2017

Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and NSA Have, Can, and Should be Doing

Sergio Suarez

Sergio Suarez

Is America Safer? The USA FREEDOM Act of 2015 and what the FBI and NSA have, can, and should be doing.

This paper will delve into the provisions of the USA Freedom Act of 2015 which was signed into law by President Obama on June 2 2015. The analysis will look into whether the changes will enhance or detract from the United States National Security posture and how U.S. Intelligence agencies should conduct surveillance going forward.

Introduction

The USA FREEDOM Act of 2015 ushered in a wave of new provisions which significantly curtailed the manner in which intelligence was to be collected in the United States. In doing so, President Obama and the United States Congress seemed to heed to demands of privacy advocated which believed that surveillance on American citizens no longer comparted with the U.S. Constitution and thus infringed on basic civil liberties. Possibly lost in this debate was the effect that these changes would have on surveillance on the internet. While much of the USA FREEDOM Act targets what has come to be known as "dragnet" collection of phone calls, it did little to change the type of surveillance that is done over cyberspace.

This piece will explain why the USA FREEDOM Act negatively affects the intelligence community's ability in detecting future attacks on the United States. While legislators significantly curtailed telephone surveillance, they need to ensure that any fundamental change to internet surveillance goes through robust public debate to ensure informed decisions.

Following the leaks of the National Security Agency's various surveillance programs, Congress attempted to reform the method in which surveillance was conducted domestically. In doing so, the USA FREEDOM Act prescribes certain restrictions on what and how intelligence agencies can collect information on. After various failed attempts, Congress was able to craft a bill which seemed to answer many of the critics concerns. One important question needs to be asked, – Is America Safer?

In answering this question, this paper will consist of four parts. Part I will focus on the history of surveillance laws in the United States. The section will highlight and focus on the intelligence legal restraint that existed between analyst and law enforcement officials in regards to information

sharing. Prior to the terrorist attacks of September 11, 2001, analyst in the NSA primarily worked through a patchwork of surveillance laws, which restricted the ability for the agency to conduct domestic surveillance. During the time when the Foreign Intelligence Surveillance Act was passed, there was a concern within the American public that the National Security Agency could be used as a political tool to spy on opposition parties. Thus, the law was enacted to curtail the power to gather intelligence on individuals located within the United States.

Part II will focus on current legislation and executive action effecting government surveillance. From 2008 through 2014, various attempts were made to either expand or retract the ability for the intelligence community to collect data. This contemporary phase of surveillance began in 2001 with the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). As the name suggests, the law radically expanded the parameters from which the NSA and FBI could conduct domestic and foreign surveillance over internet and via telephone. Following the rapid expansion and subsequent questioning of the constitutionality, the overall surveillance apparatus changed due to various amendments and other pieces of legislation.

Part III will focus on the current role of the federal courts in the surveillance debate. The judiciary has been on the forefront in determining the legality of the executive branch's surveillance program. There are several cases currently litigated which could dramatically change the type of information collected absent further legislative action.

Part IV will delve into the provisions of the USA FREEDOM Act of 2015. The overall argument centers on the theory that the current state and need of intelligence investigations are incompatible with the provisions of this Act. The law fails to take into account the nature of current threats. In particular, current threats often use the internet and encrypted telephone signals to

inspire, recruit, and communicate. The analysis explains how the provisions will impede certain investigations, and offer recommendations on a current solution. Policymakers must ensure that the surveillance is robust enough to mitigate threats but tailored enough to comport with the U.S. Constitution.

Part I. - Was America Safe? The history of surveillance in the United States

Communication networks inevitably play a vital role in our daily lives. Millions of Americans use these systems to conduct business transactions and communicate via the telephone and internet each day. [1] Although the intricacies of these systems may differ, they all share one common thread: they are global communications networks in which users send, receive, and store information at an astronomical pace[2]. However, as history has shown us, these very networks have the potential to inflict physical destruction. Much like crime in the physical world, computer networks used to commit crimes often, provide clues and evidence which when studied, provide a blueprint to prevent future crime. The increasing sophistication and use of communication systems to commit certain crimes prompts law enforcement to familiarize itself with these platforms.[3]

The purpose of this section is to provide a brief history of surveillance in the United States. Prior to the turn of the 21st century, surveillance was conducted under a patchwork of laws which were difficult to decipher and even more difficult to implement. A basic framework is necessary in order to understand the effects of subsequent legislation. An understanding of surveillance laws

---

[1] See generally Manuel Castells, The Rise of the Network Society (2000); Frances Cairncross, The Death of Distance: How the Communications Revolution Will Change Our Lives (1997).

[2] Orin S. Kerr; "Internet Surveillance after the USA Patriot Act: The Big Brother that Isn't" North Western University Law Review.

[3] See U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations, at vii (2001) [hereinafter CCIPS Manual] ("The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers."), available at www.cybercrime.gov/searchmanual.wpd

is primarily concerned with answering the following question; who can collect the data and where is it located? The answers to these questions are crucial in understanding the policy behind the restrictions.

The disclosures of former NSA contractor Edward Snowden created a cloud of distrust amongst the American public. Congress attempted to reply but could not come to a solution to satisfy both the intelligence community and privacy advocates. The reaction prompted the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (USA FRERDOM) Act of 2015, which radically curtailed the ability of the U.S. government to collect metadata without specific judicial authorization. The law also affected the type of data collected and the location of said collection. However, before we understand where we are going, we must first understand where we came from.

