University of California, Santa Cruz

32 Years After Orwellian "1984": The Surveillance State and National Security

A Senior Thesis submitted in partial satisfaction of the requirements for the degree of

BACHELORS OF ARTS IN SOCIOLOGY AND LEGAL STUDIES

by

Ean L. Brown

March 2016

Advisor: Professor Hiroshi Fukurai

This work is dedicated to my dad Rex along with my family and friends who inspired me to go the extra mile.

Special thanks to Francesca Guerra of the Sociology Department, Ryan Coonerty of the Legal Studies Department and Margaret Shannon of Long Beach City College for their additional advising and support.

Abstract

This paper examines the recent National Security Agency (NSA) document leak by former NSA contractor Edward Snowden and analyzes select programs (i.e. PRISM, Dishfire, and Fairview) to uncover how the agency has maintained social control in the digital era. Such governmental programs, mining domestic data freely from the world's top technology companies (i.e. Facebook, Google, and Verizon) and listening in on private conversations, ultimately pose a significant threat to the relation of person and government, not to mention social stability as a whole. The paper will also examine the recent government document leak *The Drone Papers* to detail and conceptualize how NSA surveillance programs are used abroad in Afghanistan, Somalia and Yemen. Specifically, this work analyzes how current law is slowly eroding to make room for the ever-increasing surveillance on millions of innocent Americans as well as the changing standard of proof through critical analysis of international law and First and Fourth Amendment Constitutional law. Following a discussion and legal critique of NSA programs, this paper will offer policy recommendations to help mitigate the current issue of mass surveillance.

Key Words: Crime, Standard of Evidence, NSA Surveillance, Extrajudicial Killing, National Security

1. The History of the NSA and its Surveillance Parts:

In the time it takes to read this paper, the United States government will have collected approximately 83 million domestic phone calls. This statistic comes from the 2013 Global Surveillance Disclosure by former National Security Agency (NSA) analyst Edward Snowden[1]. The "Snowden Files", as they have come to be called, detail unprecedented information about the specific programs and practices of the elusive NSA. This leak was so profound that classified documents are still being analyzed and published to the American public. To further our understanding of government surveillance and the notion of national security, a new massive data leak has shed light on the use of predatory drones. *The Drone Papers*, like the 2013 Global Surveillance Disclosure, sheds light on the current heavily debated issue of the use of predatory drones to maintain U.S. national security interests, while showing how the NSA's surveillance programs are used to locate individuals deemed acceptable to kill.

This paper will examine the recent National Security Agency (NSA) document leak by former NSA contractor Edward Snowden and analyze select programs (i.e. PRISM, Dishfire, and Fairview) to uncover how the agency has maintained social control in the digital era. Programs that are able to mine domestic data freely from the world's top technology companies (i.e. Facebook, Google, and Verizon) and listen in on private conversations pose a significant threat to the relation of person and government, not to mention social stability as a whole. I will also examine the recent government document

[1] James Ball, NSA collects millions of text messages daily in 'untargeted' global sweep The Guardian (2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (last visited Oct 19, 2015).

leak *The Drone Papers* to detail and conceptualize how NSA surveillance programs are used abroad in Afghanistan, Somalia and Yemen. The work will specifically analyze how current domestic and international law is slowly eroding to make room for the ever-increasing surveillance on millions of innocent Americans as well as the changing standard of proof as pertaining to the U.S. Constitution.

2. Literature Review

It is necessary to understand and define the above NSA operational units because both separately and in conjunction, they execute many of the data mining programs that have been revealed via the Snowden Files. Also, it should be noted that the NSA is only part of the intelligence community that is charged with collection of electronic data and information. The U.S. intelligence community (IC) is made up of seventeen U.S. government agencies that include the FBI, CIA, and all five branches of the military. What makes the NSA unique is the fact that rather than collecting electronic intelligence in a human aspect, they are focused on digital data such information from social media, bank transactions, and GPS tracking technology that is used to piece together a mosaic of digital patterns that is then used to provide a history and narrative of an individual.

The National Security Agency (NSA) is an institution devoted to the interception and collection of information as it relates to national security. For the purposes of this paper, national security can be defined as the need to protect and secure the nation from foreign and domestic threats. Threats can include any intent to physically harm the nation, such as the attacks on September 11th, 2001, or the ever-increasing threat of cyber attacks on systems the United States relies on to protect our defense and other

infrastructure systems. To put it simply, anybody or anything that poses a threat to the United States is a threat to national security.

The creation of the NSA came as a result of several post-World War II intelligence offices. At the time, the Navy, Army and Air Force all had their own intelligence branches with additional aid from the FBI. To solve the inconsistency and dysfunction between all of the intelligence offices, President Truman ordered that a special committee be formed under the direction of the Secretary of State and Defense to streamline the intelligence process[2]. The Brownnell Committee in June of 1952 made the recommendation that all communication intelligence (COMINT) operations be given to one office under the direct supervision of the Secretary of Defense. Although the committee made specific recommendations regarding the chain of command for the newly conceived agency, the President and National Security Council made changes that placed the Secretary of Defense as an executive agent over the director of the NSA[3]. This in a sense made it possible for the agency to operate with little oversight in order to achieve the mission of gaining intelligence via signal intelligence (SIGINT), which is the collection of communications via electronic radio signals.

Currently, the NSA is still entrusted with the collection of SIGINT. They serve as protector of America's most sensitive national security information and intercept cyber intelligence from foreign threats. To achieve this goal, the agency is divided into three main operational task forces. The first of these is Global Access Operation (GAO), tasked with data collection overseas. Second, is the Special Source Operation (SSO), whose task it is to compile information on domestic threats, whether they are terrorist sleeper cells or

[2] George F. Howe, The Early History of NSA, 11-17 (2007)
[3] Supra Note 2

treasonous citizens. The last operational unit is the Tailored Access Operation (TAO), which is charged with exploitation of computer systems, or to simply put it, hacking. Most of the programs that will be detailed and explained in the following pages are operated under the SSO and TAO[4].

It is important to give attention to the use of the NSA's various programs and how they relate to one another because it is how the government pieces together a story about who you are. Also, these programs and information about them have come out of the Snowden Files released by independent news outlets. There are four logical ways to conceptualize the purpose and use of these programs, which include domestic versus international as well as bulk collection versus targeted collection. I will be focusing on the domestic spectrum, although there are some programs that occupy both realms.

3. Domestic Surveillance Programs

Immediately after September 11, 2001, two main counter terrorism surveillance programs existed: Thinthread and Trailblazer. Thinthread's program contributors, William Binney and Thomas Drake (who would later become whistleblowers), urged that Thinthread was a better solution to Trailblazer because of its streamlined design and programmed anonymity protection for data collected. The only way the program could be used to actively search a target was with the presence of a court warrant. The program collected financial data, GPS data, travel records and web searches[5]. Although Thinthread boasted an unprecedented ability to collect and adapt to new technology, it was ultimately

[4] Laura K. Donohue, Privacy and Surveillance, The Cost of Counterterrorism Power, Politics, and Liberty 182–272, 182-272, http://www.jstor.org/stable/40042805 (last visited Jan 12, 2015).

[5] Joshua Rothman, Takes: The N.S.A.'s Surveillance Programs - The New Yorker, The New Yorker (2013), http://www.newyorker.com/books/double-take/takes-the-n-s-a-s-surveillance-programs (last visited May 4, 2015).

scrapped by the NSA in favor of Trailblazer. Trailblazer did not have the same anonymity protections as Thinthread and therefore was easier to abuse in its ability to actively search and surveil targets.

