decision was referenced in the US case of *Boyd v. United States* (1886) with Supreme Court explaining the importance of *Entick* and the underlying principle of privacy,

⁹⁰ "U.S. Constitution: Fourth Amendment." FindLaw. Mar. 2009. <<http://supreme.lp.findlaw.com/constitution/amendment04/01.html#1>>.

⁹¹ *Ibid*.

⁹² Hornberger, Jacob G. "The Bill of Rights: Searches and Seizures." Welcome to The Future of Freedom Foundation. Mar. 2009 <<http://www.fff.org/freedom/fd0410a.asp>>.

“...They (the principles from *Entick*) apply to all invasions on the part of the government and its employees of the sanctity of a man’s home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offense; it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden’s judgment.⁹³

So often in today’s society judgments like this are ignored and forgotten, which is why it is important we constantly review our history in order to understand what the Founders intended in their creation of the Constitution and Bill of Rights.

American colonists utilized these two British rulings on privacy as a basis for their own appeal against the far-reaching powers of the British government before the revolution. Even after American independence, the Founders still looked back to these standards as a foundation for creating their own protections of privacy. Thus, it is no surprise of how James Madison chose to word the amendment, mandating that specific warrants must be obtained on probably cause in order to lawfully enter into a man’s house for the purpose of searching.

The two clauses of the amendment have come to be points of contention throughout the life of the Supreme Court, with various justices taking different views on the clause relationship. Should the amendment be taken to read that the only reasonable search and seizures are those **pursuant** to warrants issued under the prescribed safeguards or if only searches with warrants must adhere to the second clause while there are reasonable searches within the first clause that do not need to follow the standard of the second clause.⁹⁴ This is a fundamental point of question with respect to the Fourth Amendment and one that the Supreme Court has dealt with since the creation of the Bill of Rights. Throughout the history of Fourth Amendment cases, the

⁹³ Ibid.

⁹⁴ "U.S. Constitution: Fourth Amendment." FindLaw. Mar. 2009. <<http://supreme.lp.findlaw.com/constitution/amendment04/01.html#1>>.

Supreme Court has wavered on the necessity of warrants in situations where a search could be deemed reasonable, thus blurring the interpretation of the amendment's purpose.⁹⁵

Precedent Established by Court Cases

Justice Harlan, in a dissenting opinion from *Katz v. United States*, established the standard used today by which to evaluate violations of privacy: the reasonable expectation standard. Harlan created a two part test that has the following standards to evaluate a potential violation of the Fourth Amendment; what a person consciously exposes to the public is not protected under the amendment but what a person attempts to make private (even in public) could be constitutionally protected- essentially if there is a reasonable expectation of freedom from governmental intrusion.⁹⁶ The test is subjective in that an individual determines what he deems to be private, but then there must be a counterbalancing act in which it is decided if society would agree this expectation of privacy is reasonable.⁹⁷ If both of these requirements are met, then a violation of an individual's right to privacy has occurred and the government is at fault. While the Supreme Court has utilized this standard since *Katz*, as the surveillance state grows and expands it is becoming increasingly unsuited to today's reality. At the time of *Katz* it was considered reasonable to expect your phone call conversations to be private, but today that standard may not necessarily be the same. With the PATRIOT Act and recent wiretapping schemes, many Americans would undoubtedly find that expecting a phone call to be private was unreasonable. Thus, the *Katz* standard may have reached the end of its applicability for the United States; only time will tell if a new standard needs to be created.

Thermal Sensors

⁹⁵ Ibid.

⁹⁶ Ibid.

⁹⁷ Schneier, Bruce. "It's Time to Drop the 'Expectation of Privacy' Test." *Wired News*. Mar. 2009
<http://www.wired.com/politics/security/commentary/securitymatters/2009/03/securitymatters_0326

The 2001 case of *Kyllo v. United States* dealt with the relation of the Fourth Amendment with thermal sensors. After traveling through the 9th Circuit, where it was first declared unconstitutional and then subsequently reversed, the case went to the Supreme Court. In a 5-4 decision, the court found that the thermal scanning of Kyllo's house was a search under the Fourth Amendment and thus required a warrant. The majority felt that thermal imaging of the house invaded a man's privacy because it was a reasonable expectation to not have such a check performed. While police are permitted to scan peoples' houses from an appropriate vantage point, the court felt that the usage of thermal imaging required a warrant in order to be legal.⁹⁸ Most importantly, this decision left no lasting standard by which to evaluate emerging technologies.

Global Positioning Systems

The Seventh Circuit Court of Appeals handled the global positioning system case of *Garcia v. United States*. The offense in question was whether the placement of a GPS on a vehicle (for monitoring) required an application for a search warrant. With respect to the qualities of the Fourth Amendment, the court found that there was neither a search nor a seizure in this case. Furthermore, police themselves could have easily done the surveillance performed by the GPS, making this a reasonable tracking of Garcia. Citing a Tenth Circuit case, the court established that the undercarriage of a car is on its exterior and thus there is no reasonable expectation for privacy on behalf of the driver. Moreover, the police put the GPS on the car while it was parked in a public area (as opposed to Garcia's driveway) and also did not open any part of the car. Thus, this decision established precedent that allowed for the use of GPS monitoring of cars as long as the items were placed on the cars in a public area and also on the

⁹⁸Colbridge, Thomas D. "Kyllo v. United States: Technology Versus Individual Privacy - Fourth Amendment case | FBI Law Enforcement Bulletin, The | Find Articles at BNET." [Find Articles at BNET | News Articles, Magazine Back Issues & Reference Articles on All Topics](http://findarticles.com/p/articles/mi_m2194/is_10_70/ai_80787342/pg_6/?tag=content;coll). Mar. 2009
<http://findarticles.com/p/articles/mi_m2194/is_10_70/ai_80787342/pg_6/?tag=content;coll>.

exterior of the car itself. This ruling represented a gain for the government who can now use items like GPS without a warrant as long as certain conditions are met.⁹⁹

Hidden, Outdoor, Motion Activated Video Cameras

US v. Vankesteren is a recent case that received a ruling from the Fourth Circuit on January 9, 2009. Steve Vankesteren appealed that the warrantless placement of a hidden, outdoor, motion activated video camera on his private land was a violation of the Fourth Amendment.¹⁰⁰ Vankesteren was charged with the killing of two protected birds (hawks), seen as a result of the placement of these cameras on his property. The Fourth Circuit cited a 1926 case in its affirmation of the district court decision, explaining that open fields provide an exception to the necessity of a warrant. However, all of the cases referenced by the Circuit Court (*Hester v. US*; *Oliver v. US*; *US v. Dunn*) did not deal with video camera surveillance but rather the action of law enforcement officers physically watching an area. The 4th Circuit compared the private open field of Vankesteren with hypothetical public places such as banks and parks, and therefore concluded, "Since Vankesteren had no legitimate expectation of privacy, the agents were free, as on public land, to use video surveillance".¹⁰¹ While the court utilized the standard of the reasonableness of expectation for privacy, they compared two forms of surveillance that operate in significantly different manners.

Firsthand surveillance by an officer is limited because he can only remain on watch for a certain amount of time without being detected by the landowner. Cameras, on the other hand, can be installed and run for extended periods of time without the landowner's knowledge in

⁹⁹ Batterton, Brian S. "Court order or search warrant requirements for GPS tracking on vehicles for on-going surveillance." [Police Training Courses & Law Enforcement Training](http://www.patc.com/enewsletter/legal-answers/4-oct08.shtml). Mar. 2009
<<http://www.patc.com/enewsletter/legal-answers/4-oct08.shtml>>.

¹⁰⁰ *United States v. Steve Vankesteren*. No. 08-4110. United States Court of Appeals for the Fourth Circuit. 8 Jan. 2009.

¹⁰¹ "4th Circuit Holds US Can Use Video Obtained From Warrantless Hidden Video Cameras Placed on Owner's Private Property, 1/8/2009." [Tech Law Journal Home Page](http://www.techlawjournal.com/topstories/2009/20090108.asp). Mar. 2009
<<http://www.techlawjournal.com/topstories/2009/20090108.asp>>.

addition to saving whatever images it captures.¹⁰² Although Vankesteren attempted to persuade the court to take a different method of analysis when cameras are used versus in-person surveillance, the Fourth Circuit denied any such differentiation should exist and upheld the district court decision.

Cell Phone Location

A recent case in which the Department of Justice was denied the ability to track cell phone locations real time was upheld by a federal court, following the original decision of a magistrate ruling a warrant was needed. It is necessary for the government to obtain a warrant in order to receive such information due to the existing statutes and legal precedents, hence their creation of a reasonable expectation of privacy with respect to a person's location determined by their cell phone. The Electronic Frontier Foundation filed a friend-of-the-court brief opposing the government, and cited the decision by the magistrate as the first of its kind and important to the privacy of Americans.¹⁰³

Violations of the Right to Privacy: FISA, the USA PATRIOT Act and the NSA

Foreign Intelligence Surveillance Act (FISA)

Although the Foreign Intelligence Surveillance Act (FISA) was first established after the Watergate scandal, amendments were signed into effect last year that caused significant outrage among many groups across the nation. FISA follows a different set of rules by which to obtain a warrant for the search of an individual's property, and in its history only five warrants have been denied by the FISA Court.¹⁰⁴ The US Government argues that since the purpose of FISA is not

¹⁰² Ibid.

¹⁰³ "New Court Decision Affirms that 4th Amendment Protects Location Information | Electronic Frontier Foundation." Electronic Frontier Foundation | Defending Freedom in the Digital World. Mar. 2009 <<http://www.eff.org/press/archives/2008/09/11>>.