A. Where did we come from?

Diplomatic advantage is at its very core, a battle between nations. In order to win this battle, it is necessary to have adequate information to guide the actions of a nation state. According to the Defense Security Service, agents of adversarial intelligence services target American information or assets by attempting to enlist the cooperation of a US citizen who has legitimate access to classified information.[4] In an attempt to stop and punish this activity, the FBI, DSS, and NSA engage in intelligence collecting operations in order to identify and prevent the unauthorized release of information critical to US National Security.[5] As is the case with any law enforcement

[4] Davis R. -"Striking The Balance: National Security Vs. Civil Liberties" (2003) Brooklyn Journal of International Law Defense Personnel Security Research Center – "Espionage and other compromises of National Security Case Summaries from 1975 to 2008" (2009)

[5] The NSA, FBI, and DSS conduct counterintelligence missions have all been combined under the Office of the Director of National Intelligence National Counterintelligence and Security Center. The mission of the center is to lead and support the counterintelligence and security activities of the US government, the US Intelligence Community, and US private sector entities who are at risk of intelligence collection, penetration or attack by foreign and other

operation, the personnel must adhere to current law to ensure that the information that is gathered during an investigation can be used in a later criminal prosecution.

For instance, in order for the National Security Agency to conduct surveillance on individuals within the United States, the NSA must satisfy the requirements set forth in various federal statutes. One of these statutes is the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801 et seq.). This law established a special court, the Foreign Intelligence Surveillance Court ("FISC"), which is tasked with reviewing the government's applications relating to electronic surveillance.[6] FISA was a law passed in 1978 and dictated the original procedures for physical and electronic surveillance collection of foreign information between foreign agents and agents of a foreign power. [7] American citizens can get caught within the jurisdiction of FISA if they are engaged in suspected espionage or terrorist activities.[8] The Foreign Intelligence Surveillance Act was the result of Senate Committee investigations into the legality of domestic intelligence following former President Nixon's usage of federal resources to spy while in office. [9] The acts purpose was to provide judicial and congressional oversight of the government's surveillance activities of foreign agents and other individuals located within the United States. [10]The law originally allowed surveillance for up to one year absent a court order so long as the surveillance would not acquire the contents of any communication to which a United States person was a party. [11] If however a

---

adversaries. The Defense Security Service counterintelligence mission is to identify threats to U.S. technology and programs resident in cleared industry and articulates the threat to stakeholder. *See http://www.dss.mil/ci/index.html; see also https://www.fbi.gov/about-us/investigate/counterintelligence; see also http://www.ncsc.gov/*

[6] the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511

[7] Id.

[8] Id.

[9] The Church Committee and FISA (Oct. 26, 2007), http://www.pbs.org/moyers/journal/10262007/profile2.html

[10] the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511,

[11] Id.

United States person is involved, the law mandated judicial authorization within 72 hours of the commencement of the operation.[12]

The court also has the authority to oversee request for surveillance warrants by the Federal Bureau of Investigation against suspected foreign intelligence agents and possible spies operating inside the United States. [13]

Subsequent amendments to FISA have attempted to curtail the power of the FISA court to allow orders which amount to warrantless surveillance. In *U.S. v Squillacote*, the United States Court of Appeals for the Fourth Circuit held that electronic surveillance of a "U.S. person" can only be authorized by a FISA court judge if there is 'probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power'.[14] At this time, applications to the FISA court had to contain:

> [A] statement of reasons to believe that the target of the surveillance is a foreign power or agent of a foreign power, specified information on the implementation of the surveillance, and a certification from a high ranking executive branch official stating that the official "deems the information sought to be foreign intelligence information" and that the information sought cannot be obtained by other means"[15]

The court further explained that in order for the FISA court to issue an order authorizing the targeted surveillance of a United States person when there is probable cause that the target of the surveillance is a foreign power or agent of a foreign power.[16]

---

[12] Id.
[13] Id.
[14] U.S. v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000).
[15] Id.
[16] Id.

As the war on terror intensified, so did the need for intelligence collection. Following the disclosure of a warrantless surveillance program authorized by President Bush, Congress passed the Protect America Act of 2007. The law amended the Foreign Intelligence Surveillance Act by removing the warrant requirement for surveillance of foreign intelligence targets "reasonably believed to be located outside the United States. [17] The law changed the definition of electronic surveillance making it easier for the intelligence community to conduct surveillance on foreign targets. The law defined electronic surveillance in terms of whether that target was "reasonably believed" to be located outside of the United States. [18] This new interpretation of electronic surveillance meant that warrantless surveillance only required that one of the parties be , or reasonably believe to be, international. [19]In practical terms, this meant that electronic communication could be intercepted either when the communication is transmitted to someone outside the United States or coming from someone inside the United States as long as the original target is outside the United States. The law was set to expire in 180 days.

Congress responded to this by passing the FISA Amendment Act of 2008. The FISA Amendment Act of 2008 supplanted past restrictions and provided critically important authority for the U.S. Intelligence Community to acquire foreign intelligence information by targeting foreign persons reasonably believed to be outside the United States. [20] The law added several key provision, one being that the law shielded telecommunication companies from suits for past or future cooperation with federal law enforcement authorities and companies that assist the

[17] Protect America Act, Pub. L. No. 110-55
[18] Id.
[19] Stephen Ross Johnson, Anne Passino; *The Protect America Act: Who Will Protect Us against the protector available at* http://rddjlaw.com/articles/ProtectAmericaAct.pdf
[20] *FISA Amendment Act of 2008*, THE WALL STREET JOURNAL (Jun. 19, 2008), http://www.wsj.com/articles/SB121391360949290049

intelligence community in counterterrorism. [21] The law further reauthorized parts of the expired Protect America Act by allowing for eavesdropping without court approval so long as the government filed its petition within one week. [22] The law also introduced several lawyers of oversight from the Department of Justice and Intelligence Community Inspector General and required regular reporting to both Congress and the FISA Court. [23]

FISA Amendment Act of 2008 would become the preeminent piece of legislation to authorize surveillance outside of the United States.

Part II. Lifting the legal restraints off the NSA

September 11, 2001 ushered in a new dynamic in regards to intelligence in the United States and around the world. A criticism after the attacks stemmed from the inability of various members within the U.S. Intelligence community to exchange information. In response to the increased threat, the legal constraints place on the intelligence community where loosened in order to allow law enforcement agencies to gather information. Although it is now marred in controversy, the warrantless surveillance program executed by the National Security Agency is an example of this reality.