The first set of NSA programs collected cellular phone data. Data includes: metadata, geo-location, and access to internal hardware such as the microphone or camera. Gilgamesh is an NSA program designed to geo-locate people using a cell phone's SIM card[6]. From there it is possible to track exactly where a suspect or target frequents. Another utilization of this program is for the military's use of predator drones. Cellphone metadata is collected through secret warrants approved under the Foreign Intelligence Surveillance Act by the FISA court that requires cellphone companies such as Verizon to provide the NSA and other intelligence offices with call records inside the U.S. as well as internationally[7]. Metadata essentially includes call time and the number called as well as other information that is not content based. Noseysmurf (also called Trackersmurf and Paranoidsmurf) aims at taking advantage of "leaky" smartphone applications[8]. Most notably the NSA has utilized flaws in the popular smartphone game Angry Birds to access the microphone and tracking location in both Apple and Android phones. Dishfire is a program that is designed to collect text messages from phones all around the world. The NSA partners with GCHQ, its British counterpart, to determine border crossings via cellular tower roaming, financial transactions from credit cards that

---

[6] Glen Greenwald & Jeremy Schahill, The NSA's Secret Role in the U.S. Assassination Program, The Intercept (2014), https://theintercept.com/2014/02/10/the-nsas-secret-role/ (last visited Aug 3, 2015).

[7] James Ball, Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data The Guardian (2014), http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data (last visited Jul 5, 2015).

[8] Supra Note 7

are linked to a user's phone number, as well as metadata and content of text messages[9]. The NSA also has the technology to defeat cellphone encryption through its massive and sophisticated decryption tools enabling them to listen in on phone calls[10].

Along with cell phones, personal computers are the targets of NSA data mining programs. As our use of computers increasingly relies on the internet, the NSA and other intelligence agencies have expanded their technology to meet the internet's growing use. Programs like Happyfoot are used to "piggyback" off of advertisers' tracking of consumers through internet cookies[11]. This allows the NSA to gain insight into an individual's internet surfing habits. Tor, a popular web browser used to anonymize users from the sites they visit, has partially been hacked by the NSA in a program called Egotisticalgoat. At the time of the report in 2013, the agency could only decrypt a small portion of user information, but it can be inferred that their ability to decrypt has developed in the past couple years[12].

4. The Prism Program

---

[9] Jeff Larson, SPY AGENCIES PROBE ANGRY BIRDS AND OTHER APPS FOR PERSONAL DATA PRO PUBLICA (2014), https://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data (last visited Jul 27, 2014).

[10] Craig Timberg & Ashkin Soltani, BY CRACKING OF A5/1 CELLPHONE CODE, NSA HAS CAPABILITY FOR DECODING PRIVATE CONVERSATIONS WASHINGTON POST (2013), https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (last visited Aug 7, 2015).

[11] Ashkin Soltani, Andrea Peterson & Barton Gellman, NSA USES GOOGLE COOKIES TO PINPOINT TARGETS FOR HACKING WASHINGTON POST (2013), https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/ (last visited Aug 8, 2015).

[12] James Ball, Glenn Greenwald & Bruce Schneier, NSA AND GCHQ TARGET TOR NETWORK THAT PROTECTS ANONYMITY OF WEB USERS THE GUARDIAN (2013), http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (last visited Jul 20, 2015).

The NSA is not strictly limited to internet surveillance; they have a dedicated team through the Tailored Access Operation (TAO) that is able to break through the most sophisticated firewalls (Appelbaum, Horchet, Stocker). Most of this hacking is made possible through secret backdoor entrances into software that companies like Microsoft provide the NSA. Although this may seem farfetched or science fiction-like, it is through the most prominent program that this is made possible. The Prism program was first revealed in June of 2013 by Glen Greenwald and Ewen MacAskill who were the two reporters from *The Guardian* who met with Snowden in Hong Kong to retrieve what would later be known as the Snowden Files. Prism is an extensive program that actively mines data from each of the world's nine top technology conglomerates[13]. The most notable companies include: Microsoft, Google, Facebook, YouTube, Skype, and Apple. Through a FISA court order, these companies were compelled to provide the NSA and intelligence community with full access to their servers to provide access to stored records as well as real time updates on a target. According to *The Guardian,* the NSA's use of this program was to circumvent the downfalls of the FISA court when surveillance warrants were not granted[14]. To execute this program, the NSA used the FBI as the server for these orders, which accompanied a gag order, so that the technology companies could not disclose this information to its customers.

---

[13] Glenn Greenwald & Ewen MacAskill, NSA PRISM PROGRAM TAPS IN TO USER DATA OF APPLE, GOOGLE AND OTHERS THE GUARDIAN (2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (last visited Mar 13, 2015).

[14] Nick Hopkins, UK GATHERING SECRET INTELLIGENCE VIA COVERT NSA OPERATION THE GUARDIAN (2013), http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism (last visited Mar 13, 2015).

The Prism program really serves as a sobering revelation to hundreds of millions of Americans because these companies provide us with the digital world that many of us are a part of. Computer users rely on Apple or Windows computers and their accompanying programs in order to complete work- or school-related functions. Similarly, people rely on Google for a convenient search engine to start research or access Gmail to send emails. Social media sites such as Facebook and Instagram encapsulate everything about us from vacation photos to religious viewpoints. All these tools of the twenty-first century are essentially compromised by the government through programs like Prism and its accompanying sister programs that infiltrate our computers and phones.

The sum result of these programs are stored in a massive data trove located in Bluffdale, Utah. From there, the data that is collected by the above programs are able to be searched upon at a moment's notice through the intelligence community's version of a google search engine called ICREACH (Intelligence Community Reach)[15][16]. ICREACH is used by most offices of the intelligence community, including the FBI and DEA, and contains data on foreigners as well as the ability to search state and national databases to collect information on a target. This information, accessed through ICREACH that contains data obtained through secret NSA programs, is then used to compile a biography of who you are through a process called "linkability," a term coined by Jacob Appelbaum. Keep in mind that these tools are meant for the prevention of terrorist

---

[15] Ryan Gallagher, HOW THE NSA BUILT ITS OWN SECRET GOOGLE THE INTERCEPT (2014), https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/ (last visited Dec 10, 2014).

[16] Ryan Gallagher, OBAMA FACES CALLS TO REFORM REAGAN-ERA MASS SURVEILLANCE ORDER THE INTERCEPT (2014), https://theintercept.com/2014/09/02/obama-12333-surveillance-nsa-rights-groups-letter/ (last visited Dec 10, 2014).

attacks, in turn protecting American life and property, but what has been largely gathered since the existence of these programs was made public is that American citizens' data and personal information is being gathered illegally[17].

5. The Drone Papers

On October 15, 2015, *The Intercept* released a collection of documents collected from an unnamed whistleblower source. These documents provide insight into the use of predatory drones on targets abroad, but it also details how some of the above NSA programs are used to find and surveil individuals. The exposé, as outlined by *The Intercept*, details how the U.S. government used signal intelligence (SIGINT), which it borrowed from the NSA, to geo-locate individuals suspected of terrorist ties and assassinate them in areas where war has not been declared. Along with the "Kill Chain" article, *The Intercept* also reveals that the U.S. government is fully aware that the current utilization of predatory drones yields an intolerably high civilian casualty rate. *The Drone Papers*, as they have come to be called, not only prove that the U.S. under the Obama administration takes out its targets using the kill-and-capture method, but also grimly reveal how these individuals are targeted on the bases of precarious data used as incriminating evidence.

In May 2013, The White House released a fact sheet on the policy standards and procedures for the use of force in counterterrorism operations outside the U.S. and areas of active hostilities. In the opening of this document, The White House assures that the President (Obama) "made clear that, in carrying on this fight [against Al-Qaida and its associates], we will uphold our laws and values and will share as much information as

[17] A full list of programs can be seen on appendix "A". Available at: https://projects.propublica.org/nsa-grid/

possible with the American people and the Congress, consistent with our national security needs and the proper functioning of the Executive Branch"[18]. Although this statement seems to contain the rhetoric of a transparent legally binding promise from President Obama, it is clear that these words only mean that the U.S. will uphold its own laws at it sees fit, with no regard to international law or diplomacy. Also, this initial statement imposes a moral standard by saying that the values and laws of the U.S. will seek international and global justice for those suspected of terrorist activities outside of U.S. law. Another issue in this statement is that it is made clear how much power the executive branch really has in matters of national security.

