5-2017

Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer?

Tayler Houston
University of Tennessee Knoxville, nhousto@emory.edu

Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer?

Tayler Houston

4/29/17

Senior Thesis

I. Introduction

The phrase “mass surveillance” burst onto the world scene in June 2013, when Edward Snowden leaked thousands of NSA documents to the press. These documents contained the shocking revelation that the United States government began spying on its own citizens after 9/11 by collecting phone data, internet search logs, and chat histories. It is important to note, of course, that the US government carried out surveillance on both citizens and non-citizens before September 11, 2001. However, 9/11 marked a turning point in the history of US surveillance. No proof has ever been found that mass surveillance occurred before 9/11.

All surveillance pre-9/11 can be considered traditional surveillance. This encompasses many different techniques that will be detailed in the next section. For now, I will define traditional surveillance as activities such as watching a specific target and looking for specific behavior. In comparison, mass surveillance involves gathering data on millions upon millions of people, not necessarily targets, and sifting through the data for useful information. We now know that this became the norm after the terror attacks of 9/11. The Constitutionality of these programs has been endlessly debated and critiqued, but the question is outside the scope of my research. The programs are occurring regardless of their legality. Therefore, the appropriate question concerns whether or not these mass surveillance programs are efficient and effective uses of national security dollars. Do they make a real difference in stopping terror attacks? Or do traditional, cheaper methods perform at least as well? By undertaking several case studies, I will show that post 9/11 mass domestic surveillance programs are ineffective and inefficient.

II. Terms and Background

In this section I will define key terms necessary to the research. A succinct definition of mass surveillance and targeted surveillance must be established before we can proceed. I will define

mass surveillance in both the positive term of what is it, and the negative definition of what it is not. Negatively defining mass surveillance serves the dual purpose of defining traditional surveillance as well. In an article for the *International Journal of Law, Crime and Justice,* Marie-Helen Maras defines traditional surveillance as: "…the surveillance of a specific individual (or individuals) on a case-by-case basis, based on reasonable suspicion (or probable cause)."[1] Maras' definition covers the two basic requirements of targeted surveillance: (1) The person under surveillance must be a specific person or group, and (2) the person must be suspected of engaging in terrorist activity. These two requirements contrast sharply with mass surveillance programs. Privacy International provides a good working definition of mass surveillance on their website. The definition reads:

> Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring. Any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance.[2]

This definition is a good starting point for a study of mass surveillance. The contrast to traditional, targeted surveillance is readily apparent. Mass surveillance collects data on large swaths of entire populations rather than a specific set of suspected individuals.

History of Mass Surveillance Since 9/11

Mass surveillance rose to prominence after 9/11 as the country looked for answers. The most pressing questions of the time were: (1) How did this happen? and (2) How can it be prevented in the future? The internet's development into something resembling what we know today

[1] Marie-Helen Maras. "The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'?" *International Journal of Law, Crime and Justice* 40, no. 2 (2012): 65.
[2] "Mass Surveillance," Privacy International, accessed January 26, 2017, https://www.privacyinternational.org/node/52.

coincides with these questions. The new technological capabilities of the internet allowed true mass surveillance programs to be developed at a time when the country faced one of the scariest times in its history. This created a perfect storm for mass surveillance programs to gain acceptance among government leaders and national security experts. Many of these mass surveillance programs remain classified to this day and only their most basic features are known. However, leaked documents from 2005 confirmed the existence of such programs. But it was not until Edward Snowden's infamous leaks in 2013 that the functions of these programs truly came to light.

Snowden's revelations remain the best sources of information about these programs, as the government still considers the programs vital to national security. Therefore, my research will focus on the mass surveillance program most illuminated by Mr. Snowden: the Planning Tool for Resource Integration, Synchronization, and Management (PRISM). This program is the cornerstone of the NSA's mass surveillance programs, and enough is known about its workings to assess its performance. Other programs such as BULLRUN and Magic Lantern will remain outside the scope of this research. Both programs remain so heavily classified that there is simply not enough data to assess their effectiveness or even ascertain the true extent of the programs. PRISM can be assessed and studied, so it will compromise my data and analysis of mass surveillance.

PRISM

The largest mass surveillance program revealed by the Edward Snowden leaks was PRISM. One of the leaked documents actually contained the slides from a Powerpoint presentation that the NSA created to explain PRISM. The remainder of this section will show the timeline of the PRISM program, the scope of its surveillance, and the purpose of the program.

PRISM works by pulling data directly from private company servers to NSA databases.[3] The NSA does not directly collect the data for the program. Rather, it takes the metadata from the company servers. For the purposes of this research, metadata will be defined as the following. "Data that serves to provide context or additional information about other data."[4] What does this mean for mass surveillance data collection? The company collects a call log assigned to a certain phone number. The NSA then takes that information from the company server to its own databases. The information inside the call log such as phone numbers, length of calls, location of both phones involved in the call compromises metadata. The metadata provides the NSA with a significant amount of information about a person's communication history.

I will now discuss a timeline and scope of the PRISM program. This will help define the program's parameters and discern a good estimate of how much metadata the PRISM program actually collects. According to the leaked Powerpoint, the PRISM program began collecting data from the servers of Microsoft on September 11, 2007.[5] When a company like this hands over data to the NSA, it hands over all communication data. The comprehensive list includes: emails, chat, videos, pictures, stored cloud data, file transfers, video conferences, login activity, and social media activity.[6] This means that Microsoft gives the PRISM program all of the emails collected on its network. All file transfers across the Microsoft Office products also eventually make their way to the NSA. This also means that Microsoft turns over all communications collected through Xbox Live, Hotmail, and other platforms underneath the Microsoft corporate

[3] "NSA Prism program slides," *The Guardian,* November 1, 2013.
[4] "Metadata", Business Dictionary, http://www.businessdictionary.com/definition/metadata.html, accessed February 1, 2017.
[5] "NSA Prism program slides," *The Guardian,* November 1, 2013.
[6] Ibid.

umbrella. As we can see, the data collected from just Microsoft contains an astonishing array of electronic information.

PRISM grew slowly after the Microsoft collection began in 2007. PRISM's collection of Yahoo data started in March 2009.[7] Yahoo was the only new company in 2009. The timeline speeds up significantly in the new decade. Google, Facebook, and PalTalk all joined PRISM in 2009. The collection of Google data in particular represented a breakthrough for PRISM, as we shall see below. Youtube, Skype, and AOL data all entered the PRISM collection system between September 2010 and March 2011. Finally, the last company PRISM began collecting from was Apple in October 2012.[8] The nine companies I mention here are tech giants. Collectively, they provide virtually all services possible on the internet. Therefore, PRISM contains information from all major forms of communication online. The exact amount of metadata collected by the program cannot be accurately determined due to the customer privacy policies of these companies. However, practically everyone on the internet uses these nine companies in some capacity. With virtual certainty, we can estimate the amount of metadata collected to be measured in the trillions rather than millions or billions.

