UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30 | Issue 4 Article 5

Summer 2014

Where Has Privacy Gone? How Surveillance Programs Threaten Expectations Of Privacy, 30 J. Marshall J. Info. Tech. & Privacy L. 795 (2014)

Michael Greene

WHERE HAS PRIVACY GONE? HOW SURVEILLANCE PROGRAMS THREATEN EXPECTATIONS OF PRIVACY

MICHAEL GREENE*

I. INTRODUCTION

Suppose you are a member of an unpopular religious organization that has domestic U.S. offices and international affiliates. You may understand that because of your religion others may be suspicious of you, or that others do not trust you. If you were to discover that all of your communications had been wiretapped, stored, and cataloged, and all of these documents and wiretaps and logs were mistakenly delivered to your home, you would be able to sue the government for unreasonable search and seizure.[1] Unfortunately, that was not the case when, in 2012, the Ninth Circuit Court of Appeals in California vacated the judgment in *Al-Haramain Islamic Foundation, Inc. v. Obama*,[2] and dismissed the case when the government invoked the "sovereign immunity"[3] and "state secrets"[4] privileges to cover up a warrantless

* J.D. Candidate, 2015. The author attends the John Marshall Law School and graduated from Eastern Illinois University with a B.S. in Political Science in 2009.

1. Nobody knows how or who sent the documents to the Al-Haramain Foundation. Jon B. Eisenberg, *Suing George W. Bush: A Bizarre and Troubling Tale,* SALON (July 9, 2008), http://www.salon.com/2008/07/09/alharamain_lawsuit/.

2. Al-Haramain Islamic Found., Inc. v. Obama, 690 F.3d 1089, 1089 (9th Cir. 2012).

3. Carrie Newton Lyons, *The State Secrets Privilege: Expanding its Scope Through Government Misuse,* 11 LEWIS & CLARK L. REV. 99, 104-06 (2007).

4. *Id.* (discussing that state secrets is a privilege that was invoked by the Department of Defense in *United States v. Reynolds* in 1953, which the Supreme Court granted, restricting the production of information and materials required for plaintiffs in an acci-

wiretap.[5] Although the Islamic charity in *Al-Haramain* had received documents and logs that outlined the warrantless wiretap of their organization, they were unable to sue the government and ensure protection from overzealous and unconstitutional search and seizure.[6]

Unfortunately, the realization of *Al-Haramain* is not that government agencies possess the technology to conduct such sweeping surveillance, but that even when they are caught and a plaintiff satisfies all requirements to seek a relief, the government can protect itself from such lawsuits by invoking broad protections like "sovereign immunity" or authorizations from intelligence gathering programs.[7] *Al-Haramain* is the first lawsuit that addressed recent changes in the authorization of national intelligence gathering programs. Despite national attention given to this case, intelligence programs operated unimpeded to absorb and catalog information and communications transmitted through the United States.

It is fundamental that private citizens have the ability to challenge the constitutionality of policies and laws that have been enacted and carried out by its representative government. In recent years, and even months, there has been a deluge of information that has shed light on the abilities of national intelligence agencies to gather information and records of the communications made by U.S. citizens. Through information leaks by former workers, it has become known that millions of Americans have been targeted by intelligence agencies with unprecedented access.[8] These agencies have used pressure on communication and service providers to give direct access to secure private communications with impunity. With every new information leak, there is a growing distrust and want for change, but so far plaintiffs do not have the legal ability to challenge these programs.

---

dental death case because the deceased had been involved in a top secret weapons program); *see* States v. Reynolds, 345 U.S. 1, 3-4 (1953).

5. This is against the express statements made by President Obama during his inauguration in which he guaranteed that the use of state privileges would not be continued to stop the prosecution or control of surveillance programs. Joshua Kopstein, *Denied in the Supreme Court, Warrantless Wiretap Opponents are Losing Ground Fast*, VERGE (Mar. 1, 2013), http://www.theverge.com/2013/3/1/4043944/denied-in-the-supreme-court-warrantless-wiretap-opponents-are-losing.