The document goes on to state that the government has a preference of capturing those suspected of terrorist activity, so that they can be (under U.S. law) lawfully captured and questioned to mitigate any further terrorist plots. As we will discuss shortly, the U.S. rarely upholds this policy of capture versus kill. In the event that the U.S. does utilize lethal force, five criteria points must be met before such action is taken[19]:

1. Near certainty that the terrorist target is present;
2. Near certainty that non-combatants will not be injured or killed;
3. An assessment that capture is not feasible at the time of the operation;
4. An assessment that the relevant governmental authorities in the country where the action is contemplated cannot or will not effectively address the threat to U.S. persons, and;

[18] Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities, THE WHITE HOUSE (2013), https://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism (last visited Jan 22, 2016).

[19] Supra Note 17

5. An assessment that no other reasonable alternatives exist to address the threat to U.S. persons.

As drones have been used extensively outside active conflict areas where US military forces are not physically present, it is helpful and important to use the standards offered in the above document to critically analyze U.S. action, as made evident through *The Drone Papers*.

Predatory drones have become a key tool for seeking U.S. combatants under the Obama administration. *The Guardian* has reported that the Washington currently has 678 various drones in its service[20]. Although the unmanned areal vehicles (commonly referred to as drones) have become an important resource to the U.S. and other countries, they have in some cases become a tool for extrajudicial killings in lieu of putting boots on the ground in areas where the U.S. does not have official military operations. Drone operations are typically carried out by drone pilots in America, halfway around the world from where the mission is taking place. The missions are operated under either the CIA or the U.S. military's Joint Special Operations Command (JSOC) with strikes largely taking place in Yemen, Somalia and Afghanistan.

Although drones are able to spend long periods of time in the air surveilling potential targets, the CIA and JSOC borrow geo-location and other tracking technology from the NSA. It is through the GILGAMESH program that geo-locates a cellphone SIM card that the U.S. was able to carry out an attack on a man named Bilal el-Berjawi,

[20] Simon Rogers, DRONES BY COUNTRY: WHO HAS ALL THE UAVS? VISUALIZED THE GUARDIAN (2012), http://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country (last visited Dec 22, 2015).

suspected of terrorist activity in 2012[21]. Prior to the strike, el-Berjawi was on the phone with his wife who had just given birth and as a slide obtained by the source notes, he was under surveillance via cell phone geo-location for quite some time.

The U.S. government has a long history with using euphemisms to cover up conduct that would seem too unsettling for the American public as well as those carrying out orders, and killings via drones are no different. When drones fire upon, and kill the intended subject, it is called a "jackpot"; such was the case with el-Berjawi[22]. *The Drone Papers* yield not only these seemingly playful euphemisms, but also the shocking meaning behind them. When an individual is chosen for consideration of a drone strike, they and their information are organized on what's called a "baseball card". This card is essentially a report on the individual, affiliates and other "incriminating evidence" that is sent up the kill chain for authorization of a sixty-day authorization to kill[23]. If a baseball card is approved for a kill, the individual is targeted utilizing all intelligence resources at the government's disposal, including NSA surveillance tools.

The assassination of el-Berjawi outlines how this rhetoric is used in a real scenario. When el-Berjawi was selected, he was placed on a baseball card in a group full of others for selection. After his selection, he became the "objective" of a drone operator to find, fix and finish. When the CIA was able to locate and track him, they used a predatory drone to fire a Hellfire missile aimed at el-Berjawi, but also his cellphone's

---

[21] Josh Begley, THE DRONE PAPERS: A VISUAL GLOSSARY THE INTERCEPT (2015), https://theintercept.com/drone-papers/a-visual-glossary/ (last visited Oct 15, 2015).
[22] Supra Note 20
[23] Cora Currier, THE KILL CHAIN: THE LETHAL BUREAUCRACY BEHIND OBAMA'S DRONE WAR THE INTERCEPT (2015), https://theintercept.com/drone-papers/the-kill-chain/ (last visited Oct 15, 2015).

SIM card. When this scenario occurs, it is referred to as a "touchdown"[24]. After the killing of el-Berjawi, the rhetorical process captures him as another statistic, rendered as an enemy killed in action (EKIA). The mislabeling of people as EKIAs, however, reveals that using drones as assassination tools is as imprecise as it is unlawful.

Even though the CIA and other military units have unprecedented access to technological tools to aid their quest to find, fix and finish, predatory drones yield a high error rate when targeting and killing a suspected individual. According to the information obtained by *The Intercept*, over a five-month period and 155 people killed, only nineteen "jackpots" were actually achieved[2526]. Statistically nine out of ten people killed in these drone strikes were not the intended targets, meaning they were most likely civilians. Although these individuals are innocent civilians, they are still catalogued as enemy combatants by the U.S.

The loss of innocent lives, as well as the rhetorical masking of this grim fact, underscores how problematic it is to use drones and other NSA programs to carry out these extrajudicial killings. Apparently, this rate of failure has been an acceptable loss for America's quest to squash out the never-ending War on Terror. Although these are extreme examples of Washington's utilization of NSA programs, it cannot be ignored that this issue has far surpassed the surveillance of the American population as exposed by Edward Snowden in 2013.

6. The International Criminal Court: An Analysis of *The Drone Papers*

[24] Supra Note 20
[25] Statistical graph on drone error rate is available on appendix "B". Available at: https://theintercept.com/drone-papers/a-visual-glossary/
[26] Supra Note 20

In light of the findings in *The Drone Papers*, it may be appropriate to begin a discussion in the international arena through the policy of the International Criminal Court (ICC). Although the U.S. and most of its allies are not participatory members of the ICC, it is necessary to analyze and conceptualize these actions by the U.S. in the lens of the objective global citizen. As of now there hasn't been much conversation on the use of predatory drones that are used in conjunction with NSA surveillance technology except for a few formal complaints to the ICC by humanitarian rights groups as well as families of the victims. Naturally these complaints have not received mainstream national attention and have fallen on deaf ears.

Along with the issue of the U.S. not being a member of the court, additional challenges arise when the ICC decides to take legal action. Largely, the court defers to the states making the claim to settle amongst themselves prior to elevating the action in question to international legal proceedings. This is known as complimentary, in that if the above criteria are not met, then the court may impose its legal authority[27]. If the nation is unable to hear and effectively try the conflict, the court will utilize the gravity threshold to determine international importance under the two levels of criteria that consist of international social outcry and the issue of whether or not this is a systematic or large scale event[28]. Upon satisfying these two prerequisites, the court can determine what, if any, four prosecutorial jurisdictions it can pursue.

7. ICC Jurisdiction

[27] Lailey Rezai, *U.S. Drone Policy and the International Criminal Court,* AMICC, July 22, 2014

[28] Supra Note 25

Currently the ICC operates under four subject matter jurisdictions that are set forth by the Rome Statute as adopted in 2002. The four prosecutorial jurisdictions include: 1) Genocide 2) Crimes Against Humanity 3) War Crimes and 4) Crimes of Aggression. For the purposes of this paper, I will be analyzing Washington's culpability for all these except genocide[29].

8. Crimes Against Humanity

Under crimes against humanity, the ICC investigates incidents such as murder, imprisonment and deprivation of fundamental civil liberties. As noted by AMICC, the court will only address a drone case if the attack on civilians is widespread and systematic[30]. What we have learned from the recent leak in *The Drone Papers* tells us that there have been gross amounts of civilian casualties (referred to as "enemies killed in action") and that officials have cited the many issues and problems associated with the uncertainty of predatory drone use[31]. However, and of course, with any good lawyer this fact can be argued for or against. To help navigate through U.S. culpability in crimes against humanities, AMICC cites a 2009 drone strike at the funeral of a high-ranking Taliban official as carried out by the CIA. The result of this attack was 83 individuals killed, many of whom were women and children while the intended target escaped with no injury[32].