Next, I will explain exactly how PRISM works and how prevalent it has become in the intelligence community. The NSA designed PRISM to pick up information from non-American sources. In fact, no American data should be picked up by the system. As we shall see, this is not the case, however. The first key to understanding PRISM is that it is not a completely unrestricted surveillance program. According to former Director of National Intelligence Clapper PRISM "cannot be used to intentionally target any U.S. citizen, or any other U.S. person, or to

[7] Ibid.
[8] Ibid.

intentionally target any person known to be in the United States."[9] "Intentionally" is the key word here. The NSA must be 51 percent confident of a target's foreignness to collect the data.[10] The 51 percent certainty represents no practical barrier to collection because of the way data travels around the world before entering the servers of the nine partner companies. The NSA PowerPoint explains that data takes the cheapest and easiest path to its final destination. This path will not always be the most physically direct.[11] What this means in real terms is that most data bounces around servers in multiple countries before being collected. The NSA simply needs to be 51 percent confident the data originated outside the United States before it can collect the data. Most of the data created in the United States bounces off servers outside the U.S. before returning to its final destination. The NSA can point to those stops as justification for collection and a belief that the data originated outside the border. Therefore, countless numbers of American citizens' data has no doubt been collected by PRISM on "accident" when the program wrongly thought the data originated outside the United States. The NSA seemingly cares little that it is collecting data on American citizens. PRISM training material obtained by the *Washington Post* "instruct new analysts to make quarterly reports of any accidental collection of U.S. content, but add that 'it's nothing to worry about.'"[12]

For all the denial and misdirection by the NSA, PRISM is a data mining program at its core. For this research, I will use the following definition of data mining. Data mining is "the process of collecting, searching through, and analyzing a large amount of data in a database, as

---

[9] James Clapper, "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," June 8, 2013.
[10] Benjamin Dreyfuss and Emily Dreyfuss, "What is the NSA's PRISM program? (FAQ)," *CNET,* June 12, 2013.
[11] "NSA Prism program slides," *The Guardian,* November 1, 2013.
[12] Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post,* June 7, 2013.

to discover patterns or relationships."[13] Many industries, such as online retailing, use data mining to identify the products individual consumers will find most interesting. Data mining algorithms are the reason certain advertisements appear on the sides of websites we surf. PRISM took the concept and uses it to identify certain physical locations and phrases that send up red flags. Data mining programs work by using algorithms to search the tags found in metadata. A tag is simply a description attached to the metadata. For example, an email originating in Australia that concerns giving money to the koala bear fund would likely hold the tags of Australia, money, and koala. Tags exist to make large amounts of data easily searchable. In essence, tagging data represents half of the PRISM program. The best analogy for a data mining surveillance program is trying to find a needle in a haystack. The collection of emails, text messages, and video chats from the nine tech companies mentioned above is the haystack. Applying tags to the data essentially separates the haystack into millions of different pieces of hay that can be seen individually instead of as a solid, huge group. The final step contains the actual mining.

The intricacies of data mining cannot be adequately described here. Therefore, a stripped down version will be used to explain how PRISM works in principle. The actual algorithms are too complicated for anyone without a doctorate in computer science to understand. PRISM uses both anomaly detection mining and cluster detection mining. Anomaly detection can be summed up as follows: "Statistics can be used to determine if something is notably different from this pattern."[14] In a data set as large as PRISM's, this type of mining reveals important distinctions. The vast majority of communications data collected by PRISM likely talks about mundane topics such as dinner plans, shopping lists, and other general conversations between friends and family.

---

[13] Data Mining, dictionary.com, http://www.dictionary.com/browse/data--mining, accessed February 3, 2017.

[14] Alexander Furnas, "Everything You Wanted to Know About Data Mining but Were Afraid to Ask," *The Atlantic*, April 3, 2012.

The tags on this data probably include nothing beyond restaurant names, country of origin, and basic conversation topics. A Google search of homemade bomb ingredients clearly stands out in that group. This is the essence of PRISM. The bomb tag on the Google search sends up a red flag and notifies the NSA to dig deeper into the individual involved in the red flag.

The deeper surveillance after a raised red flag falls into the cluster detection category. Cluster mining compromises exactly what it sounds like. Algorithms search for a cluster of words originating from the same source. The goal here is to reveal subgroups within the data that differ significantly from the dataset as a whole.[15] The following example of the two data mining techniques found in PRISM working in tandem will explain the program fully. A person in ISIS-controlled territory in Syria sends an email to a relative in New York City asking for money. The combination of the email originating in ISIS territory and the money tag placed on the data should raise a red flag through the anomaly detection algorithm. A cluster detection algorithm then goes into effect to look at the person's other communications collected by PRISM. It will look for tags that look suspicious when combined with Syria and money. The program may find a text message to the same New York City relative with the words *ISIS* and *plans*. It may also turn up a Youtube search for "How to make explosive devices." Then the final find could be a Skype call between the New City relative and ten computers in Aleppo, Syria where the relative promises a donation to the cause. Taken together, these tags send up another red flag via the cluster algorithm. At this point, the NSA either arrests the target in New York City on conspiracy and terrorism charges or continues to collect evidence in an effort to uncover a larger plot. In theory, this is exactly how PRISM should stop terrorist attacks.

[15] Fumas, "Data Mining."

The budget of PRISM is unknown but has been hotly debated. The leaked Snowden PowerPoint lists the PRISM program cost at approximately $20M annually.[16] The $20M figure is the only number ever released, willingly or otherwise, by the NSA. Many experts and industry insiders believe this to be a low figure. This may be the cost of moving the metadata from the company servers to the NSA datacenter in Utah, but the movement is hardly the only cost of the program. The data center itself must be factored into the equation. The new data center cost a reported $1.7B to build. It also uses 65 megawatts of power per month.[17] The facility is a massive expenditure made necessary by the vast collection of data. The Utah datacenter houses state of the art equipment. However, things change fast in the tech industry. It is not unreasonable to conclude that the center will require renovation in 20-25 years to convert to the newest data storage capabilities. Twenty-five years ago, the most common form of storage was the floppy disk. Therefore, we can divide the $1.7B by twenty-five to get a per year cost of the facility. That answer computes to $68M. This figure can be tacked onto the program cost. Additionally, the NSA must pay for the data to be looked through regularly. "According to the NSA's director of compliance, the agency queries its databases about 20 million times each month."[18] Checking the databases costs money even if an algorithm does the work. The programmer that designed the algorithm received payment as well. All these costs add up to significantly more than $20M per year. The real cost of operating, based on these fairly conservative calculations, runs closer to $100M annually.

Traditional Surveillance History Since 9/11

16

17 Rory Carrol, "Welcome to Utah, the NSA's desert home for eavesdropping on America," *Guardian,* June, 14, 2013.

18 John Mueller and Mark G. Stewart, "Secret without Reason and Costly without Accomplishment: Questioning the National Security Agency's Metadata Program," *ISJLP* 10 (2014): 412.

Before the internet and associated technology made programs like PRISM possible, the FBI, CIA, and NSA relied on much more traditional techniques to stop terrorists. These techniques include using informants, setting up stings, and deploying undercover agents to perform targeted surveillance of individuals under suspicion. This section will look at each of these surveillance techniques and see how the intelligence community still uses them to stop terrorists in the modern age. The strategies may be dated, but they still achieve the desired results in many cases.