6. The Al-Haramain Foundation was awarded over $2,500,000 in damages and legal fees for warrantless wiretaps, the award was vacated upon appeal and successful invocation by Department of Justice that the suit endangers state secrets and national security. *Id.*; *see Al-Haramain Islamic Found., Inc.*, 690 F.3d at 1089.

7. Kopstein, *supra* note 5.

8. *Everything You Need to Know about PRISM*, VERGE (July 17, 2013), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

Clapper v. Amnesty International USA[9] was the most recent lawsuit addressing national intelligence programs but it met equally challenging results.[10] *Clapper* was dismissed by the Supreme Court of the United States for a lack of showing that the plaintiff was injured by warrantless wiretaps.[11] *Clapper* did not address the important question of whether or not warrantless wiretaps are constitutional.[12] The dismissal created a Catch-22, criticizing secret government programs requires the very information that the government refuses to disclose.[13] Now that these secret government programs have been exposed through leaked classified documents, courts cannot be as dismissive without addressing what so many of these legal battles have been challenging.

This Comment will explore the current National Security Agency (NSA) surveillance programs, their constitutional and legal basis, and the future legislation and litigation that will develop since the leaking of classified documents.[14] Section II will also explore the historical background of the current NSA surveillance programs, which has survived litigation. It will describe how the current Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA) evolved from previous governmental surveillance programs.[15] This section will elaborate on

---

9. *Clapper* was not the first litigation that has gotten as far the United States Supreme Court, but it has been the most scrutinized of all early lawsuits because it happened just before Edward Snowden leaked information detailing the extent of NSA surveillance programs. *See generally* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

10. The respondents in *Clapper* are composed of ACLU attorneys as well as various other groups that represent foreign clients involved in litigation in the United States. Kopstein, *supra* note 5.

11. *Id.* (delivering a 5-4 opinion, Justice Alito stated respondents lacked the required showing that individuals were actually damaged by government surveillance of their communications to establish Article III standing to successfully challenge Section 1881a of the Foreign Intelligence Surveillance Act of 2008); *see Clapper*, 133 S. Ct. at 1143.

12. Kopstein, *supra* note 5 (noting that respondents lacked standing to challenge the Foreign Intelligence Surveillance Act 2008 Amendment, so the Court did not discuss whether the Act violated constitutional separation of powers or the violation of U.S. person's civil liberties); *see Clapper*, 133 S. Ct. at 1154.

13. Kopstein, *supra* note 5 (discussing that the plaintiffs wanted to challenge the Foreign Intelligence Surveillance Act 2008 Amendment and were seeking an injunction to compel the release of information that the Department of Justice was refusing to disclose); *see Clapper*, 133 S. Ct. at 1148-50.

14. Since the initial release and subsequent releases of classified documents established the ways in which information has been collected and stored, there has been a dramatic increase in demanding Congressional Sub-committees by non-committee members to openly discuss how the information is disseminated. *Everything You Need to Know about PRISM*, *supra* note 8.

15. Mark D. Young, *Defense Policy: Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 STAN L. & POL'Y REV. 11, 12-13 (2011).

the different governing bodies that control or implement the various surveillance programs. This historical look will establish how current surveillance programs have grown over the past decade and how the legal framework for justification has been utilized. This section will then describe the current programs that have been discovered through documents leaked to *The Washington Post* and *The Guardian* in June 2013.[16] This section will also outline how these programs obtain information.