¹⁰⁴ Weaver, William G., and Robert M. Pallitto. "The Fourth Amendment and the Foreign Intelligence Surveillance Act authored by Weaver, William. and Pallitto, Robert." All Academic Inc. (Abstract Management, Conference

for law enforcement, but rather for information gathering, it is justified in this ease of obtaining a warrant. These FISA warrants are “becoming more like general warrants or writs of assistance, the very things that the Fourth Amendment was meant to guard against.”¹⁰⁵ However, FISA is the method by which other governmental organizations are authorized to conduct searches; thus, this process is the standard the government must follow.

USA PATRIOT Act

After being enacted merely weeks after the 9/11 terrorist attacks, the USA Patriot Act has continually received heavy criticism for its violation of civil rights. Under the legislation, the government gained new powers that pose clear threats to the civil liberties of all Americans. According to California attorney John Russo, the following are several of the most threatening aspects of the act,

“1) Federal agents may conduct surveillance and searches against U.S. citizens without having to show they have "probable cause" to suspect criminal activity. The targeted person is not notified, nor given a chance to challenge the action. 2) Agents can conduct "sneak-and-peek" searches without prior notice in common domestic crime investigations. This provision prevents anyone from challenging a potentially wrongful search. Prior to the Patriot Act, courts have required law enforcement to "knock and announce" themselves before conducting searches. 3) The government now has broad access to any person's business or personal records, including library records; book-buying habits; medical, marital counseling or psychiatric files; business records; Web-surfing habits, credit reports and even a person's genetic makeup. 4) The government does not have to give notice, obtain a warrant or a subpoena, or show there is probable cause that a crime has been committed. Persons turning over personal data to the government (such as librarians, doctors, co-workers or neighbors) are prohibited, under threat

Management and Research Search Engine). Mar. 2009

<http://www.allacademic.com//meta/p_mla_apa_research_citation/0/6/2/0/6/pages62068/p62068-2.php>.

¹⁰⁵ Ibid.

of federal criminal prosecution, from telling anyone.”¹⁰⁶

These new powers violate every American’s right to privacy, as enumerated under the Fourth Amendment. The USA Patriot Act provides an opportunity for the government to bypass the accepted standard of warranted searches, as well as other surveillance values, in order to increase the ease by which to watch any individual they desire. In this way, the USA Patriot Act represents an enormous infringement upon American civil liberties and remains a threat in the life of every American- not only the ones who are suspects. It is a gross exaggeration of power on the part of the US Government, one that must be checked with the power and wisdom of the Constitution.

National Security Administration

The National Security Administration (NSA) came under scrutiny with respect to the 4th amendment shortly after the 9/11 terrorist attacks. As a ‘security measure’ following this tragedy, the NSA implemented a program that allows it to authorize wiretaps without a court order.¹⁰⁷

“It allows the NSA to target phone calls without a warrant when one of the callers is outside the United States and the intercept is done on U.S. soil. The program was retroactively authorized by a secret executive order in early October 2001. The program has been reviewed every 45-60 days, and had been renewed over thirty times by the middle of December 2005.”¹⁰⁸

¹⁰⁶ Russo, John A. "Barriers to the Constitutional Right to Privacy / Patriot Act -- Forgoing liberty for safety?" San Francisco Bay Area; News, Sports, Business, Entertainment, Classifieds: SFGate. Mar. 2009
<<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/01/29/EDGGQ4K29F1.DTL>>.

¹⁰⁷ "NSA eavesdropping program ruled unconstitutional - Aug 17, 2006." CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News. Mar. 2009
<<http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/index.html>>.

¹⁰⁸ "The NSA Wiretapping Program." The Center on Law and Security. Mar. 2009
<http://www.lawandsecurity.org/publications/ForTheRecord/NSA_jan_07.pdf>.

As a result of this program, many began to question the constitutionality of its creation and existence, which eventually led to a court decision on the matter.

In 2006, a case was brought in the U.S. District Court for the Eastern District of Michigan, on behalf of several plaintiffs including branches of the American Civil Liberties Union, the National Association of Criminal Defense Lawyers, the Washington and Detroit branches of the Council on American-Islamic Relations and Greenpeace.¹⁰⁹ The plaintiffs' came with the following claim against the National Security Administration,

“[They question the] legality of a secret program (hereinafter “TSP”) undisputedly inaugurated by the National Security Agency (hereinafter “NSA”) at least by 2002 and continuing today, which intercepts without benefit of warrant or other judicial approval, prior or subsequent, the international telephone and internet communications of numerous persons and organizations within this country.”¹¹⁰

Judge Anna Diggs Taylor heard the case and decided against the NSA, declaring its wiretapping procedures to be in violation of the Constitution, especially of the First and Fourth Amendments. Judge Taylor was quoted as saying, “...the program ‘violates the separation of powers doctrine, the Administrative Procedures Act, the First and Fourth amendments to the United States Constitution, the FISA and Title III.’ She also noted that ‘the president of the United States ... has undisputedly violated the Fourth in failing to procure judicial orders.’”¹¹¹ With this ruling established, it is likely that more questions about NSA’s program will be asked, thereby allowing people to realize the importance of the Constitutional question present as a result of NSA’s wiretapping scheme.

¹⁰⁹ "NSA eavesdropping program ruled unconstitutional - Aug 17, 2006." [CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News](http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/index.html). Mar. 2009
<<http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/index.html>>.

¹¹⁰ American Civil Liberties Union v. National Security Agency, et al. No. 06-CV-10204. United States District Court for the Eastern District of Michigan. 17 Aug. 2006.

¹¹¹ "NSA eavesdropping program ruled unconstitutional - Aug 17, 2006." [CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News](http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/index.html). Mar. 2009
<<http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/index.html>>.

Expansion of Presidential Power

After the tragedy of 9/11, the United States faced a new frontier never before explored: that of how to best protect American citizens without infringing upon their liberty. However, the manner in which the Bush administration handled this challenge resulted in an excessive expansion of governmental, specifically presidential, power. Instead of remaining within Constitutional powers, the administration chose to expand their reach as a result of “military necessity” and override the prohibitions existing within the Fourth Amendment. The October 23, 2001 memo recently released (beginning of March 2009) reveals that the Bush administration superseded any restrictions of the Constitution because of the Presidential power to override laws during a time of war with military power. The memos reveal this sudden expansion of Presidential power, through the "use of force ... [that] might include ... employing surveillance methods more powerful and sophisticated than those available to law enforcement agencies." and that domestic "military action might encompass ... intercepting electronic or wireless communications."¹¹² Moreover, the memo suggests that not only will the government watch suspicious individuals, but it will also watch innocent Americans.

Thus, the memo is demonstrative of the dramatic extension of Presidential war powers: the ability to allow, without a warrant, the watching of any American on American soil. The memos themselves show the intent of expanding governmental power by saying, “the current campaign against terrorism may require even broader exercises of federal power domestically”.¹¹³ This is a clear assertion that the power of the president could inevitably be expanded, perhaps even beyond what is Constitutional. While the expansion of Presidential power is warranted during a time of war in order to protect the United States, the augmentation witnessed after 9/11 overstepped the intent of this feature and subsequently unleashed a fury of unconstitutional actions against the American people. As Judge Taylor concluded in her opinion (mentioned previously),

¹¹²Opsahl, Kurt. "Bush Administration Claimed Fourth Amendment Did Not Apply to NSA Spying | Electronic Frontier Foundation." Electronic Frontier Foundation | Defending Freedom in the Digital World. Mar. 2009 <[http://www.eff.org/deeplinks/2009/03/bush-administration-asserted-fourth-amendment-did->](http://www.eff.org/deeplinks/2009/03/bush-administration-asserted-fourth-amendment-did-).

¹¹³ "Declassified Memos Reveal Vast Claims of Executive Power." American Constitution Society : ACS Blog : The American Constitution Society for Law and Policy (ACS). Mar. 2009 <<http://www.acsblog.org/separation-of-powers-declassified-memos-reveal-vast-claims-of-executive-power.html>>.

"It was never the intent of the framers to give the president such unfettered control, particularly where his actions blatantly disregard the parameters clearly enumerated in the Bill of Rights," she wrote. ". . . There are no hereditary Kings in America and no powers not created by the Constitution. So all 'inherent powers' must derive from that Constitution."¹¹⁴

Judge Taylor is right- the Constitution must be the foundation upon which all US Government decisions are made, and when deviations are made from this standard, the United States faces a time in which civil liberties and civil rights are threatened by the institution that is in place to protect them. Thus, to protect our selves and our country from the prospect of an overbearing surveillance state, the power of the Constitution must be reinstated as soon as possible.

South Africa and The United States: Are We Becoming a Police State?

The problem with increased surveillance extends beyond the inconvenience of long lines in the airport and the fear of an agent at the other end of a call; it is the first step toward the creation of an authoritative police state. The curbing of civil liberties can be a way to improve the security of a state, but it is always the consolidation of power within a minority group. If left unchecked, that power can fester, authorizing anyone associated with governmental power to abuse and control the citizenry. It is therefore the potential for abuse that must be emphasized in any discussion on the formation of police states. As Americans, we like to think of our system as

¹¹⁴ "Post details: NSA's broad wiretapping program declared unconstitutional." [FourthAmendment.com](http://fourthamendment.com). Mar. 2009 <http://fourthamendment.com/blog/index.php?blog=1&title=nsa_s_broad_wiretapping_program_declared&more=1&c=1&tb=1&pb=1>.

progressive and libertarian; perhaps counter intuitively, however, this faith in the personal protection of our laws seems to be the lifeblood upon which the government feeds for increasingly expanded and authoritarian legislation. While America remains a fundamentally successful representative democracy, the passage of laws such as the PATRIOT Act and the Military Commissions Act has already begun to increase the potentiality for eventual totalitarianism. It is the purpose of this brief to investigate, through an in-depth comparison with South Africa, what privacy violations have meant for other states and what they could mean for the future of America. The motivations, justifications, and manifestations of the most notable privacy violations will be discussed and placed within a uniquely American jurisprudential context to better analyze the lessons America can learn and address the fundamental question: are increased surveillance measures merely a short-lived response to a real threat, or is America at risk of becoming the next police state?