The FBI and other national security agencies have used informants to help solve all manner of crimes since their inception. In fact, acquiring informants who can testify to the guilt of a criminal is probably the oldest investigative technique in the world. "Courts have countenanced the use of informers from time immemorial."[19] Informants remain important tools for stopping terrorism, but the nature of terrorism has brought about changes in how they are used. Informants historically provided excellent information for white collar crimes such as fraud. Additionally, informants have been instrumental in bringing down crime families involved in gambling, drugs, and prostitution in the past. This is because informants are people involved in the crime organizations that have intimate knowledge of the illegal activities. Also, law enforcement could afford to receive bad information when dealing with these crimes because fraud and gambling are typically thought of as victimless crimes. At the very least, the victims' lives are generally not at stake even if their property or finances may be. In contrast, terrorist attacks embody the very definition of a mass victim crime. Terror attacks aim to maim or kill as many people as possible to create fear and further the aims of a terrorist organization. As a result, national security agencies need to find a higher number of informants and also more

[19] *United States v. Dennis*, 183 F.2d 201, 224 (2d Cir. 1950)

knowledgeable informants. Many lives potentially hang in the balance. As a result, the number of informants increased dramatically after 9/11 from just 1,500 in 1975 to over 15,000 in 2014.[20] This represents a 1,000 percent increase in informant numbers in 40 years. The rules for handling informants also changed in response to the demands of terrorism. The executive branch holds much more sway in matters of national security and defense than in domestic law enforcement scenarios such as the crime families I discussed earlier. Therefore, the executive branch possesses much more leeway when dealing with terror informants than they do with traditional informants. This can mean anything from more secrecy surrounding the identity of the informant, to more pay for informant services, to recruitment of individuals the government would rather the citizenry not know it associates with on a regular basis.[21] In short, the rules and regulations that traditionally governed informant and government interaction loosened significantly after 9/11. The mass killing associated with terror attacks necessitated a 'by any means necessary' approach to informant based intelligence.

National security agencies adopted a more aggressive approach to sting set-ups after 9/11. Many of these operations have been accused of crossing the line into entrapment scenarios, which is illegal in terrorism cases as in other cases. However, the legality of these techniques is outside the scope of my research. This section will focus on the frequency of the use of the technique, while its effectiveness will be discussed later in the paper. Once again, the F.B.I. and other agencies do not release exact statistics and details for every case, but enough information exists to make an informed estimate on the number of undercover stings performed. The information surrounding the stings set up to catch Al Qaeda sympathizers in the early 2000s are

[20] Emily Stabile, *Recruiting Terrorism Informants: The Problems with Immigration Incentives and the S-6 Visa*, 102 Cal. L. Rev. 237 (2014): 244.
[21] Ibid., 244-245.

still classified in many instances, as the Bush administration operated more in the shadows. There is significantly more information about the operations to stop ISIS sympathizers in the last few years. Therefore, all the information in the next paragraph relates to stings on ISIS supporters in the US in the previous five years.

Since late 2013, almost 90 people in America have been charged with providing some level of support to ISIS. In the first few months of 2014, only 30 percent of the two dozen ISIS cases featured evidence from an undercover sting. From the last half of 2014 until February 2015, the number grew to 45 percent. Finally, since February 2015, the number grew to 67 percent, with 40 of the 60 cases featuring evidence obtained through undercover stings.[22] The rise in stings came about for a very specific reason—stings do not require a warrant or any outside approval. This means stings can be set in motion immediately once a target is acquired.[23] Security agencies only have a finite amount of time to stop terror plots before the attack takes place. Every day the agency saves by initiating a sting rather than waiting on judicial approval could be vital to saving lives.

The actions taken by undercover agents to set-up a sting or acquire evidence vary greatly from case to case. Understanding how many different actions undercover operatives can take is important to understanding their usefulness. Traditionally, undercover agents infiltrated organizations and gathered intelligence to implicate members on conspiracy charges or obtain unknowing confessions. In the post 9/11 world, undercover agents act much more proactively to take down targets. Several examples from the past few years illustrate the point. In North Carolina, an undercover agent repeatedly asked a suspected domestic terrorist if he thought he

[22] Eric Lichtblau, "F.B.I. Steps Up Use of Stings in ISIS Cases," *New York Times,* June 7, 2016.
[23] Ibid.

could actually carry out an attack. The suspect wavered until finally saying yes in 2015. The agent then sold the suspect an AR-15 assault rifle. The FBI immediately arrested and charged the man on terrorism charges after the sale took place.[24] This scenario demonstrates a much more proactive use of undercover agents. Security agencies are no longer content to wait for suspects to radicalize fully and commit crimes on their own. They want to identify people in the process of radicalizing via undercover agents. Then, they use the agents to complete the radicalization process and arrest the suspect before an attack has any chance of materializing.

The case of Hasan Edmonds shows the full extent of undercover activities in the post 9/11 era. Mr. Edmonds published posts on social media that the FBI found threatening. They immediately assigned an undercover operative to establish contact with Mr. Edmonds in the hope of eventually setting up a sting if the posts were his true beliefs. The operative and Mr. Edmonds exchanged messages over the course of a few months discussing ISIS and commitment to the terrorist organization's cause. Eventually, the operative saw Mr. Edmonds' messages becoming more and more radical. Edmonds told the undercover operative he planned to travel to the Middle East to receive training from ISIS. The operative agreed to go with him.[25] It is impossible to know whether Edmonds would have reached that stage of radicalization without the encouragement of the undercover operative. Edmonds felt he had found a friend and brother in the cause, and the two radicalized at the same pace. Regardless, when Edmonds bought tickets to travel to the Middle East to train with ISIS, he broke several laws. A couple of weeks later, Edmonds went to Chicago Midway International Airport to travel to the Middle East with the operative. The FBI awaited him at the airport and took him into custody upon arrival.[26]

[24] Ibid.
[25] Ibid.
[26] Ibid.

Much like informant usage, national security agencies became much more proactive and aggressive when using undercover operatives to stop terrorists after 9/11. The surveillance techniques are traditional, but their use evolved with the times and the changing threats presented by terrorists.

III. Data and Methods

The remaining sections of this paper will present the findings of my research. Terrorist attacks are extremely uncommon in America. For the most part, the anti-terrorism strategy in America works. However, the brutality and loss of life associated with terror attacks mean that "for the most part" is not good enough. Any successful attack could lead to large numbers of deaths and a huge increase in fear and uncertainty for citizens. Improvement is possible and necessary in anti-terrorism methods until attacks disappear entirely. Unfortunately for my research, the success in preventing terror attacks leaves a small number of attacks to study. Additionally, the secrecy surrounding national security makes it even more difficult to find reliable and comprehensive data. Therefore, my research will focus on the terrorist attacks in Orlando, San Bernardino, and Boston. I will do this using a case study method that I will detail below. All the perpetrators of these attacks made communications and online searches that should have been detected by PRISM. It is my contention that these attacks could have been prevented if national security agencies had relied less on mass surveillance techniques and used other tools at their disposal. These three case studies show the weaknesses of PRISM, and illustrate why traditional surveillance methods need to be utilized more going forward.

A succinct definition of a case study is needed before I explain why it is the best option. A case study is defined as "the documentation of some particular phenomenon or set of events which has been assembled with the explicit end in view of drawing theoretical conclusions from

it."[27] Here, I use this process. Specifically, I look at what is known about perpetrators' communications and activities as they developed into radicalized terrorists. I will then identify key behaviors that PRISM should have been able to identify and demonstrate the shortcomings of the program.

The case study method is the proper choice for my research for several reasons. The first is that it suits the aims of my research. As Roger Gomm explains in *A Case Study Method,* case studies work best when "the aims are understanding, extension of experience, and increase in conviction in that which is known."[28] The goal of this paper is to understand why PRISM failed to identify these people before they acted, and to show that these failures demonstrate weaknesses in the program that may lead to more attacks in the future. Also, my data shows traditional methods work better than mass surveillance does. The case studies affirm this fact.

The second reason a case study approach works best is the aforementioned secrecy and lack of data surrounding most terrorist attacks and intelligence agencies. Most terror plots never become public knowledge. The major attacks that do receive national coverage are subjected to incredible scrutiny by academics and journalists alike. News organizations in particular dig until they learn everything possible about the people responsible for the attacks. This leads to a wealth of data available about these attacks and how the entire process unfolded. A case study approach fits with this type of research because I can systematically lay out all the information known about the perpetrators using in-depth case studies and then draw conclusions from the similarities found in all three cases. Gomm explains that case studies are usually too narrow to draw specific

[27] Gomm, Roger., and Hammersley, Martyn. *Case Study Method*. (London: SAGE Publications, 2013), 169.
[28] Gomm, Roger., and Hammersley, Martyn. *Case Study Method*. (London: SAGE Publications, 2013), 21.

conclusions, but they work very well when making broad general conclusions that apply to similar occurrences.[29] As my findings will show, many terrorists attacks are similar occurrences. By using a case study method, I will be able to identify the similarities easily and then make relevant conclusions that show the problems with PRISM.