Section III will analyze previous lawsuits that have not survived judicial discretion. The lawsuits that were decided were done so before significant information about current surveillance programs and how they operate was revealed. This analysis will look at whether, with this new information, plaintiffs would have been victorious in challenging surveillance legislation, or conversely, whether this new information would still not be enough for plaintiffs to state a claim and seek injunctive relief. The decisions that had been reached in these previous lawsuits stand on shaky ground but may still persuade a different opinion.[17]

Section III will also look at the current state of political and societal fallout from the revealing of the NSA documents. This is important to understand the context in which both sides of the debate must be aware of to ensure equilibrium between national safety and protected civil liberties. This section will also address the current pressure on private organizations that have been linked to the NSA surveillance programs and their attempts at creating more transparency.[18] Next, Section III will address the recently proposed legislation and determine how, if passed, it will address future government surveillance programs and how it can be proactive in limiting different paths that surveillance can go down.[19] Finally, section III will endorse a more rigorous legislative mandate of surveillance protocol then what has been proposed.

---

16. *Everything You Need to Know about PRISM*, *supra* note 8.

17. Kara Brandeisky, *NSA Surveillance Lawsuit Tracker,* PROPUBLICA (July 10, 2013), https://projects.propublica.org/graphics/surveillance-suits.

18. Adi Robertson, *Dropbox Joins the Call for Transparency, Asks Government to Let it Publish Surveillance Requests*, VERGE (Sept. 24, 2013), http://www.theverge.com/2013/9/24/4765660/dropbox-asks-government-to-let-it-publish-surveillance-requests.

19. The legislation that will likely survive the scrutiny required before it will be passed does not accomplish any significant changes to the ability of government agencies to conduct surveillance programs or intentionally target U.S. persons. Sean Hollister, *New Bill Seeks to Outlaw Bulk Surveillance, Shine Light on Secret FISA Court System*, VERGE (Sept. 25, 2013), http://www.theverge.com/2013/9/25/4771878/intelligence-oversight-surveillance-reform-act-constitutional-advocate.

In explaining this proposal, Section III will address both sides of the debate and look at the judicial opinions that have been offered on surveillance programs. This section will explain the pro-surveillance argument of necessity to protect the United States from future terrorist or national security threats as well as the civil liberties argument for ensuring the protection of the right to privacy from over-intrusive governmental surveillance. Moreover, this section will proffer a new standard for reasonableness when discussing future surveillance programs. Finally, section IV will conclude.

II. BACKGROUND

The rapid growth of instantaneous global communication has connected distant lands and fostered the spread of ideas, but it has vastly outgrown antiquated interpretations and protections of privacy.[20] In an increasingly connected world, privacy groups have challenged the moral and legal authority of government agencies collecting and storing private communications.[21] However, these privacy groups have encountered systemic resistance and lacked sufficient legal protection to challenge the governmental authority.[22]

Over the past decade, significant steps have been taken through the executive office to engage in warrantless wiretaps of international communications with the goal of intercepting terrorist organizations.[23] Following the terrorist attacks on September 11, 2001, President George W. Bush determined that the requirements of the Foreign Intelligence Surveillance Act (FISA) were overly burdensome and instructed the National Security Administration (NSA) to intercept electronic communications into and out of the United States, in which there was reasonable belief that one party was a member of or working with Al Qaeda.[24] This secret wiretapping program became known as the

---

20. When the Foreign Intelligence Surveillance Act was enacted in 1978, fax machines were the quickest and most prevalent form of sending and receiving information documents. Young, *supra* note 15.

21. The Electronic Privacy Information Center filed a petition arguing that the Foreign Intelligence Surveillance Court does not have the authority to "require production of all domestic call detail records" in the wake of a leaked court order approving a bulk gathering of Verizon customers' metadata. Adi Robertson, *Privacy Group Challenges NSA Phone Surveillance in Supreme Court Petition,* VERGE (July 8, 2013), http://www.theverge.com/2013/7/8/4504466/privacy-group-challenges-nsa-phone-surveillance-in-supreme-court.

22. Kopstein, *supra* note 5.

23. Anthony M. Schults, Note, *The "Surveil or Kill" Dilemma: Separation of Powers and the FISA Amendments Act's Warrant Requirement for Surveillance*, 86 N.Y.U.L. REV. 1590, 1600 (2011).