Why South Africa?

It is first important to explain the choice of South Africa in light of the other police states around the world, such as Stalinist Russia, Nazi Germany, modern Rwanda, and the modern United Kingdom¹¹⁵. Each of these states has been categorized as a police or surveillance state, and each offers unique points of comparison with recent patterns in American law; however, there are key reasons why each must also be omitted from the majority of this brief. First, because this brief is about the *potentiality* for the formation of a police state, it is important to avoid comparisons with Nazi Germany and Rwanda. These are both nations that followed governmental abuses to their final end—genocide—and thus comparisons with these aggressive states carry the implication of the inevitability of this result. We are dealing with a nation at the beginning of its journey toward police statehood; to compare it even with the early stages of German or Rwandan governmental expansion smacks of conspiracy and speculation. Stalinist Russia can be omitted because of the wide culture gap between the United States and Communist Russia; the comparison, to work, must stay within the western world. This is why South Africa is

¹¹⁵ Some studies have compared the United States to the State of Israel, which is western, democratic, and the target of terrorist attacks; however, Israel's compulsory military service nullifies its legitimacy as a point of comparison with the United States.

an exceptional point of comparison. First, run by a European-style Parliament with nominal democracy, South Africa embodied western ideology. Second, its journey toward police statehood was propagated by the fear of terrorism or insurrection, fears with which a post 9/11 America can identify. Third, South Africa took its transformation into a police state far, but it did not reach the level that it did in Nazi Germany. Finally, South African apartheid reached its height from the 1970s to the 1990s, just late enough to have access to similar surveillance technologies and just early enough for its full effects to be known. While the modern UK is a wonderful example of a similarly western, representative surveillance society created as such out of fear of terrorism, its true nature and effects cannot yet be known. Therefore, South Africa under Apartheid offers the most insight into the possible effects of continued emphasis on American security.

Effects of Apartheid and Emergency Legislation

South African Apartheid formally began in 1948 when the white Afrikaner population commenced their decades-long process of racial discrimination and oppression of the black African majority. Though “ordinary,” non-emergency law, the Afrikaners attempted to hold the majority at bay by stripping them of their property and citizenship; when this was not enough to quell rebellions, the South African state would enact emergency law with no external regulation, leading to the police-related deaths of 624 adults and 92 children in 1986 alone¹¹⁶. Similar “states of emergency,” often precipitated not by actual black violence but rather the Afrikaner fear of it, were declared by then State President P.W. Botha in 1985 and 1986 and then renewed each year until 1990¹¹⁷; therefore, the collective result of increased surveillance, discrimination, and executive expansion of power in South Africa was countless deaths and still more civil liberty violations, all committed in the name of national security.

What is of note in assessing the Apartheid State is that there *did* exist an in Apartheid South Africa an *enumerated right to privacy* that was consequently deemed secondary to the

¹¹⁶ LYA 75

¹¹⁷ *Ibid.* 9

security of the State.¹¹⁸ The fact that such a right existed within a written framework establishes South Africa as an historical example of a state that used a series of contemporary justifications to undermine its own constitutional framework and, therefore, proves its legitimacy as a basis of comparison with the United States' constitutional system.

The Approach

To fully understand South African Apartheid and how it relates to American privacy, we must take a four-pronged approach. First, we will compare the South African and American constitutional frameworks to determine whether there is a built-in tendency toward the evolution of a police state. Second, we will recount a brief history of surveillance and overview of security law in South Africa. Third, we will investigate individual laws and their philosophy to gain a better perspective of how their motivations and justifications can be compared to American society; and fourth, we will draw from the patterns uncovered to determine whether America is at risk of becoming a surveillance state in the vein of 1948-1994 South Africa.

A Comparative Analysis of Constitutional Frameworks in South Africa and the United States

The Constitutional framework of a state is a central concern in evaluating its inclination toward police statehood; it is therefore important to highlight the substantial differences between the British/South African Constitution and the American Constitution before investigating particular legislation. The differences relevant to security law include the composition of the branches of government, the checks in place, and the court system's competency for judicial review. In the United States, the composition of the three branches is clearly delineated within

¹¹⁸ FSSL ___

Articles I, II, and III of the Constitution. Concerning the legislature, members of both of the Houses are elected by popular vote¹¹⁹. The President is voted on by the people and elected by the Electoral College¹²⁰, and the Courts act as an “intermediary”¹²¹ between the legislature and the people through the process of Judicial Review¹²². This is the basis of checks and balances, of which James Madison wrote, “It is equally evident, that the members of each department should be as little dependent as possible on those of the others, for the emoluments annexed to their offices. Were the executive magistrate, or the judges, not independent of the legislature in this particular, their independence in every other would be merely nominal”¹²³. The judiciary, Madison writes, acts as an “auxiliary precaution” against the power of the legislature. The South African governmental framework, however, is quite different. There were three different Constitutions active throughout the years of Apartheid, but it is the final one that is of particular interest. The Constitution of 1983 was seen as a step toward the liberalization of South Africa. Whereas the previous Constitutions had a single Parliament composed of all-white members, the Constitution of 1983 established a tricameral parliament with one house, the House of Assembly, for whites, one, the House of Representatives, for coloreds¹²⁴, and one, the House of Delegates, for Indians¹²⁵; however, if the State President deemed anything a “general affair,” a process that was unregulated and up to his personal discretion, it would pass through all three houses. In this instance, it was the House of Assembly, through the President’s Council, that controlled whether or not it became law. This was a frequently abused statute in which both the House of Delegates and the House of Representatives voted down a law that would affect their own community and the House of Assembly would pass it into law¹²⁶. The whites also had an automatic majority in electing the State President, in whom near absolute powers were also invested. While South

¹¹⁹ Art. I Sec 2 & Art. I Sec 3, as amended by 17th Amendment

¹²⁰ Art. I Sec 1

¹²¹ Alexander Hamilton, Federalist No. 78

¹²² Marbury vs. Madison

¹²³ James Madison, Federalist No. 51

¹²⁴ “Coloureds” refers to individuals of mixed descent

¹²⁵ LYA 6

¹²⁶ Ibid, 7

Africa, like the US, had an electoral college system, they differed in that the houses of Parliament were each given a particular number of electoral representatives; out of 88 members, 50 were chosen from the House of Assembly, giving them automatic election of the State President along with their automatic passage of bills in the legislative branch¹²⁷. The State President had a President's Council, which existed to decide on contested legislation. Here, too, there existed a built-in House of Assembly majority, as the Council was composed of 60 members, 35 of which were chosen either by the State President or the House of Assembly¹²⁸. Thus, there was, unlike in the United States, no check on the power of the legislature or the power of the executive; in fact, the House of Assembly, for all intents and purposes, elected the State President, who then declared "general affairs" and pushed all laws, even those that in practice would affect only the colored, Indian, or black African communities, to the vote of the House of Assembly or the President's Council. Add to this the fact that black Africans, who composed the majority of the population¹²⁹, were not enfranchised¹³⁰, and one begins to see how prevalent abuses of power were. Regarding the legislature and the executive, therefore, there was no ambition to counteract ambition¹³¹.

The Judicial System: Parliamentary Supremacy, and the Potential for Executive Overhaul

The only hope for South African checks, then, lay within the judicial system, but here, too, the House of Assembly retains almost absolute authority. Unlike American law, which has stressed Judicial Review as far back as the Federalist Papers¹³², South African law was founded in the doctrine of parliamentary supremacy¹³³. While the infamous 1948 election, which brought the Afrikaners into power, resulted in a questioning of multiple old-fashioned British legal concerns, this doctrine was not one of them. Instead, with the rise of the National Party came the

¹²⁷ Ibid., 6

¹²⁸ Ibid., 8

¹²⁹ FIND CITATION

¹³⁰ Between 1976 and 1981, over 9 million black Africans were denationalized (LYA 9)

¹³¹ See James Madison, Federalist No. 51

¹³² Alexander Hamilton, Federalist No. 78

¹³³ TT 13

prominence of parliamentary supremacy¹³⁴, and by 1983, the Constitution of South Africa elaborated a sort-of parliamentary stare decisis in that “No court of law shall be competent to inquire into or pronounce upon the validity of an Act of Parliament”¹³⁵. South African law goes further in denouncing judicial review in that it expressly allows the violation of a law if such violation can be “justified in light of the court’s perception of the intention of parliament”¹³⁶. Without judicial review, the will of the legislature reigns supreme; likewise, given that even in the last years of Apartheid over 60% of the justices identified themselves as Afrikaner¹³⁷, the judiciary, like the executive and the legislature, tended to be sympathetic toward the National Party leadership. This was not always so—when the National Party gained power, the courts were composed of liberal justices appointed under the leadership of United Party leader Jan Smuts¹³⁸. The National Party, however, quickly realized the threat to their absolute power within the judiciary and thus expanded the size of the Appellate division, appointing National Party sympathizers and followers of judicial restraint and abstentionism to the newly created positions¹³⁹. Within the new National Party judiciary, even if judicial review were a prevalent ideology, it would not have been enough. As liberal Judge David Friedman said, “It is only through the courts exercising their powers fearlessly and impartially, that a proper balance can be achieved between the interest of the individual’s liberty and the interest of the state in bringing alleged wrongdoers to justice”¹⁴⁰.