IV. Findings

This research aims to support two related, but separate contentions: (1) mass surveillance is ineffective at stopping terrorism; and (2) mass surveillance programs are inefficient uses of national security resources. This section will provide evidence to support both of these claims. The opening part of the section contains many statistics and facts about PRISM usage and prevalence. These numbers show the inefficiency of the program and PRISM's lack of success. The case studies that comprise the larger, second part of this section provide real world examples of the consequences of mass surveillance failure. All of the terrorists involved in the Orlando, San Bernardino, and Boston attacks made mistakes that PRISM should have detected.

PRISM became incredibly important in national security briefings and reports quickly after its inception. The following data is accurate to June 2013, when the Snowden leaks occurred. I will use these figures to make various estimates about present day numbers throughout the section. As I note above, PRISM went live in 2007, but it did not collect data from the majority of the nine companies until 2009-10. As of June 2013, data from PRISM was cited in the president's daily intelligence briefing 1,477 times.[30] This number is astonishingly high. If we assume PRISM required a few months after its inception to collect enough data to be useable in intelligence briefings, it puts the starting date for PRISM data's inclusion in security

[29] Ibid., 101-103.
[30] Elias Groll, "By the numbers: The NSA's super secret spy program, PRISM," foreignpolicy.com, June 7, 2013.

reports at the beginning of 2008. With just a bit of math, it becomes clear how prevalent PRISM data is in national security matters. If we divide 1,477 reports by 365 days per year, the answer comes to four years and 17 days' worth of reports that feature data obtained through PRISM. This means only roughly 400-450 daily intelligence briefings did not feature PRISM data from 2008 until June 2013. There is no data suggesting this prevalence declined after June 2013, but the exact figures remain classified.

The above number includes just the daily intelligence briefing to the president. Across all national security reports, PRISM has been cited 77,000 times. For the period under study, there are around 2,000 reports each month that cite PRISM.[31] These figures are also accurate to June 2013. The limited data in the Snowden leaks show a 27 percent increase in PRISM reports from 2011 to 2012.[32] It is almost certain that the rate has increased at a similar yearly rate to the present day, but the data simply does not exist. Thus, here I assume the rate is still 2,000 reports per month to avoid inflating the numbers. Forty-four complete months have passed since June 2013. This means a minimum of 88,000 reports citing PRISM data have been created since these figures were released. These calculations clearly show the prevalence of PRISM in national security surveillance.

The next step in my research is determining the efficiency of PRISM. Efficiency can be defined as "performing or functioning in the best possible manner with the least waste of time and effort."[33] I will determine the efficiency of PRISM using this definition. I will first determine how successful mass surveillance has been at stopping terrorist attacks. Doing this serves a dual purpose. First, mass surveillance exists to stop terrorist attacks. Therefore, the only way to

[31] Ibid.
[32] Ibid.
[33] "Efficient," dictionary.com, accessed March 3, 2017.

determine its effectiveness is to determine the percentage of attacks that were foiled by the program. Second, the number of successfully stopped attacks helps determine efficiency. I will take the number of successes and calculate the percentage of total reports they comprise.

The exact number of attacks PRISM stopped has been heavily debated. The NSA publicly claimed in 2013 that PRISM played a role in stopping 54 terror plots around the globe, not just in America.[34] This claim occurred just after the Snowden leaks when public pressure on the NSA was at its highest. It has been thoroughly debunked in the years since. First, this research is only concerned with terrorism in America. Terrorism is certainly a worldwide problem, but any attacks planned to occur outside of the United States' borders also fall outside the scope of my research.

A Senate Judiciary Committee appointed to investigate the NSA uncovered new information in late 2013. Only 13 of the 54 plots had any connection whatsoever to the United States.[35] This does not mean that PRISM stopped 13 imminent terror attacks on U.S. soil. It could mean that an imminent attack was foiled, but it could also simply mean that a person in the U.S. provided some type of support for a terrorist attack somewhere in the world. This could mean anything from monetary support to actually buying the materials to make a homemade bomb. When pressed further by the Senate Committee, the NSA chief admitted that only one or two terror plots were directly foiled by mass surveillance programs such as PRISM.[36] The program likely played a minor part in stopping more than one or two attacks, but the committee's findings appear to show that only one attack was directly foiled because of mass surveillance.

---

[34] Heather Kelly, "NSA chief: Snooping is crucial to fighting terrorism," *CNN,* August 1, 2013.
[35] Shaun Waterman, "NSA chief's admission of misleading numbers adds to Obama administration blunders," *Washington Post*, October 2, 2013.
[36] Ibid.

The attack mentioned by the NSA chief appears to be the investigation and arrest of Najibulla Zazi in 2009. PRISM uncovered communications between known al-Qaida operatives overseas and Zazi.[37] This appears to be a textbook example of PRISM's anomaly detection algorithm working to perfection. The NSA immediately got in contact with the FBI and an investigation commenced. The NSA found a connection to another U.S. based extremist named Adis Medunjanin.[38] Communication between the two and overseas terrorists revealed a planned attack on the New York City subway system. The two were arrested in 2009 and sentenced to life in prison in 2012.[39] There is no disputing that PRISM worked to perfection in this instance. The algorithm threw up a red flag on Zazi's communication and directly led to the uncovering of what could have been a major terrorist attack in New York City. However, this is the only example of PRISM, and mass surveillance in general, working to perfection.

Now that the successes of PRISM are understood, it is possible to quantify its level of effectiveness and efficiency. I will begin by assessing its effectiveness. Since 9/11, four and possibly five major terrorist attacks occurred on American soil. The four attacks that virtually all experts agree constitute terrorism are the attacks in Orlando, Boston, and San Bernardino that make up the upcoming case studies, plus the 2009 shooting at Fort Hood. Information about the Fort Hood attack is classified, so there is simply not enough information for it to be a case study here. The 2015 shootings in Chattanooga are debated because no links to overseas terrorists were found. Because of this, I will exclude this attack from the list as well. Without any overseas communication taking place, PRISM had virtually no chance of detecting the attacker. As

[37] U.S. House of Representatives Permanent Select Committee, *54 Attacks in 20 Countries Thwarted By NSA Collection*, 2013, 1.
[38] Ibid., 1.
[39] Ibid., 1.

previously mentioned, PRISM must be at least 51 percent sure the data originated overseas before it can be collected. Seventy-nine people died as a result of the attacks in Orlando, San Bernardino, Boston, and Fort Hood.[40]

The above paragraph shows that PRISM essentially went one for five in stopping major terrorist attacks on American soil after its inception in 2009. Again, the NSA chief himself admitted that PRISM stopped just one attack. A 20 percent success rate is simply not good enough when dealing with terrorism. Seventy-nine people lost their lives because mass surveillance did not work well enough. PRISM and mass surveillance are not solely responsible for these failures. The previous sections of this thesis prove that the NSA and FBI use other tactics. However, I have also demonstrated these agencies relied much more heavily on mass surveillance than traditional surveillance in recent years. The over-reliance on mass surveillance systems is unjustifiable when there is only a twenty percent effectiveness rate.