Although this instance and others shed light on a troubling practice, the court will only find a nation guilty if: 1) The perpetrator has killed more than one person; 2) his conduct was committed as part of a widespread or systematic attack directed against a

[29] International Criminal Court, Rome Statute of the International Criminal Court, 2011
[30] Supra Note 25
[31] Supra Note 20
[32] Supra Note 25

civilian population; and 3) the perpetrator knew that the conduct was part of a widespread or systematic attach against a civilian population as analyzed through the Rome Statute[33]. Arguably Washington is indeed guilty under the three-pronged test as set forth by the court. Attacks such as the 2009 funeral strike or the attack that killed el-Berjawi in concert with the top secret files obtained by *The Intercept* implicate the US with a burden of proof that can hardly be declared as inadmissible.

9. War Crimes

To determine guilt under war crimes, it is first essential to determine whether or not the US is involved in an international armed conflict. Along with this fundamental question, the court would look at whether or not there is gravity to the accusation and if it indeed poses a risk to the international community. Returning to the White House's document on policies and procedures for use of force in counter terrorism operations, it can be maintained that the U.S. has acted outside the legal scope that protects it from war crimes accusations. War crimes for which the ICC would prosecute include murder, cruel treatment and attacking civilians. Undoubtedly, the U.S. is involved with all three of these violations under war crimes.

With the staggering statistical analysis of unintended individuals killed by drones as obtained by *The Intercept*, murder and the attacking of civilians become very weighted in light of the gravity threshold. The court would surely refrain from taking legal action if civilian deaths are accidental in nature; however, as detailed above, this is clearly not the case. At a civilian kill rate of ninety percent, this is undoubtedly of grave international

[33] Supra Note 27

concern[34]. Also as noted by the AMICC, the U.S. engages in what is known as double tapping[35]. This practice is carried out by firing an initial ballistic missile at a target followed by another attack after a short period of time. Such strategic firing is problematic because it notoriously kills first responders who are attempting to care for individuals injured in the drone strike, thereby further complicating future decisions on whether or not care should be rendered[36]. Attacking or killing medical personnel is illegal under customary international humanitarian law along with rules stipulated by the ICC.

10. Crimes of Aggression

Crimes of aggression have always been one of the four crimes that the ICC has jurisdiction over; however, the definition of crimes of aggression has been debated until recently in 2010. The Nuremburg Trial was the first court to prosecute for crimes against speech, which is the equivalent of the present day crimes of aggression[37]. Because states and the ICC have had little success trying and let alone agreeing on crimes of aggression, it is necessary to clearly define it in this text as written by the ICC. The current definition of crimes against humanity is "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations"[38]. According

[34] Supra Note 20
[35] Supra Note 25
[36] Supra Note 25
[37] Ayla Prentice-Cuntz & Katie Flannery, ON THE CRIME OF AGGRESSION AND THE ICC IN A QUASI-WESTPHALIAN SYSTEM INTERNATIONAL JUSTICE PROJECT (2014), http://www.internationaljusticeproject.com/on-the-crime-of-aggression-and-the-icc-in-a-quasi-westphalian-system/ (last visited Feb 12, 2016).
[38] Supra Note 27

to the court, the following constitute as an act of aggression[39]:

> (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
>
> (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
>
> (c) The blockade of the ports or coasts of a State by the armed forces of another State;
>
> (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
>
> (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
>
> (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
>
> (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

Washington's use of predatory drones undoubtedly meets the criteria set forth by the ICC. Drones operate out of US military bases in Afghanistan and North-Eastern Africa, which means there is unprecedented military access to regions that are vulnerable compared to the massive military industrial complex that is the U.S.[40]. Although it can be maintained that predatory drones only seek out alleged terrorist extremists, it cannot be forgotten that dozens of official reports cite the inaccuracy of these strikes that all too often kill civilians – women and children. Such unwarranted death is the real issue that casts the use of drones as crimes of aggression. The extrajudicial killings of the innocent that are the victims in Washington's quest to extinguish terror are clear acts of aggression

[39] Supra Note 27
[40] Supra Note 20

under the principle of negligence. How can a policy where the end result is a certain loss of life be so negligent and ruthless in its practice?

11. ICC: Concluding Remarks

The question that is being posed above is at the root of the discussion of drone strikes and international law as stipulated under the ICC. My methodology and discussion of the extreme effects of NSA surveillance programs (predatory drones) in relation to the International Criminal Court is only meant to expose how the government's actions would be perceived through the international legal lens in an ideal world where all states would adhere to global justice. It is not my intention to oversimplify or ignore the complexities of international law. However, these fundamental questions are too often overlooked and ignored by Americans as well as other first world nations.

The remainder of this paper will return to the NSA and domestic policy as analyzed through a literal-textualist view of constitutional protections and social implications to the American society.

12. Domestic Policy

There is a fundamental issue in the American government's policy regarding utilization of NSA surveillance technology and the use of predatory drones. The issue at its core is one of policy and legal misguidance. The questions that should be asked are how much of the intelligence gathered via NSA surveillance is based in reality along with questions of legality and how we have gotten to this point. Jacob Appelbaum, a cyber security expert, cites that the programs used by the NSA that track location, financial patterns, and digital communication are used in concert to build a story of a subject called

linkability[41]. This concept essentially proves guilt based on association and possible coincidence. Also, this practice by nature has many policy flaws and imperfections as evident in the thousands of people detained in the name of national security or drone strikes that have killed an estimated five thousand people[42].

13. A Political History of Control: Information as a Means of Power and Control

Of course data as provided by Edward Snowden is still being analyzed and released, but it is apparent as to what extent we, the American people and global community, are being surveilled upon. As Glen Greenwald noted when first meeting with Snowden to obtain the leaked information, this is something many people feared and subconsciously knew was happening; however, these revelations make it blatantly and shockingly true[43]. Programs like PRISM and the various other invasive programs shed light on what should be thought about as a form of global digital incarceration on thought, speech and action.

Jeremy Bentham famously conceptualized the panopticon in the late eighteenth century. The architectural prison concept featured a central guard station in the middle of the complex surrounded by cells. This design was never completely built to Bentham's specifications; however, what the design allowed was for the guard to view a high volume of inmates directly from a central vantage point. Inmates would not know when or to the extent they were being surveilled, thereby making the inmate police his or her

[41] Laura Poitras, Citizenfour (2014).
[42] Jameel Jaffer, DRONE DISCLOSURES, OFFICIAL AND NOT AMERICAN CIVIL LIBERTIES UNION (2015), https://www.aclu.org/blog/speak-freely/drone-disclosures-official-and-not (last visited Jan 7, 2016).
[43] Supra Note 39

own actions[44]. Michel Foucault expanded this idea in his 1975 book *Discipline and Punish* by illustrating how disciplinary societies can use this model in the social sense to subjugate their citizens[45]. Expanding further on this notion, Neil Richards cites the recent privacy revelations as the Electric Panopticon where the notion of the panopticon expands and further restricts civil liberties of speech, whereby individuality and diversity are hindered by a self governing[46]. Richards' take on surveillance is a crucial element that is not fully being explored by many in academia and in mainstream media coverage.

As discussed, the inaccuracy of information is quite dangerous for individuals being targeted by government but also for the rest of democratic society in that it decimates any dissent on political and social commentary that goes against hegemonic ideals of the U.S. government. Intelligence information that is problematic in its nature yields possible repeats in recent history. This can be the possibility of institutional prejudice through legal policy that was witnessed in World War II by means of Japanese internment camps, or even a more recent example of the weapons of mass destruction (WMD) that sparked national fear and fueled the invasion in Iraq. Both examples provide a window into American history where it was dangerous to be a part of a specific ethnic group due to association of being an enemy of the state, or going against the American hysteria in the wake of September 11, 2001. Also, these instances are prime examples of the dangers that come with inaccurate intelligence and the real world effects it has had.