The Judicial System: American Checks and Balances

¹³⁴ Ibid.

¹³⁵ Republic of South Africa Constitution, Act 110 of 1983 s. 34(3)

¹³⁶ TT 14

¹³⁷ LYA 27

¹³⁸ Ibid., 28

¹³⁹ Ibid.

¹⁴⁰ Quoted in Ibid., 29

The commitment to parliamentary superiority in South Africa is, of course, a far cry from American Constitutional History, in which Chief Justice John Marshall, in his famous opinion on judicial review in *Marbury vs. Madison*, evinced, “an act of the legislature repugnant to the constitution itself is void [...] Those, then, who controvert the principle that the Constitution is to be considered in court as a paramount law are reduced to the necessity of maintaining that courts must close their eyes on the Constitution, and see only the law.” Far from random, Marshall’s decision lay within an explicitly American way of thought; in *Federalist No. 78*, Alexander Hamilton espoused a similar niche for the Judicial system, arguing “It is far more rational to suppose, that the courts were designed to be an intermediate body between the people and the legislature, in order, among other things, to keep the latter within the limits assigned to their authority.”

While judicial review reigns supreme in American law, the Constitution is also vague in essential places. For example, Article III provides Congress with the power to set the number of justices sitting on the Court; throughout American history, this number has been changed from six to seven to its current number, nine¹⁴¹. Franklin D. Roosevelt’s “Court-Packing” plan, though defeated by Congress in 1937, demonstrates that America is not immune to the appeal of expanding executive power over the judiciary. Roosevelt wanted to pack the Court with those justices that were favorable to his New Deal legislation¹⁴², thereby ensuring their survival; whether or not one supports such legislation, however, does not change the fact that it is possible for Congress to amend the amount of justices and, therefore, enact legislation similar to the National Party’s expansion of the appellate division in South Africa. If the legislature and executive become sufficiently frustrated with the judiciary, history shows it is not beyond them to assume further executive control.

Where does this comparison of Constitutional frameworks lead us? America possesses some of the same institutions that abused power during South African Apartheid, including an electoral college with members appointed by the legislature and the ability of Congress to restructure, at its whim, the Supreme Court. In significant ways, however, the American Constitution protects against such abuses in ways that the ambiguities and built-in majorities of

¹⁴¹ See: The Judiciary Act of 1789, the Judicial Circuits Act of 1866, and the Judiciary Act of 1869

¹⁴² http://abajournal.com/magazine/february_5_1937/

the South African Constitution could not, through such institutions as universal suffrage, an articulated and institutionalized Bill of Rights¹⁴³, and judicial review. The American system of checks and balances negates, or at least radically reduces, the risk of a single group or person to gain absolute power. James Madison words it best, writing, “In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself”¹⁴⁴. Therefore, because the American constitutional framework does not leave it up to the discretion of one single house or person to interpret all ambiguities in the law, it is within the system of checks and balances that American protection from a police state lies *in theory*; how this is applied in practice is discussed above.

Executive Orders: A Loophole in Checks and Balances?

Executive abuse of power has the most potential in the almost dictatorial allowance of Executive Orders. The profound history of executive orders in America began in 1789 and has culminated in over 13,000 numbered orders¹⁴⁵. The astronomical number hints at the inherent ease with which the executive can wield this power, as does its contrived Constitutional derivation. While no such power exists within the Constitutional framework of the United States, every President since Washington has used the ambiguous “executive Power” granted in Article II, Section I and the subsequent “Care that the Laws be faithfully executed” clause in Section 3 to provide the executive with authority for such orders.

The problem with Executive Orders is that, though they need not pass through Congress, they carry the same weight as Congressional legislation. While these can be used in progressive ways, such as when President Dwight D. Eisenhower used an executive order to desegregate

¹⁴³ Such a proposal was explicitly rejected in the discussion over the 1983 South African Constitution (LYA 8)

¹⁴⁴ James Madison, Federalist No. 51

¹⁴⁵ <http://www.thisnation.com/question/040.html>. While this number is staggering, it is not exhaustive. The State Department retroactively added the numbers and began with the 1862 Emancipation Proclamation; therefore, 13,000 is most certainly an extreme underestimation.

schools in the 1950s¹⁴⁶, the potential for abuse is an attribute inherent—if not ordained—by the power itself. In fact, as the years have passed, executive orders have become more prevalent and more expansive than their predecessors¹⁴⁷. Such an order can, in theory, be used as a unilateral *carte blanche* for Presidential whims, and can therefore negate the other checks the Constitution was so diligent in providing for the other powers. If Congress disapproves of such an order, they can pass a law; however, the President may veto this law, and, therefore, a simple majority is not enough to override a Presidential veto. Additionally, power over matters of foreign policy and national defense are constitutionally reserved for the Executive, and therefore are unlikely to receive comment or nullification by Congress. Therefore, an executive order, when passed, will largely stand in practice, regardless of the intention of the majority of Congress. The judicial branch also theoretically provides protection against such abuses, as Executive Orders may be challenged in court as violations of Presidential limitations. Once again, however, practice does not match theory; only twice in the history of the United States has a court explicitly struck down an executive order¹⁴⁸. The power, like in South Africa, therefore lies in the reasonableness of the executive; but is such reasonableness truly demonstrated in EO 9066, in which President Franklin D. Roosevelt unilaterally delegated authority for the military to target Japanese and German –Americans and send them to internment camps? The concern over Executive Orders stems largely from the threat of the creation of a “permanent state of exception”¹⁴⁹ ([Giorgio Agamben](#)). If such a state were to be declared, it would not be unlike South Africa’s incorporation of emergency legislation into otherwise normative law.

A Brief History of South African Surveillance

¹⁴⁶ Ibid.

¹⁴⁷ An example of such expansion is moving from desegregation of schools under Eisenhower to a war with Yugoslavia under Clinton. It should be noted that all wars established through executive order have also had Congressional approval; however, the question as to whether a President can act unilaterally in declaring war through Executive Orders is has not yet been Constitutionally resolved.

¹⁴⁸ <http://www.cato.org/testimony/ct-wo102799.html>; See: *Youngstown Sheet & Tube Co. vs. Sawyer*, 343 US 579 (1952)

¹⁴⁹ See: Agamben, Giorgio. State of Exception. 2005

It is now time to look at a brief recount of surveillance and ordinary security law within South African Apartheid¹⁵⁰. Surveillance implies the clandestine collection of information, and in South Africa especially, “secret information is almost always the basis for the decision to ban or detain people, to deprive them of passports, or to inflict other arbitrary penalties upon them”¹⁵¹. Throughout Apartheid, four major laws have dictated the ordinary powers of the government in terms of surveillance and bugging: the Post Office Act 44 of 1958, the Radio Act 3 of 1952, Internal Security Act 74 of 1982, and the Criminal Procedure Act of 1977. The Post Office Act deals with the interception of communications and prior to 1972, it did not authorize wiretapping or any other interception of telecommunications¹⁵²; however, it was later amended, upon recommendation of the Potgieter Commission of 1971, to include not only telecommunications and postal items but also to target any communication between any two people for a period not exceeding six months¹⁵³. It was therefore not, as in the U.S., “particularly describing the place to be searched, and the persons or things to be seized”¹⁵⁴ but rather a more general rule that emphasized not the surveillance of particular conversations but rather the surveillance of an individual himself. The limitation of this law was that the one intercepting the materials must make a specific case for the necessity of the interception based on “the maintenance of the security of the public” and that it could only be ordered by “responsible” officials, including the National Intelligence Service, the Minister of Law and Order, the Minister of Defense, the Minister of Posts and Telecommunications, or an officer authorized by the Minister of Posts and Telecommunications¹⁵⁵. Anthony Mathews, noted South African legal scholar, perhaps words it best when he writes “The problem about this limitation is that it is purely internal and that we have, therefore, to rely on members of the ruling party and their subordinates not to abuse the power by invoking it against their opponents without adequate

¹⁵⁰ It should be once again pointed out that this brief focuses not on race law, but rather security law. Despite similar motivations, the two were seen as independent categories of law within South Africa itself.

¹⁵¹ FSSRL 179

¹⁵²¹⁵² Ibid.

¹⁵³ Ibid., 181

¹⁵⁴ United States Constitution, Amendment IV

¹⁵⁵ FSSRL 181

justification”¹⁵⁶. The idea of external checks, however, was explicitly rejected by the South African government under the belief that it was impractical, as it would inform the victim of the surveillance beforehand, thereby defeating the very purpose of surveillance. It is within this logic that the South African government reveals its bias toward national security, or perhaps more accurately, the protection of the Afrikaner government, over individual liberty. Therefore, the Post Office Act permits unannounced though somewhat regulated surveillance of individuals for security-related crimes, justifying the procedure by invoking the interests of the State over the individual.