I will now use these calculations to determine the efficiency of PRISM. PRISM boasts one stopped attack to its name. Using the previous numbers of 77,000 reports featuring PRISM up to June 2013 and a conservative estimate of 88,000 reports from June 2013 to the present, we see that 165,000 total reports, at minimum, featured data collected from PRISM. These reports played a leading role in stopping one major terror plot. This figure may be a bit unfair to PRISM. The NSA chief admitted that PRISM played a leading role in only one stopped plot. However, it did play a minor role in providing information during the other twelve plots with U.S. connections. If I relax my standards to include all 13 terror plots connected to the United States, that figure falls to 12,692 reports per attack PRISM had a hand in stopping. This figure is still astronomically high. That averages out to one report a day for over 35 years just to stop one

[40] Bobby Ilich, "The United States After 9/11: How Many Major Terrorist Attacks Have There Been In America Since 2001?," *International Business Times*, September 9, 2016.

attack. Our definition of efficient called for "the least waste of time and effort." This figure indisputably demonstrates a tremendous waste of time and effort. This wasted time, effort, and resources could be used to increase the use of traditional surveillance methods that have proved to be effective.

As the initial definitions in Section II showed, all surveillance techniques fall into the categories of either mass surveillance or traditional surveillance. Therefore, it can be safely assumed that any terrorist attack foiled by anything other than mass surveillance was primarily stopped using traditional methods. Terror attacks cannot be stopped without extensive information. As the case studies will show, law enforcement officers on the scene have very little chance of stopping a well-planned attack from occurring. Prior knowledge that only surveillance can provide is the only way to foil terror plots.

By using this logic, we can assume that traditional surveillance methods played the leading role in stopping the other 12 foiled attacks on U.S. soil since 9/11. Traditional methods obviously failed to stop the same four attacks as PRISM in Orlando, Fort Hood, San Bernardino, and Boston. Additionally, traditional methods such as informants, undercover agents, and civilian tips should have detected the activity in Chattanooga. Therefore, I will include that attack in these calculations as well. This brings the total number of attacks traditional methods should have stopped to 17. Twelve attacks were actually stopped. This computes to a 70.59 percent success rate. While nowhere near perfect, or even acceptable, this figure is over three and half times higher than PRISM. These calculations definitively prove that traditional methods are more effective at stopping terrorist attacks than mass surveillance programs.

Orlando

The following three case studies will dissect the actions of the three terrorists that carried out the attacks in Orlando, Boston, and San Bernardino. Each terrorist made mistakes and communicated with people that should have raised the red flags of PRISM. Mass surveillance failed Americans in these three cases. Many people lost their lives because PRISM does not work in practice like it claims to. The case studies will provide specific examples of the mistakes the statistics in the previous section brought to light.

First, it is necessary to detail the actual attack to understand what mass surveillance should have prevented. On June 12, 2016, Omar Mateen entered Pulse Nightclub in Orlando and killed 49 people, while wounding 53 more. The attack was the deadliest mass shooting in United States history and the worst terrorist attack on U.S. soil since 9/11.[41] Pulse is a gay nightclub. Officials initially thought the attack was "just" a hate crime, but the theory fell through when Mateen called 911 from inside the nightclub and pledged allegiance to ISIS. National security agencies immediately labeled the attack an act of terrorism.[42] These are the most basic facts of the attack. The next several paragraphs will dig into Mateen's past and show when mistakes were made in surveillance.

The FBI investigated Omar Mateen for 10 months before the attack took place. The investigation began in May 2013 and continued until March 2014. The FBI undertook the investigation because of a tenuous connection found between Mateen and a Syrian suicide bomber.[43] The bomber, Moner Mohammad Abu-Salha, was the first American suicide bomber in Syria. Abu-Salha was born in Florida but traveled to Syria to fight with an extreme, jihadist

[41] Ralph Ellis, Ashley Fantz, Faith Karimi, and Eliott C. McLaughlin, "Orlando shooting: 49 killed, shooter pledged ISIS allegiance," *CNN*, June 13, 2016.
[42] Ibid.
[43] Del Quintin Wilber, "The FBI investigated the Orlando mass shooter for 10 months — and found nothing," *Los Angeles Times*, July 14, 2016.

group there. When Abu-Salha committed a suicide bombing in Syria, national security officials began looking into possible connections he had in the United States. The search led to Omar Mateen because the two attended the same mosque in south Florida.[44] The FBI cannot legally open investigations into individuals just because they attend a certain mosque. The investigation focused on Mateen because of comments he made to a coworker that came to light during the very basic investigation of the mosque's attendees.

Mateen worked as a security guard in Port St. Lucie, Florida at the PGA Village. He told the FBI during their later investigation that several coworkers harassed him for being Islamic. The FBI determined that the harassment did take place, but the comments still warranted further investigation.[45] His response to these discriminative remarks was not to go to his boss or a civil attorney to take legal action. According to a former coworker, Daniel Gilroy, Mateen repeatedly threatened violence against minorities and made vague threats against his attackers. Gilroy stated: "You meet bigots, but he was above and beyond. He was always angry, sweating, just angry at the world."[46] Mateen also reportedly tried to scare these coworkers by claiming connections to overseas terrorists and telling them that he hoped the FBI raided his home so that he could "die a martyr."[47] The FBI decided to open an investigation into Mateen when these comments came to light during their preliminary investigation of the mosque. The formal investigation of Mateen that followed shows a failure of PRISM, while highlighting the need of more aggressive traditional surveillance.

---

[44] Lizzie Dearden, "Orlando shooting: How gunman Omar Mateen was linked to first American suicide bomber in Syria," *The Independent*, June 14, 2016.
[45] Del Quintin Wilber, "The FBI investigated the Orlando mass shooter for 10 months — and found nothing," *Los Angeles Times*, July 14, 2016.
[46] "Orlando terror attack updates: Obama meets with victims' families in Orlando," *LA Times*, June 16, 2016.
[47] Mark Mazzetti, "Omar Mateen, Twice Scrutinized by F.B.I., Shows Threat of Lone Terrorists," *New York Times*, June 13, 2016.

An important distinction must be made at this point. The FBI could only open a preliminary investigation into Mateen at this time because it had no proof he actually planned to commit an attack. According to the Department of Justice, a preliminary investigation can only last six months with the option for six more months if a breakthrough appears imminent. Additionally, wiretapping and other more invasive surveillance are prohibited during a preliminary investigation. These measures can only be taken if a full investigation is opened based on the findings of the preliminary investigation.[48] The first step the FBI took when opening the investigation in May 2013 was to add Mateen to the nationwide Terrorist Watchlist. By placing him on the Terrorist Watchlist, the FBI ensured Mateen received extra attention at airports. Also, the FBI was notified if Mateen tried to purchase a gun or was arrested for any reason by the police.[49] The FBI then transitioned into more invasive techniques. They ran Mateen's name through criminal and terrorism databases and found nothing. They also obtained his call log and found no links to anyone else on the Terrorist Watchlist or any known terrorist numbers overseas.[50] At this point, traditional methods and PRISM should have detected nothing abnormal about Mateen.