The USA PATRIOT Act would embody the state of surveillance in the United States after 2001. This piece of legislation would set the tone on how surveillance would be conducted, and on how intelligence would be collected. To this end, various existing federal laws were amended

[21]FISA Amendment Act of 2008, P.L. No.110 – 261 (H.R. 6304)
[22] Id.
[23] The act mandated that a report containing methods be sent to congress yearly. Id., see also. http://www.wsj.com/articles/SB121391360949290049;

to allow for increased surveillance. This includes *The Economic Communication Privacy Act*, the *Computer Fraud and Abuse Act*, and the *Foreign Intelligence and Surveillance Act*. [24]

The initial legal foundation for the President's surveillance program was rooted in Article II of the United States Constitution. In sum, Article II of the constitution describes the President's authority when appointing officials, in executing laws passed by the legislative branch, and actions in times of a national emergency. In regards to emergency power, Article II section 2 specifically, states "The President shall be commander in chief of the Army and Navy of the United states"[25] The question of whether the President possess authority to use the military absent a Congressional declaration of war has proven to be poignant debate throughout history.[26] An interpretation of the provision grants the President certain powers when it comes to effectuating policy regarding national security.

With the rise of the internet comes the rise of actors attempting to use the internet to cause harm. Prior to the attacks of September 11, the President's inherent authority under the Constitution was not used to authorize mass surveillance.

The NSA knew the value behind data aggregation and threat analysis during the internet boom. Prior to 2001, the NSA developed a program, code named "ThinThread", to gather information in the digital age. The program would correlate data from financial transactions, travel records, web searches, Global Positioning System (GPS) equipment, and other attributes which analyst could later use in identifying threats. [27]Although the developers sought to intercept large quantities of

---

[24] USA FREEDOM Act of 2015, Pub. L. No. 114-23

[25] U.S. CONST. art II

[26] War Powers, https://www.law.cornell.edu/wex/war_powers, *see also* Louis Fisher, Constitutional Conflicts between Congress and the President, p.249-272 (2007)

[27] Joshua Rothman, *Takes: The N.S.A.'s Surveillance Programs,* THE NEW YORKER, (Jun. 6 2013), http://www.newyorker.com/books/double-take/takes-the-n-s-a-s-surveillance-programs

foreign communication, the sweep also inadvertently collected information on American citizens. [28] The collection posed a challenge since federal law prohibited the monitoring of domestic communication absent a court-mandated warrant.[29] In order to comply with the law, NSA programmers installed privacy controls to "anonymized" American communication until a search warrant authorized the system to search for suspicious patterns. [30]

By the fall of 2004, the metadata collection program was allowed under a different legal theory. . The NSA used Executive Order 12333 as one of its legal justifications to gain access into overseas communication. Executive Order 12333, originally signed in 1981 by President Ronal Reagan, allowed for the "timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons" in regards to the national security of the United States. [31] The order was amended in 2003, 2004, and 2008; expanding the authority for the intelligence community to increase its surveillance.

A. What is going on? Surveillance as we know it

On June 6, 2013, various news outlets reported that the U.S. intelligence community was collecting large amounts of data regarding U.S. citizens. According to those reports, the National Security Agency and the Federal Bureau of Investigations were "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, emails, documents, and connection logs" that enables analysts to track individual movements and their contacts over time. [32] The NSA specifically was collecting data through a sophisticate program

[28] Id.
[29] Id.
[30] Id.
[31] Executive Order 13470 of July 30, 2008. Further Amendments to Executive Order 1233, United States Intelligence Activities Exec. Order No. 13470, 3 C.F.R. 13470 (2008)
[32] Laura K. Donohue, Section 702 and the Collection of Information Telephone and Internet Content, 38 HARV. PP LAW JRL 117, (2015)

called "PRISM" - drawing from Microsoft, Google, Yahoo!, Facebook, Skype, and other large email and social network provider's substantial data such as email, video, voice chat, photos, VoIP, and other metadata that could be aggregated to create and track an expansive digital footprint. [33] As of 2011, an Executive report stated that most of the internet communication obtained by the NSA under Section 702 of the Foreign Intelligence Surveillance Amendment Act of 2008 derived from the PRISM program. [34]

In addition to PRISM, the leak revealed that the NSA was collecting "upstream" communication on fiber cables and infrastructure. This meant that the agency was collection information directly from the servers of U.S. service providers. [35] Using this method, the NSA was able to acquire internet communication as it was transmitted through the "backbone" of the system. [36] The NSA was able to acquire more than 13.25 million Internet transactions though its use of upstream collection. [37]

B. **The FBI and the USA PATRIOT Act**.

Due to the tremendous speed with which the legislation passed, there is very little in the way of legislative history to analyze regarding Congressional intent. Thus far, the only report is the House Judiciary Committee report on House Bill 2975. Upon the most relevant provisions was Section 215 which dealt with Access to records and other items under the Foreign Intelligence

---

[33] Id.

[34] PRISM SLIDES, at 3. 7. [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011). Additionally, PCLOB later confirmed that as of mid-2011, approximately 91% of Internet communications obtained each year came through the PRISM program. PCLOB Report, supra note 2, at 34. 8. James Ball, NSA's Prism surveillance program: how it works and what it can do, GUARDIAN, June 8, 2013, http://www.theguardian.com/world/2013/jun/08/ prismserver- collection-facebook-google [http://perma.cc/TZ3R-NJTH] (including slide entitled FAA702 Operations). 9. [Redacted], 2012 WL 9189263, at *1 (FISA Ct. Aug. 24, 2012), available at http://fas.org/irp/agency/doj/fisa/fisc0912.pdf [http://perma.cc/TP7C-JB9Q];

[35] Section 702 and the collection of International Telephone

[36] Id.

[37] [Redacted], 2011 WL 10945618, at NO n.26.

Surveillance Act. This coupled with Section 702 of the Foreign Intelligence Surveillance Act of 2008 created the legal foundation from which the Federal Bureau of Investigation and the National Security Agency would operate for the next decade.