South Africa takes a slightly more regulated stance when it comes to bugging. The Radio Act of 1952 prevents the interception of private conversations by broadcasters using radio apparatuses up to 3000 GHz, which notably omits laser signals and thus leaves room for ambiguity¹⁵⁷. The Criminal Procedure Act of 1977 prohibits the invasion of private property to plant bugs, stating that officers may enter “premises for the purpose of interrogating [a person who may furnish information on an offense] and obtaining a statement from him: Provided that such police official shall not enter any private dwelling without the consent of the occupier thereof”¹⁵⁸. Warrants are issued and police officers may without warrants act, however, upon “reasonable grounds” of the commission of a crime, the disruption of the security of the state, the issuance of a warrant, or the imminent destruction of a necessary object¹⁵⁹. The question is what qualifies as “reasonable,” and what prohibits a magistrate from manipulating the ambiguities within the law to serve his own needs? The answer? Nothing. The justification for such laws and their subsequent results is the importance of the security of the state¹⁶⁰, though in South Africa the true motivation was retaining white supremacy. Once again the lack of external supervision bestows almost supreme power upon the South African leadership.

¹⁵⁶ Ibid., 182

¹⁵⁷ Ibid., 183

¹⁵⁸ Criminal Procedure Act of 1977, Sec. 26

¹⁵⁹ Ibid., Sec. 25

¹⁶⁰ In fact, entire sections of the law are dedicated to powers in connection with State security, listed as separate from other offenses.

The Pass Laws Act, Public Safety Act, Internal Security Act:

Are These Predecessors of the Military Commissions and PATRIOT Act?

We now shift our focus to individual laws, specifically enumerating those that can later be related to American expansion of powers through the PATRIOT Act and subsequent legislation. In particular, we will analyze the way in which the Afrikaner government assumed greater powers and determine whether American legislation follows similar patterns. The South African laws to be considered are the Pass Laws Act of 1952, the Public Safety Act of 1953, and the Internal Security Act of 1982. These laws will be considered chronologically to extrapolate an overarching pattern to serve as the basis of our comparison with the United States in terms of meaning, motivation, justification, and effect on the populace.

Is the REAL ID the New Pass Laws Act?

The Pass Laws Act of 1952 mandated all black South Africans ages 16 and over to carry a passbook, or dompas, with them wherever they went. This passbook listed the name of the bearer, his photograph, his fingerprints, his address, the name of his employers, the duration of his employment, and a behavioral evaluation completed by his employer. In 1952, as part of what was known as the ANC's "Defiance Campaign, nearly 8,600 pass-law resisters were arrested¹⁶¹; between 1965 and 1975, over 5.8 million individuals were arrested and prosecuted for pass-law violations¹⁶². While this is largely seen as a part of race law and not security law, it does have unique implications for the proposed REAL ID within United States law. The status of the REAL ID Act of 2005 is currently up in the air¹⁶³ thanks to issues raised by organizations

¹⁶¹ AR:PPRD 99

¹⁶² Ibid., 321

¹⁶³ http://www.nextgov.com/nextgov/ng_20090303_7315.php

such as the ACLU¹⁶⁴ and the extensions provided to states across the nation. Says Governor Mark Sanford in opposition to the REAL ID:

This proposal is one more step away from the Founding Fathers' vision of a limited federal government. Our greatest homeland security is liberty, and the Founding Fathers believed our greatest threat to liberty was a central government grown too powerful. Accordingly, they set up checks on federal power by vesting authority at the individual and state levels. REAL ID disrupts this delicate balance of power...¹⁶⁵

Implications of The REAL ID Act on Checks and Balances and Executive Power

Governor Sanford makes an important point here. The checks and balances of the American government have already been established as the single most vital Constitutional obstacle to the formation of a police state. If the REAL ID interferes with this system, American citizens may soon see a Congress vested with more power than that with which anyone is comfortable. Does the REAL ID really get rid of checks and balances? The REAL ID has a few measures associated with it. First, it has certain security requirements for licenses. Second, it mandates particular background checks to guard against fraudulent documents. Third, it enforces the verification of the authenticity of documents provided by applicants and the storage of this data for 10 years, including one's birth record and address¹⁶⁶. The security requirements for the license include one's full legal name, date of birth, gender, identification card number,

¹⁶⁴ CITE

¹⁶⁵ Gov. Mark Sanford, "Real ID Side Effects," *Washington Times*, April 14, 2008

¹⁶⁶ <http://www.ncsl.org/programs/transportation/RealIDupdate06.htm>

photograph, address, signature, some sort of feature to prevent tampering, and an unspecified machine-readable technology¹⁶⁷. For those individuals who do not get a real ID that meets the minimum requirements above, the license or identification card issued must “clearly state on its face that it may not be accepted by any Federal agency for federal identification or any other official purpose; and use a unique design or color indicator to alert Federal agency and other law enforcement personnel that it may not be accepted for any such purpose”¹⁶⁸. The possibilities for abuse based on the text of the law are therefore three-fold. First, what is the unspecified machine-readable technology? While the DHS denies the possibility of radio frequency identification (RFID) tags¹⁶⁹, there is nothing in the law that expressly prohibits this. The use of such technology would be a blatant infringement on personal privacy, as such tags emit radio frequencies that allow the monitoring of the movement of anyone who possesses such a card¹⁷⁰. As mentioned, without a REAL ID, there is no way for official verification of one’s identity¹⁷¹; therefore, the location of every US citizen who wants to drive, collect social security, fly on an airplane, use a bank, etc., would be available at any given time¹⁷². What safeguards are in place to prevent this? It seems to be the reasonableness¹⁷³ and the responsibility¹⁷⁴ of the government or the DMV officers¹⁷⁵. Instead of asking whether our government officials are reasonable, however, we should ask if it is instead reasonable of Americans to question the intentions of a

¹⁶⁷ Sec 202 B, qtd in http://www.ncsl.org/standcomm/sctran/REAL_ID_Act_of_2005.htm

¹⁶⁸ Sec 202 d. 11a and b

¹⁶⁹ CITATION DHS WEBSITE

¹⁷⁰ <http://www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html>

¹⁷¹ This claim has been denied by the DHS.

¹⁷² Because all of these activities are impossible with other forms of identification, it is in the states’ interest to ensure its citizens possesses a REAL ID (ibid), despite its probably staggering costs to the states. Likewise, in South Africa there was a lack of economical thinking, as the enforcement of the Pass Laws cost upward of \$130 million (AR:PPRD 321). This could be another way for the national government to assume increased control, as states forced into an economic downturn may look to the national government for help.

¹⁷³ Compare: Criminal Procedure Act of 1977

¹⁷⁴ Compare: Post Office Act of 1958

¹⁷⁵ Here once again the Department of Homeland Security has issued statements at odds with the text of the law, in this case asserting “To ensure that an individual’s personally identifiable information is protected, the final rule prohibits the release and use of information inconsistent with the Federal Driver’s Privacy Protection Act”

government that quietly tacked such ambiguities to vital emergency rescue legislation¹⁷⁶. The answer, of course, is yes. Unless the law is sufficiently amended, Governor Sanford's point will stand and America's last defense against authoritative power will be blind faith in the altruism of her leaders. As Congressman Ron Paul (R-Tex) warned, "History shows that governments inevitably use the power [of national ID cards] to monitor the actions of people in harmful ways."¹⁷⁷ Certainly South African history does.

The Public Safety Act: Placing Increased Power in the Hands of the Security Forces

We next turn to the Public Safety Act of 1953. The law included a variety of stipulations that expanded the security forces of South Africa, including:

1. "A Member of a security force may, without warrant of arrest, arrest or cause to be arrested any person whose detention is, in the opinion of such member, necessary for the safety of the public or the maintenance of public order or for the termination of the state of emergency, and may, under a written order signed by any member of a security *force*, detain or cause to be detained any such person in custody in a prison" 3. (1)
2. "The Minister may, without notice to any person and without hearing any person ... order that a person arrested and detained ... be further detained, and in that prison, for the period specified in the notice or for as long as these regulations remain in force" 3. (3)
3. "Any person convicted of an offence under these regulations shall be liable to...imprisonment for a period not exceeding ten years...and the court convicting him may declare any goods, property or instrument by means of which or in connection with which the offense was committed, to be forfeited to the state" (13)
4. "No civil or criminal proceedings shall be instituted or continued in nay court of law against the State or the Government of a self-governing territory, the State President,

¹⁷⁶ The REAL ID act was tacked onto the 2005 Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief.

¹⁷⁷ Not only is there the potential for government abuse, but there is also the possibility of corporations, hackers, etc., being able to manipulate the system and access information on you and, if RFID technology is used, your whereabouts. Because the REAL ID is seen as a more secure form of identification, the chance of identity theft grows exponentially.

member of Cabinet, member of security force, person in the service of a State, person acting b/c they were told to or approved to by anyone in the service of the state” 15.

(1)(a-f)

As Nicholas Haysom, a Human Rights Attorney and later Legal Advisor to President Nelson Mandela, writes, “[Such laws were] a prescription for unsupervised and unaccountable behavior on the part of the security forces, who were vested with substantial executive powers and armed with an array of violent weapons”¹⁷⁸. The Public Safety Act also began a trend within South African history in which the distinction between emergency law and ordinary law was often, for the Afrikaner government, blurred; with the passage of the Internal Security Act, it was utterly irrelevant¹⁷⁹, as a state of emergency could be declared with nothing more than the desire of the State President¹⁸⁰. Though such states of emergency were not declared until 1960, the results of placing such expanded rights into the hands of the police and military had disastrous consequences, including police shootings and the detention of over 26,000 persons by 1986¹⁸¹, 11,503 of whom were detained in the 1960 state of emergency¹⁸². By the end of apartheid, the total number of detainees had reached over 32,500 individuals, 30% of whom were under the age of 18¹⁸³.