The FBI began following Mateen using unmarked vehicles but found no bad behavior or acquaintances. They also used two undercover informants against Mateen in an effort to catch him saying incriminating statements. Mateen admitted to the informants that he had claimed radical ties at his work, but he said he did so only to stop the harassment he received.[51] The FBI

---

[48] *The Attorney General's Guideline for Domestic FBI Operations*, Washington, D.C.: United States Department of Justice.
[49] Del Quintin Wilber, "The FBI investigated the Orlando mass shooter for 10 months — and found nothing," *Los Angeles Times*, July 14, 2016.
[50] Ibid.
[51] Ibid.

found the claim suspicious and extended the preliminary search and directly interviewed Mateen twice. He brushed off the claims of terrorists ties as meaningless threats to discriminatory coworkers. The FBI could not catch him in any further lies and therefore could not convince a court to allow them to eavesdrop on his communications or gain access to his computer.[52] The investigation concluded. This meant the FBI was also forced to remove Mateen from the Terrorist Watchlist. The FBI conducted a reasonably thorough investigation using traditional methods, but Department of Justice guidelines kept them from using the most invasive tools at their disposal. The FBI's investigation after the shooting at Pulse Nightclub proved this to be a huge mistake.

After the attack took place, FBI Director James Comey said: "We are highly confident that this killer was radicalized and at least in some part, through the internet."[53] The mention of the internet brings PRISM into play. It now appears as though Mateen was radicalized through a combination of online events. He watched extremist sermons online, watched ISIS beheading videos, conducted research into ISIS beliefs, and visited chatrooms where extremists shared doctrine.[54] These are all activities that PRISM should have collected and analyzed. If we think back to my earlier example of how PRISM works, we can see strong similarities. These online interactions, when taken alone, should have sent off a red flag in the PRISM system. When taken together, there is no question that these activities should have set off a cluster algorithm. If PRISM would have detected these activities, the FBI almost certainly would have opened a full investigation and possibly charged Mateen with terrorism. At the very least, Mateen would have

[52] Ibid.
[53] "Did FBI miss signs in past investigations of Orlando killer?," *CBS News*, June 14, 2016.
[54] Del Quintin Wilber, "The FBI investigated the Orlando mass shooter for 10 months — and found nothing," *Los Angeles Times*, July 14, 2016.

stayed under surveillance and on the Terrorist Watchlist. If he stayed on the watchlist, the FBI would have been informed immediately when he purchased an AR-15 style assault rifle and 9mm semiautomatic pistol within a week of the attack.[55] Instead, Mateen legally purchased the guns under no threat of FBI notification and killed 49 people in a terror attack. The attack was entirely preventable if PRISM worked properly and detected Mateen's online activity.

Boston

The next case study I will undertake is of the Boston Marathon bombing that took place on April 15, 2013. This section will follow the same framework as the Orlando study by starting with a description of the attack, a discussion of what national security agencies tried to do, and finally, how mass surveillance failed to stop the attack. Brothers Tamerlan and Dzhokhar Tsarnaev carried out the attack near the finish line of the race. The Tsarnaev brothers built two homemade bombs inside pressure cookers. The pressure cookers were filled with pellets and nails to create shrapnel after the explosion. The brothers placed the pressure cooker bombs inside backpacks and left the bombs approximately 100 yards apart near the finish line of the marathon. The bombs exploded eight to 12 seconds apart in the extremely crowded area around the finish line. The explosions killed three people and wounded 264 others.[56] The actual loss of life in this case was much lower than that from the Orlando attack. However, the very high number of wounded suggests that a better made or more powerful bomb could have caused a significantly higher number of deaths. The nails and pellets were simply not big enough to cause a high rate of death. Regardless, this attack caused a large amount of casualties and emotional problems that could have been prevented.

---

[55] Cassandra Vinograd, "Omar Mateen Probed for Terror Ties but Legally Purchased Weapons," *NBC News,* June 13, 2016.
[56] CNN Library, "Boston Marathon Terror Attack Fast Facts," *CNN*, March 29, 2017.

The Tsarnaev family came to America in 2002 seeking asylum. They fled their homeland of Chechnya during a brutal war being waged there between Russian security forces and Islamic extremist groups in the area. The United States granted their asylum claim and Tamerlan, 15 at the time, and Dzhokhar, 8, began lives in a new country.[57] Dzhokhar appears to have adjusted to life in America as well as possible and displayed no signs of radicalization before the attack. He appears to have been directly influenced by his brother. As a result, neither traditional methods nor PRISM probably could have prevented Dzhokhar's participation in the attack. Tamerlan appears to have masterminded the attack and will be the focus of this case study.

Tamerlan represented New England in the national Golden Gloves boxing tournament in 2009 after winning the Northeast regional tournament. In the press releases leading up to the event, Tamerlan talked candidly about life in America. He stated: "I don't have a single American friend, I don't understand them."[58] Comments like these seem to hint at a strong discontent Tamerlan felt for Americans and American society. In an interview, his mother talked about Tamerlan's beliefs. She stated that he became interested in religious politics about five years before the attack. She thought he studied the subject solely to better understand the complexities of the conflict taking place in his homeland of Chechnya. She stressed that he "never, never told me he would be on the side of jihad."[59]

In 2011, close to three years after his mother stated he became interested in religious politics, the FBI opened a preliminary investigation on Tamerlan at the behest of the Russian government. The FSB, Moscow's version of the CIA, sent information to the FBI in March

[57] Peter Finn, "Tsarnaev brothers' homeland was war-torn Chechnya," *Washington Post,* April 19, 2013.
[58] Timothy Bella, "Marathon Bombing Suspect: 'I Don't Have A Single American Friend'," *CBS Boston,* April 19, 2013.
[59] Peter Finn, "Tsarnaev brothers' homeland was war-torn Chechnya," *Washington Post,* April 19, 2013.

2011. The file contained information linking Tamerlan to radical terrorists that were active in Chechnya.[60] The filed provided strong evidence that Tamerlan communicated with these radicals on a regular basis. PRISM should have already collected this data because the communications took place across international borders and were between Tamerlan and known terrorists. Regardless, the FBI opened an investigation based on the Russian intel. They interviewed Tamerlan but found no evidence of any radical ties and could not order a warrant for wiretapping or a seizure of his computer to check for overseas communications.[61] The FBI did order Tamerlan to be placed on the Terror Watchlist with a special note to detain at the airport if he tried to leave the country. However, he was entered into the database as Tamerlan Tsarnayev, instead of Tsarnaev.[62] This human error turned out to be vitally important. On January 21, 2012, Tamerlan boarded a flight in New York City for Moscow. Once there, he traveled to Chechnya where he received jihadist training for six months until returning to the United States on July 17, 2012. The misspelling of his name prevented an alert from firing either time he passed through American airports.[63] Human error clearly played a huge role in not catching Tamerlan's radicalization until after the attack. However, mass surveillance also failed the American public in this case.

Mass surveillance failed on three separate occasions in the years preceding the Boston Marathon attack. The first has already been discussed above. Russian intelligence agencies clearly knew Tamerlan communicated with Islamic radicals overseas. PRISM was designed to catch these exact types of online communications. Some of these communications must have

[60] Tom Winter, "Russia Warned U.S. About Tsarnaev, But Spelling Issue Let Him Escape," *NBC News*, March 25, 2014.
[61] Ibid.
[62] Ibid.
[63] Ibid.

taken place on a platform owned or operated by one of the nine tech giants involved in the PRISM program. Secondly, mass surveillance systems should have captured Tamerlan's communications with whoever his contacts were in Chechnya that provided him jihadist training. The identities of these terrorists and the extent to which they talked to Tamerlan before his arrival remains classified. He clearly talked to someone, or he would have had no idea where to go in Chechnya to receive jihadist training. PRISM should have collected this data as well. Finally, after returning from Russia in 2012, Tamerlan showed increasing signs of radicalization online. He posted videos of known terrorist Abu Dujana to his Youtube channel in 2012.[64] We know the NSA had access to this information because Youtube joined PRISM in the winter of 2010. Additionally, his online presence in general, from other Youtube videos to Facebook posts, appeared to show a strong increase in radical thoughts after he returned to the United States from Chechnya. Once again, we know PRISM collected all this data. It simply did not set off the algorithms that would have led to further investigation. Traditional and mass surveillance both made mistakes in the investigation of Boston Marathon attacker Tamerlan Tsarnaev. However, the mistakes made by the FBI could have been completely nullified if mass surveillance systems worked effectively.