A measure used by the FBI to gather intelligence is a process known as the issuance of a National Security Letter ("NSL"). Provisions in five federal statutes authorized intelligence official to request certain business record information connected to a national security investigation.[38] The authority to issue national security letters is analogous to the authority to issue administrative subpoenas. [39]

The USA PATRIOT Act expanded the authority granted by existing federal law and created a fifth category[40]. Under the PATRIOT Act, any FBI office around the country was allowed to issue National Security Letters without a court review in order to gather "any tangible" evidence. [41] The law also contained a gag order, which prevented the recipient from disclosing or discussing its content. [42] The constitutionality of National Security Letters was not challenged until 2013. The USA PATRIOT Improvement and Reauthorization Act[43] made the sections subject to judicial enforcement and sanctions for failure to comply with an NSL request or to breach the confidentiality requirements that attach to them. [44]

[38] Charles Doyle, CONG. RESEARCH SERV., RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND (2015)
[39] Id.
[40] Id.
[41] USA PATRIOT Act, P.L. 107-56, §505, 115 Stat. 335-66 (2001).
[42] Id.
[43] P.L. 109-177 and its companion P.L. 108-178 amended the five NSL statues to expressly provide for judicial review
[44] Charles Doyle, CONG. RESEARCH SERV., RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND (2015)

C. The USA FREEDOM Act

Following the leaks relating to the NSA bulk meta-data collection program, policymakers within the legislative and executive branch scrambled to identify and reconcile the release of the information with the potential damage to national security. The President reacted by establishing a Review Group on Intelligence and Communications Technology which was tasked with developing principles for the future of intelligence and national security in light of recent technological changes. [45] The group eventually released a report and recommendations on December 12, 2013.As the report noted, the traditional distinction between foreign and domestic surveillance was becoming increasingly difficult to distinguish. Several recommendations addressed the controversial statute under which the National Security Letters are processed. The board recommended that the NSL procedures resemble Section 215 FISA court orders in order to survive constitutional scrutiny.[46] Additional reforms proposed included: (1) court approval of all NSLs unless it is an emergency circumstance, (2) constrain Section 215 orders to investigations dealing with international terrorism and international espionage; (3) amend NSL statutes to track Section 215 minimization requirements; and (4) require greater oversight and public reporting requirements for both Section 215 orders and NSLs. [47]

On June 2nd 2015, President Obama signed into law the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act. Known as the USA FREEDOM Act, the law significantly reforms past surveillance laws at the center of protracted scrutiny following the revelations by former National Security Agency

[45] LIBERTY AND SECURITY IN A CHANGING WORLD, REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2015)
[46] Charles Doyle, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS (2015).
[47] Id at 5.

contractor Edward Snowden. The law notably revitalized Section 215 of the Patriot Act but added significant constraints. The new law ended the NSA's controversial bulk collection program in its current form by explicitly prohibiting it. In particular, the law limits the ways in which the government collects large amounts of records and adds new transparency measures to the methods used by the government to collect intelligence information. [48]

The law came to fruition after Congress allowed key sections of the USA PATRIOT Act to expire. In Am. Civil Liberties Union v. Clapper, 785 F.3d 787 (2nd Cir. 2015), the Second Circuit Court of Appeals ruled §215 of the PATRIOT Act did not authorize the bulk telephone metadata program conducted by the NSA and FBI.[49] Despite the statutory determination, the court did not specifically address the question of whether bulk surveillance violates the Fourth Amendment of the United States Constitution.[50] The court acknowledged the program's potential benefit, but reasoned that, due to the extraordinary measures, Congress would have to authorize such a program explicitly.[51]

Prior to this decision, the government used the bulk metadata program extensively in order to gain information of suspected national security threats which additionally storing information that it could query later. [52]

In addition to the Section 215 reform, various other provisions of the USA FREEDOM Act vary significantly from the USA PATRIOT Act. While phone number inquiries are still

---

[48] Julian Hattem, *Obama signs NSA bill, renewing Patriot Act powers*, THE HILL, (June 2 2015), http://thehill.com/policy/nation-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers

[49] The court determined that Congress is better positioned than the courts to understand the balance the "intricacies and competing concerns" in protecting national security and pass judgement on the value of the telephone metadata program as a counterterrorism tool. Clapper, F. 3d 787 at 824.

[50] Id.

[51] Id at 821

[52] Jonathan Ernst, *USA Freedom Act vs expired Patriot Act provisions: How do the spy laws differ*, RT, (June 1 2015), https://www.rt.com/usa/264005-freedom-patriot-act-surveillance/

permissible, the law moves the repository from the NSA to the individual phone companies[53], in addition to adding new transparency measures regarding the methods used by the government to conduct surveillance. [54] The law also grants authority to continue the acquisition of foreign intelligence information to a period of 72 hours without a court order. [55]

In order to sustain surveillance and close the intelligence vacuum created by the new law, the NSA developed a functional equivalent. The shift permits the agency to continue analyzing information revealed by email without collecting the content.[56] The program will allow the NSA to gain access to national security related information by collecting data gathered in other countries where the NSA's activities are outside of the regulations promulgated by FISA and jurisdiction of the Foreign Intelligence Surveillance Court.[57]

Due to the current structure of the Internet, U.S. domestic data is often found inside fiber optic cables located in other countries.[58] Although the NSA initially barred its analyst from utilizing American's data that they had been collected abroad, the NSA changed its internal procedures to allow such collection. [59] Under the new law, intelligence agencies would have to

---

[53] Id.

[54] Julian Hattem, Obama signs NSA bill, renewing Patriot Act powers, THE HILL, (June 2 2015), http://thehill.com/policy/nation-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers.

[55] USA FREEDOM Act of 2015, Pub. L. No. 114-23Title VII § (A)(2)(B).

[56] Charlie Savage, *File Says N.S.A. Found Way to Replace Email Program,* NEW YORK TIMES, (Nov. 19, 2015), http://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html

[57] Id.