14. House of Un-American Activities: Social Hysteria

---

[44] Bentham's Panopticon can be seen on appendix "C". Available at: http://www.wordsinspace.net

[45] Michel Foucault, Discipline and Punish: The Birth of Prisons (1975).

[46] Neil Richards, The Electronic Panopticon, The Chronicle of Higher Education (2015).

Now that a historical component on inaccurate or incomplete data has been reviewed it is now useful to dissect a historical instance of social control. In the midst of the Cold War and the seemingly impending doom that was communism, the U.S. was on a quest to seek individuals who were thought to be communist or fascist. In 1938 the House Committee on Un-American Activities (HUAC), which was a select group from the House of Representatives, was charged with finding such individuals. The HUAC was able to subpoena individuals ranging from communist sympathizers to those with political views of the far left. What this committee turned into, however, was a vicious government investigatory tool that economically and socially ruined individuals or imprisoned those who were accused and declared guilty of such crimes. Of course the HUAC lost credibility and relevance in the 1960's due to its claims against prominent Americans[47].

The HUAC and previously discussed American instances hold great relevance today with knowledge of government surveillance and extrajudicial killing of individuals. Washington is essentially creating the new generation of the HUAC in that by searching for a given topic or associating with another, you are guilty until proven innocent. By use of linkability, millions of Americans are being surveilled by holding opposing hegemonic ideals. An unknown number of Americans are currently under surveillance because of religious beliefs and ethnicity. Also, it goes without saying that when the government uses inaccurate dragnet surveillance, it harms us all and undermines what being an American is about.

15. First Amendment Legal Analysis

[47] The House Committee on Un-American Activities, Robert E. Carr (1955).

It is important to talk about how First Amendment issues as granted in the U.S. Constitution are also threatened by the NSA in the name of national security. After all, the First Amendment is a fundamental component that makes up the idea of a free world[48]. In comparison with other democratic first world nations, America has the most liberal and non-constricting protected speech afforded to its citizens. Freedom of speech proves its social worth through fluid transmission of ideas and as a tool for the people to criticize their government[49]. To analyze NSA surveillance in relation to the First Amendment, I will provide the opening to the First Amendment, which reads[50]:

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

When the revelations of widespread government surveillance became public knowledge, these constitutional protections that Americans defend with such vigor were naturally infringed upon. The very notion that the government is able to listen in on private conversations between two parties or collect google searches is very troubling because such secretive practices infringe on free speech. However troubling this encroachment may be, the United Stated government, including the judiciary branch, has continually scaled back the protections of the First Amendment in the wake of national security threats such as both World Wars and September 11, 2001. In the 1919 Supreme Court case of Schneck v. United States, the court ruled that the actions of Schneck and

---

[48] Daniel A. Farber, The First Amendment (2010).
[49] Supra Note 45
[50] First Amendment, LII / LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/constitution/first_amendment (last visited Feb 3, 2016).

others by urging for a peaceful petition of the draft was not protected under the Constitution[51]. Similarly, in United Stated v. O'Brien (1968), the courts decided that burning a draft card was not protected by the First Amendment even though it held a visceral symbolic meaning for many at the time[52]. Both of these decisions were delivered at a time of global conflict.

Much of what the government and intelligence agencies aim to prevent is a violent attack on their citizens. Surveillance of citizens by means of gathering phone calls, intercepting emails and circumventing social media has been the tool of choice post September 11th. However, these actions themselves are fundamental breaches of First Amendment protections under the Supreme Court's ruling in Brandenburg v. Ohio (1969). In this case, the state of Ohio arrested Brandenburg under a state law that made any speech that promoted crime, violence or terrorism illegal[53]. The court sided with Brandenburg and established a two-prong test to determine whether constitutional protection applies if inflammatory language is used to intentionally incite violence. Ultimately, the test stipulated that speech can be prohibited if it will incite imminent lawless action and it is likely to incite or produce such action[54].

Brandenburg can be applied to freedom of speech via public talks and social media. It protects radical speech that criticizes our government as well as hate speech (as is the case in Brandenburg). This case and other previously discussed cases affirm

---

[51] *Schenck v. United States*, Oyez, https://www.oyez.org/cases/1900-1940/249us47 (last visited Feb 20, 2016).
[52] *United States v. O'Brien*, Oyez, https://www.oyez.org/cases/1967/232 (last visited Feb 20, 2016).
[53] *Brandenburg v. Ohio*, Oyez, https://www.oyez.org/cases/1968/492 (last visited Feb 20, 2016).
[54] Supra Note 50

important components in First Amendment protections for American citizens, who rely on this amendment's tenets in the marketplace of ideas to fundamentally support democracy.

16. Fourth Amendment Legal Analysis

Current practices and policies of the Bush and Obama administrations have provided the state with a means to bypass protections granted by the Constitution and Bill of Rights. Before I proceed with conversation of the Fourth Amendment in relation to government surveillance and national security, it is necessary to provide an excerpt from the Constitution's Fourth Amendment[55]:

"[t]he 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."

17. Substantive Grounds of NSA Surveillance

In Arizona v Evans, the Arizona Supreme Court saw the danger to civil liberties posed by law enforcement's increasing use of computers[56]. The case itself reveals that during a traffic stop a Phoenix police officer searched Isaac Evans' license to find that there was an outstanding warrant for his arrest. What the officer didn't know was that Evans' warrant was cleared days before, but the information was not updated due to negligence of a court clerk. Upon the search of Evans' vehicle, the officer found marijuana. The Supreme Court ended up overruling the case in favor of Arizona;

---

[55] Fourth Amendment, LII / LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/fourth_amendment (last visited Feb 7, 2016).

[56] *Arizona v. Evans*, Oyez, https://www.oyez.org/cases/1994/93-1660 (last visited Feb 20, 2016).

however, this case brings up questions of Fourth Amendment rights in regards to technology. Law enforcement in this case used (unknowingly) inaccurate information in the arrest of Evans, and in doing so, they discovered evidence of another crime.

Although the case was not ruled in favor of Evans, there is another important concept to be drawn from this case. The exclusionary rule is a Fourth Amendment protection that is in place to negate evidence unreasonably obtained by law enforcement agencies as held in Map v Ohio[57]. However, this rule does not apply to evidence gathered from a warrant that turns out to be invalid but executed with reason[58]. Although the Arizona Supreme Court's ruling was overturned by the Supreme Court, they foresaw a future in which government as a whole would become increasingly reliant on computers in relation to law enforcement. The court recognized a "potential for Orwellian mischief" in years to come, as stated in the opinion[59].

Undoubtedly the concept of Arizona v Evans holds extreme relevance today. New technology offers society greater possibility to expand knowledge and ideas. Conversely, technology gives way to a greater susceptibility of (t)error, both on the side of the user and machine. What should be greatly considered is how this surveillance and tracking through linkability will become a part of an individual's permanent digital record. This idea greatly parallels NSA surveillance and its utilization through predatory drones. Substantiated evidence is undoubtedly negated when analyzing the ISR's Task Force

[57] *Mapp v. Ohio*, Oyez, https://www.oyez.org/cases/1960/236 (last visited Mar 20, 2016).
[58] Exclusionary Rule, LII / LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/exclusionary_rule (last visited Feb 8, 2016).
[59] Arizona v. Evans, 514 U.S. 1 (1995)., ARIZONA V. EVANS, 514 U.S. 1 (1995). (1995), https://www.law.cornell.edu/supct/html/93-1660.zd1.html (last visited Feb 8, 2016).

2013 publication that cites the erroneous use of predatory drones[60]. Errors cited include limited surveillance time, which severely limits the context and assurance needed to make a decision to kill an enemy combatant. The internal publication also cites that there is inaccurate or incomplete information and a general lack of resources. These findings from the U.S. government woefully contradict what President Obama has hailed to be a legally sound and invaluable resource to the ongoing War on Terror.