San Bernardino

The third and final case study is the San Bernardino, California terrorist attack that took place on December 2, 2015. Married couple Syed Rizwan Farook and Tashfeen Malik carried out the attack at the San Bernardino Health Department where Farook worked. The couple arrived during a training session armed with an arsenal of automatic weapons and opened fire.

[64] Tim Lister, "Dead Boston bomb suspect posted video of jihadist, analysis shows," *CNN*, April 22, 2013.

The pair killed 14 people and wounded 22 others.[65] Farook and Malik appear to have plotted numerous attacks during their marriage, but chose to carry out this one because a Christmas party was scheduled to take place after the training session. The extremely radicalized pair felt that the Islamic Farook should not have to participate in the party.[66] This case provides the strongest evidence that PRISM, and mass surveillance in general, does not work. The couple expressed radical beliefs online numerous times, yet they were never placed on a watchlist or the subject of a preliminary investigation. The attack came as a complete surprise to all levels of law enforcement.

In its post-attack investigation, the FBI uncovered several instances of long term planning by the couple. Farook appears to have planned attacks with longtime friend Enrique Marquez as far back as 2012.[67] This was before he even knew Malik. Marquez extensively cooperated with authorities after the attack. He suffered from serious mental health issues and Farook drew him in with radical teachings. He gave no explanation for why they called off their planned attack except for Farook changed his mind. Marquez sold two assault rifles used in the attack to Farook years before the San Bernardino attack took place.[68] This stockpiling of weapons and early planning shows that Farook was almost certainly completely radicalized by the time he met Malik.

Tashfeen Malik was born in Pakistan but lived in Saudi Arabia most of her life. She and Farook met on an online dating site in the summer of 2013. They began extensively emailing one

[65] Mark Berman, "One year after the San Bernardino attack, police offer a possible motive as questions still linger," *Washington Post*, December 2, 2016.
[66] Ibid.
[67] Michael S. Schmidt, "San Bernardino Couple Spoke of Attacks in 2013, F.B.I. Says," *New York Times*, December 9, 2015.
[68] Ibid.

another almost immediately and seemingly quickly fell in love. Both told their respective families about the rapidly developing relationship.[69] However, a darker relationship emerged alongside the romantic attachment. The FBI uncovered several emails between the couple that expressed each one's desire and support for "jihad and martyrdom."[70] Their radical beliefs appear to have been part of the catalyst that led to the quick bond between the two. The FBI uncovered no emails specifically mentioning an attack the two planned to carry out together, but the correspondence showed a definite support for violent extremists. This type of talk continued for the three to four months the couple carried on an exclusively online relationship.[71] There is no question that these emails should have been intercepted by PRISM and raised a red flag via the anomaly detection algorithm.

Farook and Malik decided they wanted to meet in person. Farook traveled to Saudi Arabia in October 2013 to make his pilgrimage to Mecca and meet Malik. According to her immigration file, the two confirmed their love for one another and agreed to marry. She immediately began the process of applying for a visa to move to America with Farook.[72] She received instructions to travel to the United States consulate in Saudi Arabia for her visa interview to determine whether the relationship was real or simply a ploy to get her into the United States. She clearly knew Farook very well from their online communications and easily passed the interview and legally entered the United States on July 27, 2014. Her interview

---

[69] Justin Fishel, "Inside the Immigration File of San Bernardino Shooter Tashfeen Malik," *ABC News,* December 22, 2015.
[70] Michael S. Schmidt, "San Bernardino Couple Spoke of Attacks in 2013, F.B.I. Says," *New York Times,* December 9, 2015.
[71] Ibid.
[72] Justin Fishel, "Inside the Immigration File of San Bernardino Shooter Tashfeen Malik," *ABC News,* December 22, 2015.

contained no questions about radical beliefs or jihadist support.[73] National security agencies had no way of knowing they authorized a potential terrorist to live in the United States. Mass surveillance systems designed to uncover these type of communications failed to identify Malik or Farook as extremists.

Farook and Malik married in August 2014, less than a month after Malik entered the country. After their marriage, they seemed to have begun preparing for an attack fairly quickly. Farook began slowly acquiring weapons from different places. He purchased some from friends and others from gun stores, but all were acquired legally. By the time the attack took place, Farook and Malik each had assault rifles, semiautomatic handguns, bulletproof vests, and nearly 2,000 rounds of ammunition.[74] This is an enormous stockpile of weapons and ammunition the couple purchased legally and without questioning from authorities because they were never placed on a watchlist. Additionally, the couple carried fifteen "pipe bombs" in their car on the way to the attack. They made these devices in their garage but never deployed them during the attack. Investigators speculate that the couple planned to carry out another attack after the first but were killed by police too quickly.[75]

Officials have still not determined a motive for the attack. Malik posted to Facebook just before the attack began and pledged allegiance to ISIS on behalf of her and her husband.[76] This led investigators to believe the couple were in contact with someone in ISIS that directed the attack. The investigation yielded no firm proof of this mystery connection with an ISIS member.

---

[73] Michael Martinez, "San Bernardino shooting: Couple radicalized before they met, FBI says," *CNN*, December 9, 2015.
[74] Sari Horwitz, "Guns used in San Bernardino shooting were purchased legally from dealers," *Washington Post*, December 3, 2015.
[75] Ibid.
[76] Mark Berman, "One year after the San Bernardino attack, police offer a possible motive as questions still linger," *Washington Post*, December 2, 2016.

However, the couple extensively watched ISIS propaganda, attack videos, and radical teachings.[77] This led officials to conclude that Farook and Malik were inspired by ISIS but not directly commanded by the organization. This determination helps when evaluating the effectiveness of surveillance in the case. Traditional surveillance was almost nonexistent in this case. The FBI would have needed a neighbor to see the couple making bombs to truly have a chance of stopping the attack via traditional means. This attack shows the limits of traditional surveillance as currently constructed. Mass surveillance failed entirely in this case. The couple discussed jihad and a desire to become martyrs via email messages sent from California to Saudi Arabia for months. The couple then viewed radical texts and videos online. These actions are the definition of a cluster algorithm red flag. PRISM utterly failed in the San Bernardino case just as it did in Orlando and Boston. The remainder of this paper will discuss how to fix these issues and create a more effective and efficient surveillance system that better protects Americans.

V. My Plan

This research has provided strong evidence that traditional surveillance methods are more effective than mass surveillance systems even in the internet age. The 20 percent success rate of mass surveillance system versus the seventy-one percent success rate of traditional methods clearly demonstrates a large gap in effectiveness. The case studies of the attacks in Orlando, Boston, and San Bernardino illustrate the missed opportunities of PRISM and mass surveillance. Mass surveillance did not fail because terrorists took unforeseen actions and outsmarted the programs. It failed because the mass collection of trillions of pieces of data builds too large of a haystack for any program, no matter how complex, to effectively and efficiently search and

[77] Ibid.

analyze. This research leads me to advocate for a two-pronged plan to improve American surveillance and raise the seventy-percent success rate. The first thing that must change is the usage of mass surveillance technology. Mass collection does not work, but the technology of PRISM could be extremely effective if used to monitor only certain websites and areas of the internet. This change would also make the technology more efficient and less of a drain on important national security resources. Secondly, the laws and regulations that govern FBI terror investigations must change. The FBI leads these investigations on the ground, yet they have more restrictions than any other national security agency. It is important that lawmakers give the FBI the ability to succeed in investigations. These changes could have made huge differences in Orlando and Boston.