[58] National Security Agency/Central Security Service, Office of the Inspector General, *Report of the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Pen Register and Trap and Trace Devices,* available at https://assets.documentcloud.org/documents/2511338/savage-nyt-foia-nsa-release-11-10-2015.pdf

[59] Id.

request specific information on a targeted individual in order to connect the investigation to a terror group or foreign nation. [60]

The USA FREEDOM Act also fundamentally changed the method in which NSLs are used. Two federal courts held that the absolute confidentiality requirement and limitation on judicial review violate threaten the constitutionality of NSLs.[61] The law adjusted the NSL's judicial review provision governing nondisclosures requirement by permitting recipients to disclose the extent to which "they have been compelled to comply. [62]

Regarding surveillance, the USA FREEDOM Act precludes the use of NSL authority for bulk collection of communications and financial records.

Prior to these provisional changes, NSLs had been subject to protracted litigation. Two separate federal courts initially determined that NSLs and the prohibition on disclosure did not comport with the requirements of the First Amendment. [63] On appeal, the Second Circuit dismissed the case and remanded it for consideration in light of the amendments to the NSL statutes. On reconsideration, the District Court for the Southern District of New York again concluded that the NSL secrecy requirements violated the First Amendment free speech clause and the separation of powers principles.[64] The Court of Appeals ruled that the government could invoke the secrecy and

---

[60] Jonathan Ernst, *USA Freedom Act vs expired Patriot Act provisions: How do the spy laws diffe*r, RT, (June 1 2015), https://www.rt.com/usa/264005-freedom-patriot-act-surveillance/

[61] Add citation from cases or EPIC website

[62] USA FREEDOM Act of 2015, Pub. L. No. 114-23, 12 U.S.C. 3414(a)(2) "[T]he Government authority shall submit to the financial institution…a term that specifically identifies a customer, entity, or account to be used as the basis for the production of disclosure of financial records"); 18 U.S.C. 2709 (b)("The Director of the Federal Bureau of Investigation…may…using a term that specifically identifies a person, entity, telephone number, or account as the basis for the request…")

[63] Charles Doyle, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS (2015).

[64] John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008), as modified (Mar. 26, 2009)

judicial review authority in a limited, but constitutionally permissible manner. [65] Key to this determination is the time requirement, in this case being a 10 day period, in order to allow the NSL recipient to decide whether to contest the nondisclosure requirement to the judiciary. [66] Thus, the government and the recipient get 30 and 60 days respectfully to decide whether to seek judicial review to lift or enforce the non-disclosure requirement.[67]

After following the proscribed procedure by the Court of Appeals, the Government submitted a declaration of a senior FBI official regarding the continued need for secrecy concerning the NSL. The district court concluded that the Government met its burden[68].

This ruling was in contrast with a ruling regarding NSLs in the Ninth Circuit. This court also ruled the confidentiality and judicial review provisions did not satisfy constitutional scrutiny.[69] However, the court disagreed with the Second Circuit in determining that the constitutionality could not be remedied by the proscribed revisions. The Ninth Circuit reasoned that the statutory language was too clear and that congressional intent was too apparent to apply the Second Circuits framework.[70] The court therefore barred the government from using Section 2709 to issue NSLs and from enforcing the related confidentiality provisions.

Section 501 of the USA FREEDOM Act specifically targets the use of National Security Letters in regards to Bulk collection. This section of the statute eliminates the prospect of Section 215 like bulk metadata collection under NSL authority and revises the procedures for issuing NSL

---

[65] Id.
[66] Id at 879.
[67] Charles Doyle, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS (2015).
[68] Mukasey, 549 F.3d at 885.
[69] In re Nat'l Sec. Letter, 930 F. Supp. 2d 1064, (N.D. Cal. 2013).
[70]Id at 1075.

nondisclosure provisions and for judicial review.[71] It accomplishes this by amending each of the NSL statutes and requires that inquires be limited to specifically identified information rather than the broad request for delivery of 'all…information from a recipients' customer record. [72]

The act further reforms nondisclosure orders by making them available only if the issuing official notifies the recipient of their right to judicial review and certifies that disclosure may result (1) a danger to national security, (2) in interference with a criminal, counterterrorism, or counterintelligence investigation or (3) interference with diplomatic relations of the United states. [73]

A recipient may now disclose to a necessary party in order to execute the order, to an attorney in order to receive related legal advice, and to anyone else approved by the issuance agency. [74] This exception is conditioned upon the recipient's notification of the issuance agency and advising those that are made aware that the nondisclosure requirement is binding on both of them. [75]

Part III. Surveillance Litigation

Prior to lapsing, various courts questioned the statutory interpretation underpinning the surveillance program. In American Civil Union v. Clapper (2nd Cir. 2015), the Second Circuit Court of Appeals ruled that §215 of the PATRIOT Act did not authorize the bulk telephone metadata program conducted by the National Security Agency. Although the surveillance was ruled illegal, the court did not get to the question of whether bulk surveillance violates the 4th

[71] Charles Doyle, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS, pg 5, (2015)
[72] USA FREEDOM Act of 2015, Pub. L. No. 114-23§ 501
[73] Id.
[74] Id at 6
[75] Id.

Amendment of the United States Constitution. The court did acknowledge the potential benefit of a program like this, but reasoned that do to the extraordinary measures; Congress would have to explicitly authorize such a program. It has been noted by the government that the program was used to gain information on suspected national security threats.[76] Despite the 180 day timeline given by Congress[77] ,

On November 9th, 2015, Judge Richard Leon of the United States District Court for the District of Columbia issued an injunction against the National Security Agencies bulk metadata collection program.[78] The decision in Klayman v. Obama, was very narrow as it applies only to specific named Verizon customers.[79] The court reasoned that the plaintiffs are likely to establish that the bulk collection program does violate the 4th Amendment. [80]

The Foreign Intelligence Surveillance Court ruled that Congress' deliberate allowance of an 180 day period following the date of action to suspend the bulk collection program authorized the extension of another warrant. In this case, the government applied to seek a renewal of authority granted by FISC.[81] The specific order was in regards to the production of non-content phone call detail records in bulk to the National Security Agency on an ongoing daily basis pursuant to Title V of FISA. [82] On June 2, 2015, Section 705(a) of the USA FREEDOM Act amended the sunset provisions to change the date from June 1 2015 to December 15, 2019. [83]

---

[76] Jonathan Ernst, USA Freedom Act vs expired Patriot Act provisions: How do the spy laws differ, RT, (June 1 2015), https://www.rt.com/usa/264005-freedom-patriot-act-surveillance/

[77] USA FREEDOM Act of 2015, Pub. L. No. 114-23§ 101 (a)(i).