Within the four statutes gleaned from the Public Safety Act, there are three main points of comparison with the United States: first, the investment of the power of detention in all members of the security forces; second, the arresting and detention, without notice or hearing, of any individual for an unlimited period of time; and third, the inability to hold a criminal trial against anyone associated, directly or indirectly, with the State. The overall implication of the law in writing into ordinary law what were normally powers reserved for emergency laws is likewise a point of comparison. All four of these provisions are essential in police states, because they

¹⁷⁸ FYA 75

¹⁷⁹ See: Internal Security Act 36 of 1965; Criminal Procedure Act 56 of 1955, amended by Section 7 of the Criminal Procedure Amendment Act 96 of 1955

¹⁸⁰ TT 19

¹⁸¹ FYA 77

¹⁸² TT 19

¹⁸³ TT 22

imbue executive power within the security forces and suppress primary checks on the government by stripping citizens of habeas corpus and the right of appeal, all within a permanent context. The American Military Commissions Act (MCA) is most akin to this law and will be discussed following the Internal Security Act, which likewise sheds light on the significance of the MCA.

The Internal Security Act and the Military Commissions Act:

The Role of Detention and Habeas Corpus in the Formation of a Police State

The Internal Security Act, passed in 1982 at the behest of the Rabie Commission of Inquiry into Security Legislation, was the product of the consolidation of earlier South African Security statutes¹⁸⁴ and served as the legal go-ahead for police brutality for almost a decade. Within the law, the writ of habeas corpus was excluded in all instances of detention¹⁸⁵, brutal police interrogation, often categorized as torture, was authorized¹⁸⁶, and laws generally reserved for states of emergency were incorporated into ordinary law. Under the act, anyone within the South African security forces, no matter how junior, was permitted to arrest and detain¹⁸⁷ with no trial and no opportunity for bail¹⁸⁸. Because of the ambiguous definitions of the crimes, police had what amounted to a *carte blanche* to detain anyone from actual terrorists to outspoken political activists¹⁸⁹. The period of detention under the 1987 State of Emergency was limited to 30 days; however, the Minister of Law and Order frequently, if not always, abused his power to extend that deadline indefinitely¹⁹⁰. The Detainees' Parents Support Committee (DPSC) conservatively

¹⁸⁴ FYA 38

¹⁸⁵ LYA 24

¹⁸⁶ See: Sect 6, Terrorism Act of 1967.

¹⁸⁷ Waks vs. Jacobs 1990 (1) SA 913 (T) distinguished between ordinary and emergency law, finding that the power to detain was reserved only for senior police officials unless a state of emergency was declared.

¹⁸⁸ Internal Security Act 74 of 1982, Sect 29

¹⁸⁹ FYA 24

¹⁹⁰ FYA 40

determined that from June 12 to December 31 of 1986, 25,000 people were detained, many of who were under the age of eighteen¹⁹¹. These detainees were, in general, “subjected to a harsh and punitive regimen that seemed largely unrelated to the purposes of securing public safety”¹⁹². They were forced to undergo beatings, solitary confinement, and starvation¹⁹³, children as well as adults.

Torture and the suspension of habeas corpus do two dangerous things for a state government. First, both of them imbue the security forces and/or government with almost entirely unchecked power, which as we have seen is the foundation of a police state. Second, both of them involve the government treating its population as less than humans¹⁹⁴ and remove one of the people’s vital checks on governmental power. Does America follow the South African model by allowing torture and suspending Habeas Corpus? Yes and no. The suspension of the writ of habeas corpus has a Constitutional basis, as “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”¹⁹⁵. Despite this provision, the United States Supreme Court ruled in *Boumediene vs. Bush* that Section 7 of the Military Commissions Act of 2006 was unconstitutional because of its suspension of the writ of habeas corpus¹⁹⁶. Justice Kennedy had an acute awareness of the importance of habeas corpus in securing individual freedom when he wrote, “the Framers viewed freedom from unlawful restraint as a fundamental precept of liberty, and they understood the writ of habeas corpus as a vital instrument to secure that freedom.” Therefore, while the legislation existed to abolish the writ of habeas corpus, judicial review precluded it from doing so in practice. *Boumediene vs. Bush*¹⁹⁷ serves as a quintessential example of the power of checks and balances in preventing

¹⁹¹ *Ibid.*, 41

¹⁹² *Ibid.*, 42

¹⁹³ *Ibid.*, 43

¹⁹⁴ In fact, freedom from torture is a human right, as declared by The Universal Declaration of Human Rights, and the United Nations’ International Covenant on Civil and Political Rights, Part III Art. 7

¹⁹⁵ United States Constitution, Art. I Sec 9

¹⁹⁶ <http://www.salon.com/opinion/greenwald/2008/06/12/boumediene/>

¹⁹⁷ See also: *Hamdi vs. Rumsfeld*, [542 U.S. 507](#) (2004) and *Hamdan v. Rumsfeld*, [548 U.S. 557](#) (2006),

police state legislation and maintaining the people's check on governmental abuses through habeas corpus.

Torture in the United States is a similar story. The U.S. has admitted to torture,¹⁹⁸ and the Department of Justice has confirmed physical and verbal abuse of 762 post 9/11 detainees¹⁹⁹. It seems the executive has no qualms about using torture and instead fears the Supreme Court²⁰⁰, which has continuously asserted its right to judicial review in cases involving detention and torture. In *Haman vs. Rumsfeld*, for example, the government argued that the Supreme Court did not have the right of judicial review over military tribunals; the Supreme Court, however, explicitly rejected this judgment. But what happens when the government passes a law that negates judicial review? Unsatisfied with the clear judicial oversight established in *Hamden*, Congress enacted the Military Commissions Act of 2006, which authorized the indefinite detention of "enemy combatants" and explicitly removed it from the potential for judicial review. While *Boumediene* ensures habeas corpus is maintained by rendering parts of the law unconstitutional, there have as of yet been no cases in the Supreme Court dealing with the issue of judicial review. Thus, the executive and legislature seem to be doing their utmost to parallel the Internal Security Act; in so doing, they violate international humanitarian law²⁰¹ and provide the underpinnings for an increasingly oppressive police state. The judiciary has done its best to halt such a progression; however, within a system based on checks and balances, is it wise to invest all hope for the future on one branch? There is little difference between when one institution prevents the expansion of power and when one institution asserts it.

The United States and it's Future: What does this mean?

¹⁹⁸ http://www.usatoday.com/news/washington/2009-01-14-pentagon-torture_N.htm

¹⁹⁹ U.S. Department of Justice Office of the Inspector General, *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks*, June 2003. *Supplemental Report on September 11 Detainees' Allegations of Abuse at the Metropolitan Detention Center in Brooklyn, New York, December 2003*. Twelve detainees were killed as a direct result of the torture they endured (see: http://www.humanrightsfirst.org/media/2006_alerts/etn_0222_dic.htm)

²⁰⁰ <http://edition.cnn.com/2008/POLITICS/07/24/cia.torture/index.html>

²⁰¹ <http://www.unhchr.ch/hurricane/hurricane.nsf/view01/13A2242628618D12C12572140030A8D9?opendocument>

Though our analysis of South African and American law, we have discovered that America has the legislation and the technology to become a surveillance state. What America lacks, however, is the Constitutional framework to do so. Judicial review, a multi-party system, an enumerated Bill of Rights, universal suffrage, and organizations like the ACLU and Human Rights First serve as the vital checks on the power of a power-hungry executive. That being said, the executive has spent the better part of the post 9/11 years enacting laws supported by the legislature that expand its powers to the obvious detriment of American privacy. With the implementation of the REAL ID Act and the furtherance of existing laws like the PATRIOT Act and the Military Commission Act, the government can easily usurp power and use it to monitor its citizens. Such behavior is not only rooted in international precedent but also fits with the American trend toward annexing executive power. What South African apartheid teaches us is that disguising emergency legislation as ordinary law is one of the first steps toward a police state; with ambiguous definitions so prevalent in American legislation, it is obvious this is a step that has already been taken. So the question remains: Are we a police state yet? No. But will we be in the future? If the judiciary and the people surrender their vital checks on American government, yes. But if not, the intricate interlacing of powers as designated by the United States government serves itself as a fundamental safeguard against the annexation of executive power. Checks and balances will not work unless each establishment embraces its powers, and that means the people must hold the government responsible for every attempt at expansion of power. America teaches that meeting one's potential is of the utmost importance; when it comes to the government reaching its potential apex of power, this is a lesson Americans would do well to forget.

Rights, Limits, and Education: What can we do as citizens?

Learning our lesson is something that is much easier said than done, especially in a society where privacy violations not only go under the radar too often, but are even applauded as a necessary measure for the War on Terror. The only real solution is to increase awareness through education, reminding people of their constitutional freedoms, and especially drawing a line between national security and individual rights. While there is no immediate method to do this, it starts with immersing the lessons of the constitution into our elementary, middle, and high school classes. It also begins with grassroots movements and electing people who are aware that there is a clear distinction between security and privacy and that while security is important, we also need to secure our rights. Many of the people apathetic to change in our nation will ask, “Can we really change the law? What can a few people really do?” but we have to remember that some of the most important historical changes in our world have come from the people themselves. If we as citizens of the United States continue to sit back and think that we cannot change the law, then that is the only thing that will stop us from protecting our rights and also the fundamentals that our constitution is based upon. The impacts of not preserving these core values have had and will continue to have greater effect on our daily lives than we will be able to truly comprehend. As shown above, many of our rights are already slowly deteriorating in the name of security and racial profiling of those who look as if they are Muslim has increased ten fold. Most importantly, the premise of our legal system, “innocent until proven guilty”, is slowly becoming “guilty until proven innocent”. Illegal searches and intruding technologies have created a world where we are slowly all becoming suspects and losing our right to not only privacy, but innocence as well.