Since Arizona v Evans, databases have only grown in size and sophistication. Not only have the NSA and other government agencies been quick to utilize the power they offer, but private third-party enterprises have started to use this technological behemoth too. For example, it has since been discovered that auto insurance companies are looking to social media sites such as Facebook and Twitter to determine your eligibility for auto insurance and rates[61]. This disturbing new business practice is easily executed by looking at information you willingly provide and by analyzing your friends. What this essentially does is dictate what your rate will be by running a cost benefit analysis on who you appear to be in conjunction with driving records. Auto insurance companies are among the many industries that are now beginning to utilize social media platforms to make judgments on individuals.

18. Privacy and Seizure of Information

---

[60] Small Footprint Operations 2/13, THE INTERCEPT (2015), https://theintercept.com/document/2015/10/14/small-footprint-operations-2-13/#page-6 (last visited Oct 15, 2015).

[61] Brandon Mercer, INSURANCES COMPANIES TO USE FACEBOOK, TWITTER SOCIAL MEDIA PROFILES TO SET RATES CBS SAN FRANCISCO (2015), http://sanfrancisco.cbslocal.com/2015/04/24/insurances-companies-to-use-facebook-twitter-social-media-profiles-to-set-rates/ (last visited Mar 11, 2016).

As noted in programs such as the notorious PRISM program -- which actively collects data from Google, Facebook and Skype -- our Fourth Amendment rights are indeed infringed upon by our own government[62]. As it should be noted, the United States Supreme Court has always been slow to adjust to new technology. Olmstead v. United States (1928) held that wiretapping a phone in a person's private business was not considered a "search" within the meaning of the Fourth Amendment[63]. Even though by today's standards most would consider a phone conversation in nonpublic space to be private, the court did not. Currently, we find ourselves in the same predicament in regards to the internet with all the services, means of communication and informational power it grants us. Twenty-five years ago very few could imagine the awesome tools that the internet and computer have become, and the courts are no different. In 1967 when Katz v. United States was presented to the court, the similar issue of phone tapping was in question again[64]. Katz, who had been suspected of illegal gambling, was arrested after using a pay phone (in an enclosed booth) to broker a deal. This time the court cited that individuals do have a reasonable expectation of privacy when using a pay phone or a phone in the privacy of an individual's privately owned space, except in instances where a justified and legally sound warrant is present[65].

Katz became one of the first instances where the court outlined a middle ground for privacy along with citing the increased social role the telephone plays in society. Justice Stewart in his concurrence wrote that if an individual occupies (in this case) a

---

[62] Supra Note 13
[63] Laurence Tribe & Joshua Matz, Uncertain Justice: The Roberts Court and the Constitution (2014).
[64] *Katz v. United States*, Oyez, https://www.oyez.org/cases/1967/35 (last visited Mar 13, 2016).
[65] Supra Note 60

phone booth, he is "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world"[66]. Also concurring, Justice Harlan framed a two-part test under the Fourth Amendment, citing that the Fourth Amendment is triggered when a person has an actual expectation of privacy and society is prepared to view that expectation as reasonable[67]. This case and the previously cited cases underscore fundamental privacy expectations that should be recognized and applied when the government attempts to surveil its own citizen. This is an overarching idea on constitutional rights as afforded by the Fourth Amendment because naturally sensitive nuance exists when credible and ethical national security is weighed.

Speaking on society and technology, it is imperative that third party technological services such as Facebook and Gmail be scrutinized. When we use these services often times a user terms of agreement are accepted by the user in order to use the service. These agreements vary and fall outside of the cases as previously described because they are offered by a private company and not the government. Supreme Court case Smith v. Maryland (1979) brought the question of whether or not the search "pen register" (used to record numbers in pay phones) qualified as an infringement of rights under the Fourth Amendment[68]. The court used what would be known as the third-party doctrine to state that we lose any reasonable expectation of privacy when we have provided the information to someone else[69]. This concept could easily be translated to cases of public and searchable information via platforms like Google.

---

[66] Supra Note 60
[67] Supra Note 60
[68] *Smith v. Maryland*, Oyez, https://www.oyez.org/cases/1978/78-5374 (last visited Mar 13, 2016).
[69] Supra Note 63

Both Katz and Smith seem contradictory of one another and place significant responsibility on the court to distinguish between what should be considered private. A decision on privacy and reasonable searches relies on social meaning of the technology in which the search yields evidence at the time of a given case. An important consideration for the courts would be to expand the legal definition of "papers" as cited in the Fourth Amendment. The term "papers" is a fundamental concept in the notion of privacy in the digital age. "Papers" today translates into an array of First Amendment activity that we all engage in on a daily basis and should be protected under a concept of reasonable privacy under the Fourth Amendment.

Nonetheless, it is imperative that the courts intervene in the issue over digital and personal privacy and serve as a watchdog for the government. The Constitution is a living and breathing document that needs to maintain the protections it grants to the American people. Also, Americans, along with the judiciary, need to be cautious in how privacy is handled in relation to third-party technology services. Large social media companies thrive by having a large user base that expands and grows their business when they obtain smaller companies, as Facebook did with Instagram, WhatsApp and Moves[70]. Such a familiar means of business expansion would be undermined, and customers and capital would likely be lost, if users did not trust these services. As noted in PRISM and various court orders issued by FISA, these terms of agreement are often voided in the name of national security. Not only is this an issue of privacy for the American but also corporations that are undermined by predatory surveillance as imposed by Washington. It would be wise for American-based companies to stand up for constitutional rights like

[70] Facebook, THE FACEBOOK COMPANIES, https://www.facebook.com/help/111814505650678 (last visited Mar 2, 2016).

Apple recently did in denying the FBI a program to allow law enforcement to hack the phones of suspects[71].

19. The Patriot Act and FISA

When looking at current government surveillance, it is important to note that we too are in a state of global conflict. A little over a month after the attack on the Twin Towers and Pentagon, President Bush signed the U.S. Patriot Act into law on October 26, 2001. This law, despite the revisions and expansions made to it, is widely seen as one of the greatest losses of civil liberties in American history. The Patriot Act is based on older laws such as the Espionage Act of 1917 and enhanced by executive action such as Presidential Directive 20, which integrates cyber tools of the NSA with National Security, in short creating what Snowden disclosed in 2013[72]. The Patriot Act is also responsible for enhancing power to the Foreign Intelligence Surveillance Act (FISA) court under section 702 from the previous 1978 FISA legislation[73]. The U.S. Patriot Act, along with other secretive executive action, has created a historical reoccurrence in what is considered free and safe speech as well as a change in the standard of proof -- all in the name of national security.

The FISA courts bring up a sticky debate regarding their relevance to law and society because they are charged with balancing civil liberties against national security. There is absolutely a need for a specialized court to judicially review the intelligence

---

[71] Customer Letter - Apple, APPLE (2016), http://www.apple.com/customer-letter/ (last visited Feb 16, 2016).

[72] Brett Burney, The Patriot Act, American Bar Association (2007).

[73] Dia Kayyali, THE WAY THE NSA USES SECTION 702 IS DEEPLY TROUBLING. HERE'S WHY. ELECTRONIC FRONTIER FOUNDATION (2014), https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why (last visited Mar 3, 2016).

communities' requests for various warrants due to the sensitive nature of national security. As the Brennan Center for Justice concluded in a recent report is that is mission of balance has eroded after September 11th and the signing of the Patriot Act into law[74]. By enhancing the privileges of the intelligence community, the court is working with one hand tied behind its back due to insufficient security clearance that supersedes the FISA court's ability to have the full context of a case. Often times the court will only receive a document of general procedures of how the NSA will decide on whom they can eavesdrop on[75]. Another huge issue that the congressional committee of intelligence, that is supposed to serve as a watchdog for FISA, only receives the number of cases the court sees in a year, not the number of warrants approved or context. In reality, congress has no oversight, while the FISA court has slight informative context on who the NSA is surveilling. Only the executive and few advisors are purview as to the oversight of the NSA, making the agency their premier form of intelligence and social control.