[78]Cody M. Poplin, *D.C. District Court Issues Injunction in Klayman v. Obama,* LAWFARE, (Nov. 9 2015), https://www.lawfareblog.com/dc-district-court-issues-injunction-klayman-v-obama

[79] Klayman v. Obama, 800 F. 3d 559, (D.C. Cir. 2015)

[80] Id.

[81] In re Application of the F.B.I., No. BR 15-75, 2015 WL 5637562 (Foreign Intel. Surv. Ct. June 29, 2015)

[82] Id.

[83] USA FREEDOM Act of 2015, Pub. L. No. 114-23§ 705 (a)

Part IV. Where we go from here? What the FBI and NSA should be doing

The challenges and scrutiny to U.S. surveillance programs have direct domestic and international consequences. With the expansion of the internet and free trade around the world, governments from various nations have begun to analyze and attempt to solve the difficult balance between privacy and security. Any sound counter-terrorism strategy requires assistance from allied countries. The cornerstone of this cooperation is sharing information. This section will analyze the effects that U.S. surveillance laws have had on allied countries and what the NSA and FBI should be doing going forward.

A. Global effects of U.S. Surveillance

Much of the United States ability to trade information over the internet has centered on a safe harbor. Negotiated under the European Commission's Data Protection Directive, the safe harbor allows United States companies to self-certify compliance with the European Union's data protection law. [84] The certification allows for the transfer of personal data from the European Union to the United Stated without risk of prosecution from European regulators.[85]

The European Court of Justice, concerned with the accused U.S. surveillance services of conducting mass indiscriminate surveillance, invalidated the U.S.-E.U. Safe Harbor scheme which thousands of companies relied on to transfer personal data to the United States.[86] Prior to the Safe Harbor's invalidation, more than 4,500 U.S. companies relied on the agreement to ensure adequate

---

[84] Brendan W. Miller et al., European Court of Justice Invalidates U.S.-E.U. Safe Harbor Agreement, The National Law Review (October 9, 2015), *http://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safeharbor-agreement*

[85] Id.

[86] Liam Tung, *Top EU court sinks Safe Harbor over US spying and rattles tech industry*, ZDNET, (Oct. 6 2015), http://www.zdnet.com/article/top-eu-court-sinks-safe-habour-over-us-spying-and-rattles-tech-industry/

compliance with in personal data transfer. [87] The legal action began following the publications regarding the U.S. mass government surveillance by the NSA that ignited concerns EU data stored by United States companies was under illegal surveillance. [88] The suit specifically alleged that the law and practices of the United States did not offer sufficient protections against surveillance by public authorities.[89] The court determined the safe harbor agreement enabled interference by the United States government and therefore compromises the essence of the fundamental right to privacy under EU law. [90] The court emphasized that data protection regulators in each of the European Union member states should have oversight over the methods used to collect and use online information from their counties citizens. [91] Agreements between big technology companies and the E.U. are expected to receive additional scrutiny which would make it more difficult to transfer European information oversees. [92]

B. Ensuing proper tools are available to combat terrorism; reauthorization of Section 702

As the President has stated, "[T]he Administration will work expeditiously to ensure our national security professionals again have the full set of vital tools they need to continue protecting the county". [93] This will not be possible if Section 702 of FISA is not reauthorized.

---

[87] On October 6, the European Court of Justice invalidated the Safe Harbor privacy pact between the U.S. and the European Union. Brendan W. Miller et al., European Court of Justice Invalidates U.S.-E.U. Safe Harbor Agreement, The National Law Review (October 9, 2015), *http://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safeharbor-agreement*

[88] Id.

[89] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[90] Id.

[91] Currently, there are 28 countries in the European Union; Austria, Belgium, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK. https://www.gov.uk/eu-eea; *see also* Mark Scott*, Data Transfer Pact Between U.S. and Europe is ruled Invalid*, THE NEW YORK TIMES, (October 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0,

[92] Id.

[93] THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY, STATEMENT BY THE PRESIDENT ON USA FREEDOM ACT (2015)

Under the authority of Section 702, the government collects telephone and Internet without obtaining individual warrants for the specific people it targets.[94] Decisions about which telephone and internet communications to collect are made by executive branch personnel with the Foreign Intelligence Surveillance Court overseeing the categories of foreign intelligence the government seeks, the procedures it employs, [95] and its adherence to statutory and constitutional limitations. [96]

Prior to utilizing section 702, the President relied on three legal theories to support a surveillance program: (1) the President's inherent Article II authority as Commander in Chief of the Armed Forces; (2) the 2001 Authorization for the Use of Military Force (AUMF); and (3) the War Powers Resolution. [97] The FISA Amendment Act (FAA) added three Sectionss (Section 702, 703, and 704) which adapted to new technologies.[98] FISA Section 702 empowers the Attorney General and the Director of National Intelligence to authorize, for up to one year, the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information"[99]

Similar to Section 215, there is doubt with the constitutionality of Section 702. Evaluating the constitutionality of Section 702 poses a unique challenge since a relevant Fourth Amendment

---

[94] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON SURVEILLANCE PROGRAM OPERATED PERSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PG 89 (2014)

[95] United States Foreign Intelligence Surveillance Court Rules of Procedure, *available at* http://www.uscourts/rules/FISC2010.pdf.