Increasing Awareness: Education and Understanding

Understanding the Bill of Rights and why they were created within the Constitution is one of the most fundamental points that should be in our educational curriculum. While every child “supposedly” learns the Bill of Rights and its importance, it is shocking to see how little they actually learn of the importance and application of their rights and also, how much they actually remember. In a study conducted in 2000, researchers found that, “although educators demonstrate greater knowledge of First Amendment freedoms than the general public, roughly

one in five can not recall any of the five freedoms. While three out of four educators recall freedom of speech, fewer than one in four can identify each of the other freedoms.”²⁰² But that wasn’t the only problem that this study found. Not only were educators unsure of their rights, but those who were teaching students about rights were reluctant to talk about why certain rights, such as free speech or privacy were important because they felt that their authority in the classroom might be undermined.²⁰³ In summary, these are the two parts of the first problem: Teachers themselves are not well-educated about the Bill of Rights and what they are entitled to in the Constitution and even those who are educated are not willing to adequately address the importance of those rights.

The second problem derives from how little these students remember, even within a year of being taught. This is the result of an insufficient impact not being made when the Bill of Rights is introduced. Children are taught to believe that these rights are concepts that the government will always protect, not that there are many governments in the world who currently do not protect these rights. Additionally, several states use them to create surveillance states and administer every move of their citizens. According to a study done by the Center for Civic Education, while high school students are still more aware of their rights than adults who had been removed from school for a varying lengths of time, “students [who study them are] misinformed about specific constitutional rights and ignorant of the meaning, history, and application of key concepts...”²⁰⁴. Even those who remember what their rights are do not remember the importance of them and why they need to be applied today. Reports from the National Assessment of Educational Progress have also stated that there are “glaring gaps” in the amount of knowledge middle school students show concerning their rights and also about what

²⁰² Comparisons of educators' opinion with those of the public are based on the annual State of the First Amendment survey released by the First Amendment Center in July 2000.

<http://www.freedomforum.org/templates/document.asp?documentID=13390>

²⁰³ Viadero, Debra. "Celebrating Bill of Rights, Schools Tackle 'National History Lesson'" Education Week Web only (4 Dec. 1991). Education Week. Editorial Projects in Education. 22 Apr. 2009
<<http://www.edweek.org/ew/articles/1991/12/04/14histor.h11.html#top>>.

²⁰⁴ Quigley, Charles N. et al. PRELIMINARY REPORT ON HIGH SCHOOL STUDENTS' KNOWLEDGE AND UNDERSTANDING OF THE HISTORY AND PRINCIPLES OF THE UNITED STATES CONSTITUTION AND BILL OF RIGHTS. Calabasas, CA: Center for Civic Education, 1987.

the term ‘civil liberties’ even means.²⁰⁵ While almost two decades have passed since the studies were completed, recent articles have shown that students do not assimilate the importance of their rights and those who do learn about them, do not retain this knowledge in the long run.

The Long Run: Adults and Civil Liberties Education

The core problem with rights is derived from what was discussed previously. While we should not necessarily expect children to remember their exact rights or understand the magnitude of those rights, *in the long run*, those children become adults who are capable of instigating change. When the importance of these rights is discarded, intolerance, dissolution of privacy, and other related problems will occur. While people generally agree that rights are positive, many people who do not understand the value and importance of these rights do not support civil liberties for everyone, a paradox on its own. A study conducted in the 1980’s showed adults who had learned what the Bill of Rights represented during the 1950s had attitudes that were “generally positive, but support for certain liberties and rights [markedly declined] when they [were] applied to cases involving unpopular minority groups or individuals.”²⁰⁶ Even those who had been taught their rights and liberties did not believe they applied to all people, regardless of affiliation, religion, etc.

On first intuition, it seems somewhat unreasonable to think that our current movement towards to the surveillance state is a result of the failure of education to cement the significance of our Bill of Rights. However, historian Michael Kammen acknowledges that studies found that half of the adult respondents misconceived the role and powers of the Supreme Court in our constitutional system defined by separated powers and checks and balances. He also argues that this “long-standing public ambivalence to and misunderstanding of the Supreme Court's role in protecting individual rights against the potential tyranny of majority rule”²⁰⁷ illustrates how often individuals are the real reason governments can get operate freely. When people misunderstand

²⁰⁵ Ravitch, Diane and Chester E. Finn, Jr. WHAT DO OUR 17-YEAR-OLDS KNOW? A REPORT ON THE FIRST NATIONAL ASSESSMENT OF HISTORY AND LITERATURE. New York: Harper & Row, 1987.

²⁰⁶ McCloskey, Herbert and Alida Brill. DIMENSIONS OF TOLERANCE: WHAT AMERICANS BELIEVE ABOUT CIVIL LIBERTIES. New York: Russell Sage Foundation, 1983.

²⁰⁷ Kammen, Michael. A MACHINE THAT WOULD GO OF ITSELF: THE CONSTITUTION IN AMERICAN CULTURE. New York: Alfred A. Knopf, 1986.

their rights they cannot fight for those rights and when they misunderstand the institution that protects those rights, then they give the institution free reign to use their rights as it wants. By the time they leave high school and are of voting age, it is essential that students can “define, analyze, and evaluate”,²⁰⁸ the issues put forth in the Bill of Rights and that they understand the vital need we have for them in a world where many of these rights go unprotected.

While many argue that education is only a long-term solution, it becomes a short-term solution when more people, especially teenagers, become involved. When students are educated on certain subjects, particularly those that may apply to their daily lives, their views change on issues such as minority rights, privacy rights, and the role of the Constitution as a whole. These are the people who then start grassroots movements and lobby their representatives to enact change. What differentiates America from many of the historical and even current examples of countries that violate the rights and liberties of their citizens is that America still has many mechanisms in place where the people can tell the government what they want. Without the education of the people, and making them aware of what possibilities are open to them, however, change can never truly occur. The only way we can truly stop a surveillance state from developing is to ensure that an ample amount of people make their voices heard and elect people who will listen to their voices in the first place.

Security and Privacy: Where do we draw the line?

Currently, our legal system supposedly works under the doctrine of “innocent until proven guilty,” but many would argue that with the current surveillance technologies being used, people are now “guilty until proven innocent.” This means that every person becomes a suspect, whether they are suspected of committing a crime or not. Under surveillance states or the beginnings of a surveillance state, the burden of proof no longer lies on the state but on the individual. Every act can be monitored without the individual being a suspect and that forces the individual to prove his innocence. Furthermore, the facts are never given the benefit of the doubt and are instead always deemed to be suspicious, which can be extremely harmful. It is important to draw the line where the burden on proof lies when reviewing the conflicting ideals of privacy and security. As a Washington Post article from 2006 states, this debate “is about the limits of

²⁰⁸ Patrick, John. "Teaching the Bill of Rights." www.ericdigests.org. ERIC: Education Resources Information Center. 22 Apr. 2009.

the Fourth Amendment, which protects people from being swept into criminal investigations unless there is good reason to suspect they have broken the law.”²⁰⁹ When everyone becomes a suspect, then not only have we lost the right to privacy, but national security also loses its value.

Security: of the State, by the State, and for the State?

When addressing issues of security and privacy, it is important make a distinction between the two and also learn to fight security when it overpowers our right to privacy. When we lose our right to privacy, there is a reasonable chance that we are also losing what secures our liberty as well. We are losing the rights that secure us from an overly powerful state. It is imperative that we protect these rights that seem to be frivolous at times in order to prevent further rights abuses that may occur if we do not keep watch. As an article in the American Conservative quotes,

Three months after 9/11, [Attorney General John] Ashcroft announced, “To those who scare peace-loving people with phantoms of lost liberty, my message is this, your tactics only aid terrorists for they erode our national unity and ... give ammunition to America’s enemies.” Ashcroft is wrong to portray any criticism of Bush administration civil liberties policies as aiding and abetting terrorism. America is overdue for a searching examination of the powers the Bush administration has seized and the powers it is seeking.²¹⁰

There is a clear line between what Attorney General John Ashcroft deems necessary for security and what the reality of the situation reveals. It is necessary that we, as American citizens, understand that peaceful protests and fighting for our civil rights and liberties does not become “ammunition for our enemies.”²¹¹ Rather, they are the core values that our nation stands upon. The impact of losing these core values is far greater than we can measure.

²⁰⁹ Weiss, Rick. "Vast DNA Bank Pits Policing Vs. Privacy." *Www.washingtonpost.com* 3 June 2006. The Washington Post. 22 Apr. 2009 <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/02/AR2006060201648_pf.html>.

²¹⁰ Bovard, James. "Surveillance State." *Www.amconmag.com* 19 May 2003. The American Conservative. 22 Apr. 2009 <<http://www.amconmag.com/article/2003/may/19/00008/>>.