24. The expansion of Bush era communication monitoring has increased the ability of the NSA to collect metadata information, even when indiscriminately targeting net-

Terrorist Surveillance Program (TSP), and was claimed by President Bush as a legitimate exercise of authority granted under Article II of the Constitution and supplemented by the Authorization for Use of Military Force (AUMF).[25] President Bush argued that AUMF was authorized by FISA as a statutory exception to limits of wiretapping.[26]

In 2007, Congress passed the Protect America Act (PAA) as a temporary measure to establish procedures for the government to conduct surveillance.[27] PAA authorized warrantless surveillance of foreign communications that were routed through the United States as well as international communications involving U.S. citizens, if the foreign party was reasonably believed to be located outside of the United States.[28] PAA streamlined the NSA's abilities to conduct covert surveillance of communications and transferred the power to approve the international surveillance from the Foreign Intelligence Surveillance Court (FISC) to the attorney general and director of the NSA.[29] Following the adoption of PAA, the FISC's sole role was ex post facto review of government surveillance.[30]

A. THE FISA AMENDMENTS ACT OF 2008

The FISA Amendments Act of 2008 (FAA) was passed and signed into law in July 2008 as an attempt to establish guidelines for government surveillance of communication.[31] FAA codified the PAA and TSP into a sweeping programmatic surveillance program which retained the broad authorization of the Attorney General and NSA to conduct warrantless wiretaps.[32] The FAA authorizes the Attorney General and the Director of National Intelligence (DNI), for up to one year, to target non-U.S. persons reasonably believed to be located outside of the United

---

works that are guaranteed to include U.S. persons. *Id.* at 1601.

25. The rationale of the Bush administration during this period was cavalier at determining whether actions taken to protect national security would ever step too far over the protection of civil liberties. *Id.*

26. *Id.*

27. Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 295-96 (2009).

28. *Id.* at 296.

29. *Id.*

30. *Id.* (noting that the current role of the FISC court is still one of review, however, with recent information leaks, the FISC court has declared that some of their decisions should be released).

31. William C. Banks, *Law at the Intersection of National Security, Privacy, and Technology: III. Focus on FISA: Article: Programmatic Surveillance and FISA: of Needles in Haystacks,* 88 TEX. L. REV. 1633, 1645 (2010).

32. *Id.*

States to acquire foreign intelligence information.[33] The FAA refined the wrinkles of international surveillance by restricting intentional targeting of U.S. citizens and instructed the acquisition of communications must be conducted in a manner "consistent with the fourth amendment to the Constitution of the United States."[34] Furthermore, FAA states:

> The Attorney General, in consultation with the Director of National Intelligence, shall adopt procedures that are reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time . . . to be located in the United States.[35]

In theory, these limitations would protect U.S. citizens from surveillance, but the government cannot reliably know the target's location or his identity.[36] Under the FAA, the Attorney General must submit the procedures it wishes to utilize in surveying targets to the FISC for review.[37] Following the protocol of the PAA and TSP, the FAA allows for blanket surveillance and data mining of any non-U.S. citizens, including those who are neither suspected of terrorism nor any other national security threat so long as the collection of foreign intelligence is a significant purpose of the surveillance.[38] Although the FAA does not allow for targeting a particular U.S. citizen, the FISC can authorize the broad surveillance of all international communications of a geographical location in the United States.[39]

Following the FAA, the government is not required to identify the specific modes, whether through telephone, e-mail addresses, places, or property where the programmatic surveillance will be directed.[40] After a FISC judge approves of the program features, Executive Branch officials authorize surveillance or compel communication carriers to assist in surveillance.[41] It was not known how the NSA or other government agencies collected data and conducted surveillance until the recent

---

33. Section 703(a) establishes the authority of the Attorney General and the Director of National intelligence jointly and specifically states, "reasonably believed" and "to acquire foreign intelligence information." FISA Amendments Act of 2008, 154 Cong. Rec. H 1707, 1721 (2008).

34. *Id.*

35. *Id.*

36. Banks, *supra* note 31.

37. *Id.* at 1645-46.

38. *Id.* at 1646.