ISIS changed the way terrorist organizations use the internet. In the years just after 9/11, mass surveillance may have been necessary to find online conversations between terrorists because the internet was not very well understood by the average person looking to connect with al-Qaeda or by al-Qaeda themselves. This statement is not true with ISIS. The organization understands how to spread propaganda online and find recruits around the world using the internet. PRISM and other mass surveillance programs need to be refocused on just these areas of the internet. For example, in 2014 at the height of its terror campaign, ISIS posted a video to one of its countless chatrooms explaining how to make a bomb and set it off in Times Square.[78] The New York City Police Department was extremely concerned with the video, but they had no way of knowing if any potential radicals in the city watched the video. This information must be made available to the FBI and other law enforcement agencies immediately. Under the current system, these agencies need to wait for PRISM to raise a red flag on someone who watched the

[78] Thomas Tracy, "ISIS has mastered social media, recruiting 'lone wolf' terrorists to target Times Square: Bratton," *New York Daily News,* September 17, 2014.

video to begin an investigation. As we have seen, these flags could be raised too late or never raised at all. Important information gets lost in PRISM's immense haystack.

I propose drastically reducing the size of the haystack. PRISM should collect data only from these chatrooms, extremist run social media accounts, and radical Youtube channels that promote jihadist teachings. There is no precisely determined figure for exactly how many chatrooms and social media accounts ISIS and other terrorist organizations have at their disposal, but it is a substantial number. These sites are also not hard to find using just an elementary Google search. PRISM should be geared towards monitoring the communications on these websites and determining whether any IP addresses found on the site originate in the United States. If they do, a preliminary investigation should be immediately opened into the owner of that IP address. It may turn out to just be a curious American citizen that stumbled upon the site, but every potential threat must be taken seriously. This method would surely raise more red flags and start more investigations. Mateen, Tsarnaev, and Farook and Malik would all have been detected if mass surveillance technology shifted to function in this manner.

The haystack must become more searchable. It is certainly possible that potentially important information could be missed if these programs became so targeted on a few very specific websites. However, I believe the trade-off is worth it for three reasons. First, the current methods collects everything, but has become so big it cannot be efficiently searched which leads to mistakes and failure. Second, it is important that the FBI be given a chance to succeed with traditional surveillance methods as these have proven to be the most effective in stopping terrorism. This increased presence in key areas of the internet would start more preliminary investigations and place the onus on traditional surveillance to find the true radicals and prevent terror attacks. Third, the smaller haystack would mean less "accidental" collection of innocent

citizens' data. This is important because it would make the program more efficient, but it would also help build trust between the government and the people. The Pew Research Center found that 53 percent of Americans strongly disapprove of the government conducting surveillance that collects their data.[79] Pew also found in a 2015 study that only 19 percent of people trust the federal government.[80] It seems likely that the strong opposition to government surveillance plays a role in the high level of distrust. As we have seen, the FBI relies heavily on informants and tips when conducting a terrorism investigation. The FBI could be losing potentially valuable informants because those citizens do not trust the government anymore.

The second prong of my plan is a change to the laws overseeing FBI investigations and reducing the bureaucracy in national security. The first step must be increasing the length of preliminary investigations from six months. The National Institute of Justice studied terrorist planning methods in 2008. They found that almost 20 percent of terrorists planned for attacks longer than six months. This timeline begins when the terrorist selected a location for the attack until the attack was carried out. It did not include the time spent looking for locations or becoming radicalized.[81] The six-month time limit on FBI investigations provides too small of a window for the FBI to use undercover agents and traditional methods to find evidence. Potential terrorists have to avoid making a mistake for only half a year to be free from surveillance. If the limit extended out three years, the FBI would have been notified of Omar Mateen purchasing assault rifles in Orlando and could have prevented the attack. Three years seems like long

[79] Lee Rainie, "Americans feel the tensions between privacy and security concerns," *Pew Research Center,* February 19, 2016.
[80] "Public Trust in Government: 1958-2015," *Pew Research Center,* November 23, 2015, http://www.people-press.org/2015/11/23/public-trust-in-government-1958-2015/.
[81] Brent Smith, "A look at terrorist behavior: How they prepare, where they strike." NIJ journal 260 (2008): 3.

enough for any planning to be detected. Bin Laden only began planning for 9/11 in 1999. The largest terror attack in history took under three years to plan.[82] This information led me to choose three years as the appropriate length for FBI investigations and terrorist watchlist placement.

The bureaucracy involved in national security matters must be reduced. There are currently 17 federal agencies involved in national security intelligence.[83] This number is bloated and contributes to the inefficiency of American counterterrorism efforts. These 17 agencies should be contracted and merged into two national security agencies. One of the new agencies should combine the intelligence communities of all military branches under one umbrella. The military pursues different objectives in the fight against terrorism than domestic agencies do. It seems fairly straightforward to consolidate all the branches' intelligence communities together to foster more communication and intelligence data sharing that could save the lives of American troops.

The other new agency should combine all the non-military intelligence agencies under one umbrella. The FBI or NSA makes the most sense to head this new organization as these two agencies are the most involved in current counterterrorism efforts. This consolidation would give investigators on the ground access to all electronic information collected instead of having to request information from different agencies that are not directly involved in the investigation. Most importantly, it would allow one intelligence community leader to establish one terrorist watchlist instead of each agency investigating different people that show up on their specific radar. This would allow all government resources to be directed at each potential terrorist. This would hopefully eliminate mistakes like the misspelling of Tsarnaev when names are passed

---

[82] "9/11 panel: Al Qaeda planned to hijack 10 planes," *CNN,* June 17, 2004, http://www.cnn.com/2004/ALLPOLITICS/06/16/911.commission/.
[83] Nina Agrawal, "There's more than the CIA and FBI: The 17 agencies that make up the U.S. intelligence community," *LA Times,* January 17, 2017.

between agencies. The intelligence community would become more streamlined and vital information could be shared quickly and efficiently.

VI. Conclusion

Mass surveillance arose to ensure that terror attacks like 9/11 never happened again. It appears that programs such as PRISM have succeeded in stopping terrorist attacks only 20 percent of the time since 9/11 happened. Regardless of the legality of the mass surveillance or its social implications, the success is all that truly matters. The facts show that mass surveillance does not work. Traditional surveillance methods that existed long before 9/11 succeed over 70 percent of the time. This success rate occurred despite significant intelligence community resources being diverted to pay the roughly $100M annual operating cost of PRISM. These resources should be diverted back to traditional surveillance methods that are proven to work. Mass surveillance technology can still be useful, but only in a restructured role that aims to help traditional surveillance.

Mass surveillance technology must be directed towards collecting data only from very specific areas of the internet that potential terrorists are likely to visit. It must collect data from jihadist chatrooms, ISIS propaganda videos, and videos of extremist teachings. Additionally, the laws governing national security investigations must be changed. The length of a preliminary terrorism investigation should be lengthened from six months to three years. This would allow intelligence agents time to properly look through data and set up stings and the use of informants. Terror investigations are too important to mess up because of time constraints. The intelligence community needs time to do a thorough job that leads to the apprehension of terrorists. Finally, the intelligence community needs to be streamlined into two agencies. One

agency should focus on military intelligence that meets the armed forces' unique, strategic objectives. The other agency should include all domestic national security agencies. It should focus solely on keeping the American people safe from terror attacks. These changes would increase both the efficiency and effectiveness of American domestic counterterrorism.