[96] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON SURVEILLANCE PROGRAM OPERATED PERSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PG 89 (2014)

[97] See, e.g., President's Radio Address, WHITE HOUSE, Dec. 17, 2005, available at http://georgewbush-whitehouse.archives.gov/news/releases/2005/ 12/ 20051217.html [http://perma.cc/Z88M-4CS3]; U.S. DEP'T OF JUSTICE, Legal AUTHORITIES Supporting the Activities of the national Security Agency Described BY THE PRESIDENT (2006), available at http://www.usdoj.gov/opa/ whitepaperonnsalegalauthorities.pdf [http://perma.cc/GL5C T7H2]; Letter from William E. Moschella, Assistant Attorney General, to Sen. Pat Roberts, Chair, Senate Select Committee on Intelligence et al. (Dec. 22, 2005), available at https:// www.fas.org/irp/agency/doj/fisa/doj122205.pdf

[98] Laura K. Donohue, *Section 702 and the Collection of Information Telephone and Internet Content*, 38 HARV. PP LAW JRL 117, (2015)

[99] Public Law 110–261, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Section 702

analysis requires assessing a complex surveillance program, which entails many separate decisions to monitor large numbers of individuals which results in the collections of numerous communications of different types obtained through a variety of different methods.[100] Any Fourth Amendment assessment of the Section 702 program must take into consideration the privacy intrusions and risks together with the limits and protections built into the program that mitigate them. [101] The law has various limitations which help protect civil liberties. For instance, acquisition may not intentionally (a) target a person known to be located in the United States, (b) target and individual reasonably believe to be located outside the United States if the actual purpose is to target an individual reasonably believed to be located in domestic bounds or (c) target a U.S. person reasonably believe to be outside domestic bounds. [102]. The NSA is not allowed to use U.S. person identifiers in conducting queries of upstream data and has a specified retention period. [103]

The core of the program – acquiring the communications of specifically targeted foreign persons who are located outside the United States upon a belief that those persons are likely to communicate foreign intelligence – fits within the totality of the circumstance test for reasonableness as it has been defined by courts. [104] As a general manner, warrantless searches are *per se* unreasonable under the Fourth Amendment, although there are few specifically established and well delineated exceptions to the general rule. [105]While wiretapping and other forms of

---

[100] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON SURVEILLANCE PROGRAM OPERATED PERSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PG 86 (2014)

[101] Id .

[102] Public Law 110–261 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Section 702

[103] The retention period for Internet communications collected through upstream is two years and the retention period for data collected through PRISM is five years. Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, §3(c) (Oct.31,2011)("NSA 2011 Minimization Procedures").

[104] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON SURVEILLANCE PROGRAM OPERATED PERSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PG 88 (2014)

[105] *City of Ontario, Cal v. Quon,* 560 U.S. 746, 760 (2010)(quoting *Katz*, 389 U.S. at 357).

domestic electronic surveillance generally requires a warrant, the Supreme Court has left open the question of whether "safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security" and "the activities of foreign powers" [106] Thus, there may be a "foreign intelligence exception" to the warrant requirement permitting the executive branch to conduct wiretapping and other forms of electronic surveillance without judicial approval. [107] While the Supreme Court has not spoken directly to this exception[108], every lower courts evaluating surveillance has affirmed the existence of a foreign intelligence exception.[109]

The borderless nature of the internet creates a dynamic in which laws that are passed in the United States with regards to surveillance equally effect citizens of allied countries. Additionally, many of our allies themselves are not immune of national security threats. For example, Following an attack on satirical newspaper *Charlie Hebdo*, French lawmakers passed the "*Loi Reneignement"*. Known as the Surveillance Act, the law enables France's intelligence agencies to record calls and text messages using technology, which stores the information for later use. [110] The law does have measures in place that require that the techniques and technologies used to collect intelligence be proportionate to the target. [111] Among other things, the law grants the authority to conduct warrantless surveillance. Although the law enforcement agents must consult

---

[106] *Katz,* 389 U.S. at 358 n.23; *United States v. U.S. Dist. Court for E.Dist. of Mich, S.Div,* 407 U.S. 297, 308 (1972).
[107] PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 of FISA (89)
[108] The 1978 enactment of the Foreign Intelligence Surveillance Act forestalled the question of an exception since the Act established a framework for foreign intelligence surveillance that the executive branch obtains warrant-like orders from the FISA court before engaging in surveillance that falls within the ambit of the statute.
[109] *See United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Botenko, 494 F.2d 592, 605 (3rd Cir. 1974); United States v. Brown, 484 F.2 418, 436 (5th Cir. 1973).*
[110]Steve Dent*, France gets its own 'Patriot Act' in wake of Charlie Hebdo attack*, ENGADGET, (July 24, 2015), http://www.engadget.com/2015/07/24/france-surveillance-act/
[111] Council decision.

with an panel of judges and legislatures before conducting such surveillance, the recommendation of the panel is not binding. [112]

Home grown terrorist are now emerging as an imminent threat to U.S. homeland security. Events such as the Boston Marathon bombing in April 2013 show the threat that is posed by homegrown extremists motivated by the ideologies and objectives commonly propagated by terrorist groups. [113] The difficult for law enforcement and the intelligence community is that face to face interaction with terrorist operatives is no longer a requirement of radicalization. [114] Rather, individual. extremist are increasingly self-radicalizing over the Internet which makes prevention and detection of an attack in its early stages increasingly difficult. [115] Law enforcement will need adequate tools in order to focus on the terrorist manifesting itself within the communities which they are suppose to protec[116]t. Legislators have to deal with the reality that today's threat environment is more defused and as terrorist cells and organizations become more decentralized, they will rely on their ability to inspire homegrown recruits to carry out terrorist attacks. [117] Central to this effort to prevent homegrown extremist is the need for robust domestic surveillance which protects civil liberties and privacy as central fabric to the countries identity.