20. Social Implications of Government Surveillance

The social implications of widespread government surveillance are of a serious nature. Besides the infringement on civil liberties, there is a loss of anonymity that individuals feel not only because of surveillance programs like those of the NSA and advancements in technology. As Laura Donohue cites, the greatest impact of surveillance in the social sphere is the psychological effect manifested in an atmosphere of

---

[74] Elizabeth Goitein & Faiza Patel, WHAT WENT WRONG WITH THE FISA COURT | BRENNAN CENTER FOR JUSTICE WHAT WENT WRONG WITH THE FISA COURT | BRENNAN CENTER FOR JUSTICE (2015), https://www.brennancenter.org/publication/what-went-wrong-fisa-court (last visited Mar 3, 2016).

[75] Glenn Greenwald, FISA COURT OVERSIGHT: A LOOK INSIDE A SECRET AND EMPTY PROCESS | GLENN GREENWALD THE GUARDIAN (2013), http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy (last visited Mar 3, 2016).

suspicion[76]. Such pervasive national suspicion echoes Bentham and Foucault's theories, as some ethnic or religious minority groups essentially experience a social panopticon when cast into the atmosphere of suspicion every time they enter an airport.

A techno-driven panopticon exacerbates the problem of profiling in America. According to various reports and another from the FBI during 2002 and 2005, individuals of Middle Eastern ethnicities committed less than ninety percent of terror attacks[77]. Government surveillance, along with media and political rhetoric, has essentially created a propaganda of fear in the American and global psyche. With this perpetual fear, Washington has widened social inequality, with some fearing particular ethnicities and religions, while those who are unfairly demonized anxiously fear not only how law enforcement will view them, but also whether or not they are being actively spied on by the U.S. government.

Besides straining racial and international relations, government surveillance has socioeconomic ramifications as well, in that it curtails our national and global development and growth. We all have done things we regret and want to conceal; however, most of these mistakes do not warrant scrutiny by the government[78]. Privacy in regards to individual interaction with one another should be afforded and seen as social policy and forgiveness. As Laurence Tribe notes, if our everyday action is recorded,

[76] Supra Note 4
[77] Terrorism 2002-2005, FBI (2010), https://www.fbi.gov/stats-services/publications/terrorism-2002-2005/terror02_05#terror_05sum (last visited Mar 3, 2016).
[78] Supra Note 60

innovation suffers[79]. Although privacy is not explicitly granted in the constitution, it is a shield of our other rights that include religion and speech.

21. Policy Reform

Undoubtedly, to prohibit mass surveillance on American citizens, we need to reform through legislation and restructuring of the intelligence community to more justly control how information is used and gathered. Since Edward Snowden's NSA document leak in 2013, some national conversation has started some curtailments of surveillance in the form of legislative action. Although Washington has started to make attempts at fixing a very concerning issue, it has not been enough for Americans and surely not for the rest of the world, as *The Drone Papers* illustrate. This section will examine some popular policy ideas as well as critique the little reform that has already started to take place.

The first and most important element of change that needs to happen is the curtailment of existing powers of the government by reexamining legislation. One hundred years of legal precedent and presidential directives are mostly responsible for the NSA and intelligence community's growth in power. Such laws include, but are not limited to, the Espionage Act of 1917, Executive Order 12333, post 9/11 legislation (FISA section 702 and Patriot Act section 215), and Presidential Directive 20. These examples at their core represent an abuse in power by the President and intelligence community. June 2, 2015 saw the passing of the USA Freedom Act that aims to stop bulk data gathering and end the use of section 215 of the Patriot Act. This is a positive step in the direction of privacy and ending the NSA's misuse of power. Despite this, Edward

[79] Supra Note 60

Snowden pointed out that changes to section 215 is not enough and further advocacy and change needs to take place to end nondiscriminatory spying on American citizens[80].

Along with review of laws that have aided in unjust surveillance, the FISA court should receive attention as well. As previously noted, the FISA court is not fully apprised on the warrants that the intelligence community is seeking due to the sensitive nature of active investigations on terror both domestic and foreign. This is highly problematic because it is impossible for a judge to fully deliberate the legality of warrants that delve into an individual's most private and intimate details. There should be a reasonable transparency granted by the intelligence community so that the FISA court and its judges are able to make an informed decision. Even if there is better transparency between the intelligence community and the FISA court, additional measures of control need to be placed. These measures of control can include Supreme Court oversight or better oversight function of the congressional intelligence and national security committees. Another abstract idea of oversight would be implementing a third party to oversee actions of the NSA and intelligence committees. This idea could be similar to Japan's "Saiban-in" system of lay judges and an implementation of an inquisitorial model of inquiry[81]. Currently in America, both left and right wings of politicians desire change in how FISA operates, but the trouble is agreeing in how that will be achieved[82].

---

[80] Dustin Volz, Sarah Mimms & Lauren Fox, THE ATLANTIC THE ATLANTIC (2015), http://www.theatlantic.com/politics/archive/2015/06/senate-passes-major-nsa-reform-bill/445959/ (last visited Mar 5, 2016).
[81] Justin McCurry, TRIAL BY JURY RETURNS TO JAPAN THE GUARDIAN (2009), http://www.theguardian.com/world/2009/aug/03/japan-trial-by-jury-returns (last visited Mar 9, 2016).
[82] Anonymous interview with University of California, Santa Cruz Professor.

Presidential powers also need to be carefully reexamined by the Supreme Court and Congress. After 9/11, President Bush overtly used his presidential powers as granted by Article II of the Constitution. However, these presidential emergency powers that are granted on a temporary basis of national security have been overused with a gross misuse of presidential privilege to retain information from the public, Congress and the courts. This is seen through examination of Washington's use of predatory drones in Syria and Yemen. Corrective action regarding presidential powers can only be achieved through meaningful inquiry by Congress and the Judiciary.

Moving outside the reformation of the three branches of government, it would be useful for government to better define privacy for individuals. This creation of privacy as a civil liberty can be seen in what Donohue calls "property rights" (SOURCE DONOHUE). Many Americans may be surprised to learn that there aren't any entitlements to privacy as interpreted thought the Constitution (SOURCE TRIBE). Because of this, it is necessary to make a legally binding contract for government to respect a person's right to privacy, especially in the context of online activity. Also, the courts specifically need to catch up and recognize the role technology plays in society by granting better protections under the Fourth Amendment.

Reformation also must occur in how the NSA conducts itself along with other similar intelligence branches. This process has already started to happen in the form of public outcry that pushed the USA Freedom Act; however, as stated above, this is not enough. Just like the three branches of government, the NSA needs oversight and safeguard controls applied so that mass domestic surveillance of citizens will not repeat itself in the future. A number of checks and balances can be applied to the NSA,

including some modeled after the controls previously described. Along with this there needs to be a full audit of the surveillance programs to test for legality, practicality and substantiated truth as to their use.

Lastly and possibly most importantly, we need a stricter definition of national security. Current policy and rhetoric reveal just how vague this massively influential term is. In the name of "national security," courts are forced to withdraw from legal proceedings, leaving Congress, the judiciary and the American people in the dark about clandestine operations that may or may not be legal. With a stricter interpretation of what constitutes as national security, true oversight and policy can occur. Currently, there isn't a universal and concrete definition of national security and what it constitutes. Admittedly, unforeseen critical matters of state security might arise and prove challenging to a stricter concept of what national security is. But two possibilities exist to mitigate this issue; the first being congressional and/ or judicial approval of an expansion of the term, or secondly, make a general guideline of what national security is with some circumstantial framework. Of course other possibilities exist; however, it is crucial that there be some form of defining method and criteria in order to end the abuse of the term "national security" now used to simply circumvent governmental checks and balances to push policy or an agenda.