²¹¹ *ibid*

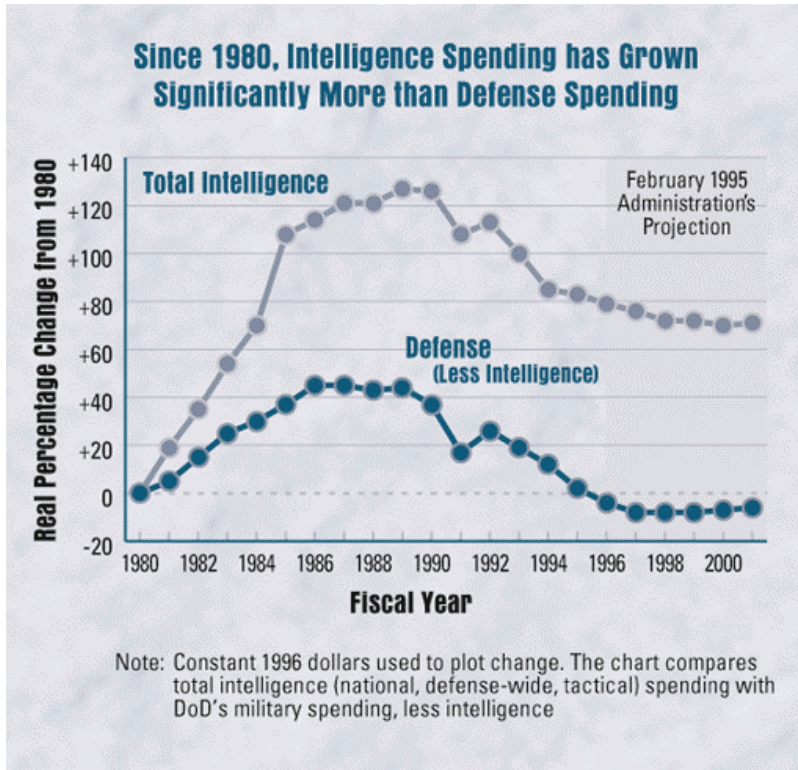
Conclusion

The Collapse of Legal and Constitutional Legitimacy: Preserving Democracy's Principles

Preserving our rights is not only important for Americans today but also to uphold the legitimacy of our constitution for future generations. If we do not protect the basic rights given to us by the constitution at the present, we may not feel the impact today. As a society who can look towards the future, however, we need to recognize the potentiality of our actions. We must see that the actions we do not stop now have the potential to do harm, more harm than if it is allowed to remain in our system. Instead of letting surveillance become something that is only used for security, we should also see transparency as security in its own right. This paper does not argue that America is a fully created surveillance state nor does it argue that America will become like South Africa because of the new technologies available to us. This paper also does not claim that these new technologies are negative or cannot be used to help our society progress; however, this paper does aim to show that we need to reinforce our rights and the constitution that our leaders have sworn to uphold. We need to ensure that we preserve the democratic principles that the United States of America was founded upon. If we lose the legitimacy of even the basic rights found in the Constitution, then we risk losing the legitimacy of the Constitution itself, an impact that has repercussions far greater than our own time.

APPENDIX

Figure 1- Graph on Intelligence Spending from 1980-1996



212

²¹² "Tracing the Size of the Annual Intelligence Budget," FAS, 1996, 5 April 2009, <http://www.fas.org/irp/budget/index.html>

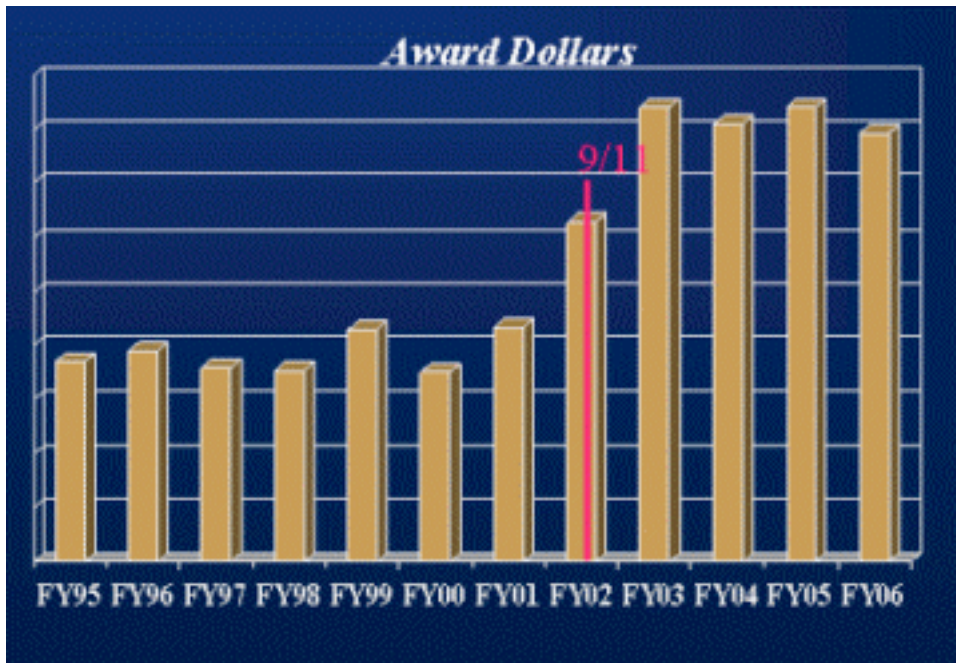
Figure 2- Intelligence Community of the United States



Source: Office of the Director of National Intelligence

Intelligence Agencies Represented (Left to Right, Top to Bottom): United States Air Force; US Army, Central Intelligence Agency (CIA); US Coast Guard; Defense Intelligence Agency (DIA); Department of Energy, Office of Intelligence; US Department of Homeland Security, Office of Intelligence and Analysis; Department of State, Bureau of Intelligence and Research (INR); Department of the Treasury, Office of Terrorism and Financial Intelligence; US Justice Department, Drug Enforcement Agency (DEA) and Federal Bureau of Investigation (FBI); US Navy Department of Marine Corps; National Geospatial-Intelligence Agency (NGA); National Reconnaissance Office

Figure 3- Projected Budget Increases in Classified Contracts for Intelligence 1995-2006



Source: www.globalsecurity.org

Figure 4- "Guesstimate" for FY 2009 Intelligence Budget

FY2009 Intelligence Budget

Total		\$66,500
	DOD	\$43,500
	Other Agencies	\$13,000
NIP - National Intelligence Program		
	CIA	\$10,000
	FBI	\$3,000
	DHS / USCG / IAIP	\$100

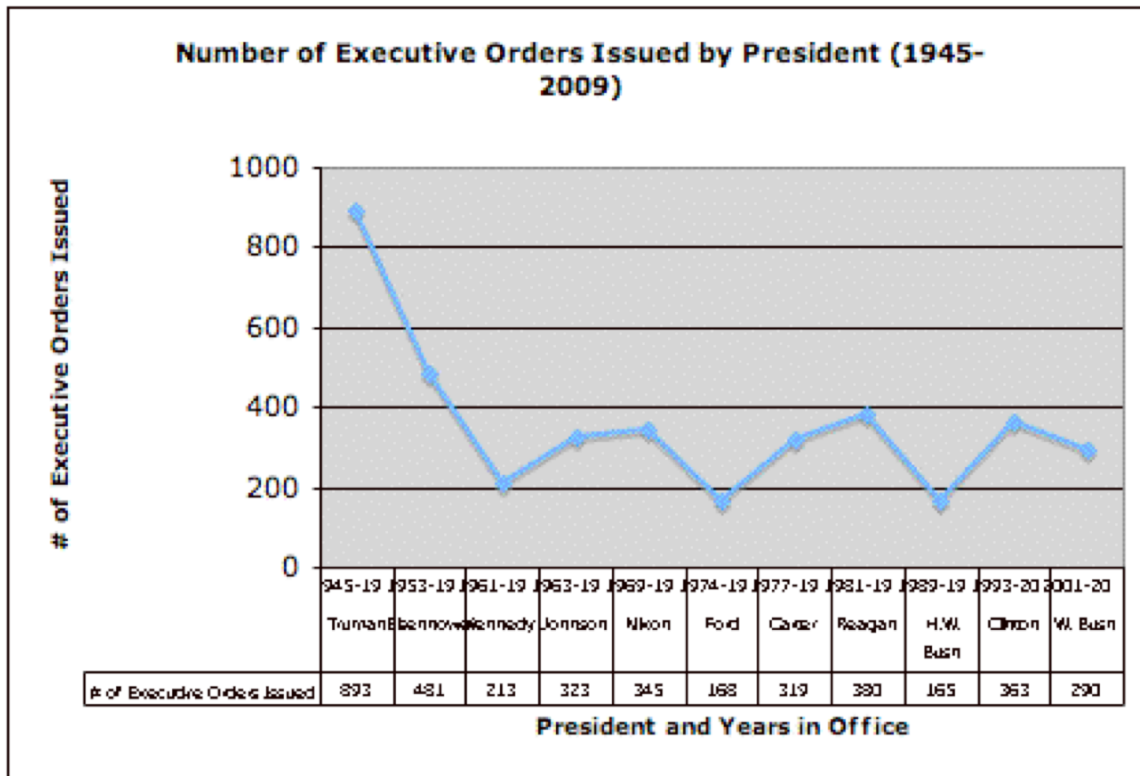
INR	\$100
Treasury	\$100
DOE	\$200
NSA	\$15,000
NRO	\$15,000

JMIP - Joint Military Intelligence Program	\$7,000
NGA	\$2,000
ex-DARP	\$3,000
DIA	\$2,000

TIARA - Tactical Intelligence & Related Activities	\$16,500
Army	\$5,000
Navy	\$3,000
USAF	\$7,000
other	\$1,500
<i>March 2008 guesstimate, in millions</i>	

Source: www.globalsecurity.org

Figure 5- Executive Orders by President



Source: <http://www.archives.gov/federal-register/executive-orders/disposition.html>