Lawmakers have made pushes to add privacy amendments in a current spending bill. The lawmakers were seeking to preserve amendments that were previously attached to the House

[112] France gets its own 'Patriot Act' in wake of Charlie Hebdo attack, ENGADGET, (July 24, 2015), http://www.engadget.com/2015/07/24/france-surveillance-act/
[113] Homegrown Islamic Extremism in 2013 The Perils of Online Recruitment & Self radicalization
[114] Id.
[115] Id.
[116] Id.
[117] Identifying Enemies Among Us Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing (18)

passed Commerce, Justice and Science (CJS) and Department of Defense appropriations bills. [118] In order to preserve law enforcement and intelligence capabilities, proposed changes should take into consideration contemporary threats abroad and at home. The amendments at issue in the CJS would prohibit the Department of Justice and the Federal Bureau of Investigation from using federal funds to require technology companies to weaken products for the purpose of back-door surveillance. [119] This is in stark contrast to the calls from intelligence and law enforcement officials on the potential impediment that certain technology can have on intelligence collection. [120]

Another amendment in the same bill would prohibit National Institute of Standards and Technology from using federal funds to consult with the National Security Agency or Central Intelligence Agency for the purpose of setting deliberately weak cryptographic standards that could be used to enable data collection.

If not properly assessed, measures like this could severely hinder investigations over suspected terrorist activity. As of the time of this paper, 71 individuals have been arrested in ISIS related criminal charges.[121] It has become apparent that the United States has become a home for a small but active cadre of individuals infatuated with ISIS ideology. [122] There have been 31

---

[118] Alexei Alexis, Lawmakers Want Privacy Amendments in Spending Bill http://www.bloomberglaw.com/exp/eyJpZCI6IkEwSDZCOVExRjU/anM9MCZzdWJzY3JpcHRpb250eXBlPWJuYWhzZG0maXNzdWU9MjAxNTEyMDMmY2FtcGFpZ249Ym5hZW1haWxsaW5rJnNpdGVuYW1lPWJuYSIsImN0eHQiOiJCQk5BIiwidXVpZCI6IndHbzV3YzVBeU1GbnFpaWdKWERSWnc9PUJ2OXpSeXJkL2R3MnVZR2RINTZ1WWc9PSIsInRpbWUiOiIxNDQ5MTA1ODczMTM0Iiwic2lnIjoiZ2toTEhZMFVyQ0pGT01nRnp1ZEYvM0pJMEk4PSIsInYiOiIxIn0=

[119] Id.

[120] CIA Director John Brennan warned that some technologies "make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it". This echoed concerns of leaders in the FBI and NSA that terrorist are using encryption to hide their tracks. Rob Lever https://www.yahoo.com/tech/s/attacks-revive-debate-encryption-surveillance-034107085.html. Nov. 16, 2015.

[121] Lorenzo Vidino and Seamus Hughes, *ISIS in America: From Retweets to Raqqa,* (Program on Exremesim, The George Washington University), Dec. 2015, *available at https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf*

[122] Id.

plots in the United States over the past seven years, with American citizens and permanent residents having planned or been intricately involved in 26 of them. [123] In the past, plots were directed by foreign terrorist organization and recruitment and planning generally required direct human interaction in order to attack. [124] The advent of the internet has changed this dynamic. Today, the internet provides an opportunity in which individuals can find analogous social networks, inspiration, and encouragement online without having to leave the comfort of their home. Since these interactions do not directly involve communications with individuals outside of the United States, the current legal structure prevents surveillance in a robust way. The domestic terrorist threat requires the same surveillance that international threats receive.

The FBI and NSA should take proactive steps to curtail some of the threats faced today. For instance, social media sites should be required to report activity on its networks, which provide guidance on terrorist activity. The relationship with the government should be comparable to the communication that take place with the private sector and the government to prevent child exploitation. [125] The current intelligence authorization bill attempts to hold internet service providers accountable for the activity that takes place on their servers. Section 603 of the Intelligence Authorization Act for Fiscal Year 2016 requires companies providing an interstate

---

[123] *Homegrown Islamic Extremism in 2013 The Perils of Online Recruitment & Self radicalization*, ANTI-DEFAMATION LEAUGUE, 2014, *available at http://www.adl.org/assets/pdf/combating-hate/homegrown-islamic-extremism-in-2013-online-recruitment-and-self-radicalization.pdf*

[124] Id.

[125] The FBI works closely with Internet service providers and search engine operators to monitor their websites and alert them when they discover illegal activity. They are also working with ISPs to retain records of online activities in order to identify predators and their activities to prosecute them. *See https://www.fbi.gov/news/speeches/child-exploitation-on-the-internet-the-dark-side-of-the-web*

electronic communication service or remote computing service to report to the authorities when they become aware that their technology is used to carry out a potential terrorist attack. [126]

Conclusion

Surveillance in the United States must be tailored to provide security but robust enough to allow law enforcement and intelligence agencies to keep the nation safe. The USA FREEDOM Act does not further safety. Under the new law, investigators can look for links in phone numbers but they must obtain a targeted warrant to get them from phone companies, which generally only keep the records for up to two years.[127] Do to provisions of the USA FREEDOM Act, the Foreign Intelligence Surveillance Court issued an order prohibiting the government from collecting phone records. [128]The law weakens the NSA and FBI's ability to search and identify terrorist plots that may be taking place within the United States during a time when the country is under a prevailing threat.

Executive within the NSA and FBI should ensure that Congress is fully aware of the potential harm that can come from continuing to undermine surveillance. Calls to weaken phone encryption and revive legislation that would require social media sites to inform the government about posts that are deemed to promote "terrorist activity" should be given a chance to be heard. [129]. That is how we can ensure that America will be safe.

---

[126] Intelligence Authorization Act for Fiscal Year 2016, S. 1705m 114th Cong. § 603 (a); see also S.Rep. No. 114-83 (Conf. Rep.).

[127] Ted Bridis, Investigators lost access to NSA-held phone records 4 days before California shootings, Canadian Press, (December 7 2015),

[128] USA FREEDOM Act of 2015, Pub. L. No. 114-23§ 103, 129 Stat. 268,272; *see also id. § 109(a), 129* Stat. at 276.

[129] Dustin Volz, Shooting sharpen debate on U.S. electronic powers, REUTERS, (December 6, 2015) *available at* http://www.reuters.com/article/california-shooting-cyber-idUSL1N13V0HV20151206#iMedrZsbhVVzDKDJ.97