22. Concluding Remarks

Government surveillance undoubtedly complicates issues of legality and policy reform. Constitutionally, these surveillance programs challenge the limits of law because they may facilitate illegal searches and seizures as well as hamper freedom of speech. It's difficult to assess how much these programs have already infringed on American civil

liberties because leaked data is still being analyzed against the backdrop of a slowly evolving court system that has not kept pace with technology and society's use of it. The NSA surveillance programs are also very dangerous in that they feed into Washington's growing use of predatory drones abroad, resulting in extrajudicial killings of innocent civilians.

Despite these sobering facts, Americans have been slow to have a national conversation after the 2013 national security leak by Snowden. According to a report by the Pew Research Center, 49% of Americans conversely feel that the government has not gone *far enough* in taking measures to protect national security[83]. Research shows that nine out of ten Americans know government surveillance exists; however, 82% think it's acceptable for the government to listen to phone conversations and read private messages to thwart terrorist plots aimed at the U.S[84]. When analyzing these findings, researchers and citizens alike must remember that issues of national security on the one hand and civil liberties on the other hand are continually reframed not only by events that happen throughout the world but also by the consent and expectations of the general population. After all, since 9/11 and the subsequent worldwide terror attacks, the general populace has come to expect a national security standard that holds our law enforcement to a zero tolerance on civilian deaths. However, this level of protection expected by society of our less-than-transparent government has yielded controversial legislation and mass

[83] George Gao, What Americans think about NSA surveillance, national security and privacy Pew Research Center RSS (2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ (last visited Mar 7, 2016).

[84] Mary Madden, American's Privacy Strategies Post-Snowden (2015), http://www.pewinternet.org/files/2015/03/pi_americansprivacystrategies_0316151.pdf (last visited Mar 7, 2016).

surveillance. While the NSA and other intelligence agencies use some valuable surveillance tools that might help prevent the next attack, they are far too often questionably applied domestically and abroad. Despite the variation of opinions on government whistleblowers, they serve as an important, and sometimes singular, watchdog to keep the government accountable and honest. Snowden has been criticized by both government and citizens for releasing sensitive information, but no matter what opinions exist of his efforts towards transparency, the fact is that this information exists to the public now, making it impossible and uncomfortably unacceptable for global citizens to claim ignorance of U.S. mass surveillance and predatory drone usage.

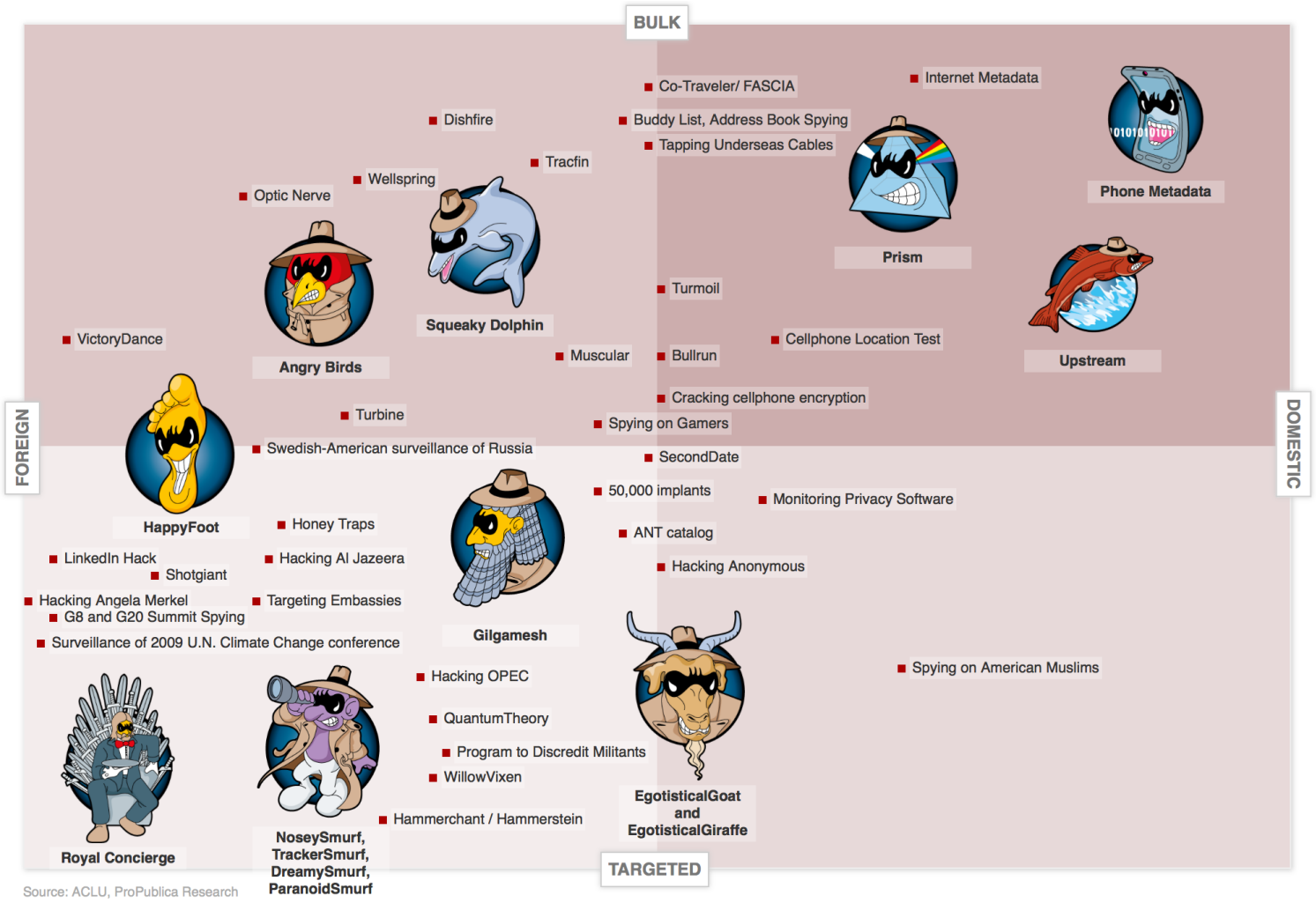
Appendix:

Appendix A: Graph of NSA Programs

Appendix B: Drone Error Graph

Appendix C: Bentham's Panopticon

Appendix A


BULK
FOREIGN
DOMESTIC
TARGETED
Co-Traveler/ FASCIA
Internet Metadata
Dishfire
Buddy List, Address Book Spying
Tapping Underseas Cables
Tracfin
Wellspring
Optic Nerve
Phone Metadata
Prism
Squeaky Dolphin
Angry Birds
Turmoil
Upstream
VictoryDance
Cellphone Location Test
Muscular
Bullrun
Cracking cellphone encryption
Turbine
Spying on Gamers
Swedish-American surveillance of Russia
SecondDate
HappyFoot
50,000 implants
Monitoring Privacy Software
Honey Traps
ANT catalog
LinkedIn Hack
Hacking Al Jazeera
Hacking Anonymous
Shotgiant
Hacking Angela Merkel
Targeting Embassies
G8 and G20 Summit Spying
Gilgamesh
Surveillance of 2009 U.N. Climate Change conference
Spying on American Muslims
Hacking OPEC
QuantumTheory
Program to Discredit Militants
WillowVixen
Hammerchant / Hammerstein
EgotisticalGoat and EgotisticalGiraffe
Royal Concierge
NoseySmurf, TrackerSmurf, DreamySmurf, ParanoidSmurf
Source: ACLU, ProPublica Research

Appendix B

HAYMAKER Operations (01 May – 15 Sep 2012)					
Type	# Ops	EKIA	Detainees	JP	%
Enabled Ops	27	2	61	13	48%
Kinetic Strikes	27	155	N/A	19	70%
Total	54	157	61	32	

Appendix C