39. *Id.*

40. FISA Amendments Act of 2008, 154 Cong. Rec. H 1707, 1721 (2008).

41. Banks, *supra* note 31, at 1646-47 (noting that how these private companies allow access to the information is still classified, because the companies are required to sign non-disclosure policies when presented with a FISC court order to relinquish data).

release of classified materials by Edward Snowden.[42]

B. PRISM

PRISM is the code name for a massive NSA program that allows direct access to nine U.S. technology and communication providers' servers.[43] PRISM is a FISC approved program that collects all foreign communications that pass through U.S. hubs.[44] The goal of PRISM is to acquire Internet metadata, such as phone records or e-mail addresses, and store them in NSA databases that can be cross checked and searched by NSA analysts.[45] PRISM works to sweep a "target's" complete e-mail inbox and outbox, including anyone who is connected to the email address.[46]

While the NSA uses Upstream collection, a physical collection of communications on fiber cables and infrastructure as data flows past, PRISM collects data by using available source codes and authorized security bypasses from private companies.[47] Upstream data is the specific content of phone calls, e-mails, videos, or other communication collected by physically tapping underwater fiber cables.[48] Recently, leaked classified documents described the analysis tools that are utilized by PRISM which include Marina (Internet data), Mainway (call records), Nucleon

---

42. Subsequent information leaks have shown that a "derogatory report" written by a supervisor when Edward Snowden worked as a CIA technician stated he had tried to access classified data that he wasn't authorized to view. Chris Welch, *Before Surveillance Leaks, CIA Supervisor Warned Snowden Could be a Security Risk,* VERGE (Oct. 11, 2013), http://www.theverge.com/2013/10/11/4827542/before-leaks-cia-supervisor-warned-snowden-could-be-security-risk/in/4167369; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

43. Subsequent information leaks show that PRISM works to funnel all Internet traffic into NSA storage facilities with little physical interaction with private company switches instead relying on intermediary pathways outside of company control. Gellman & Poitras, *supra* note 42.

44. *Id.*

45. *Everything You Need to Know about PRISM*, *supra* note 8.

46. Dan Seifert, *Secret Program Gives NSA, FBI Backdoor Access to Apple, Google, Facebook, Microsoft Data*, VERGE (June 6, 2013), http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism/in/4167369.

47. T.C. Sottek, *New PRISM Slides: More Than 100,000 'Active Surveillance Targets,' Explicit Mention of Real-Time Monitoring,* VERGE (June 29, 2013), http://www.theverge.com/2013/6/29/4478572/prism-slides-surveillance-targets-real-time-monitoring.

48. *Everything You Need to Know about PRISM*, *supra* note 8.

(voice data), and Pinwale (video data).[49] While past collection procedures allowed for FISC approval, under the current use of PRISM, real-time data, including when an individual is logged in and where he is located at a precise moment, is being collected and stored.[50]

C. INITIAL LITIGATION CHALLENGING FISA AMENDMENT ACT OF 2008

There has been a great deal of concern over how surveillance organizations have been collecting their information. Past litigation, brought by plaintiffs either seeking injunctive relief to halt electronic surveillance or to compel the disclosure of electronic surveillance programs, has failed to achieve these goals for several reasons.[51] These lawsuits have been dismissed in courts for failure to show standing because of lack of damage suffered through warrantless wiretaps[52] or after the Department of Justice invoked "state secrets" as a defense.[53]

In *Clapper*, plaintiffs sought to compel the release of information to establish that U.S. citizens were wiretapped without a warrant, violating their Fourth Amendment protection from unlawful search and seizure.[54] The plaintiffs' case was dismissed on appeal for lack of Article III standing.[55] Justice Alito delivered the opinion of the court in a 5-4 decision, stating:

> Respondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending. Moreover, even if respondents could demonstrate injury in fact, the second link in the above described chain of contingencies—which amounts to mere speculation about whether surveillance would be under § 1881a or some other

---

49. Sottek, *supra* note 47.

50. *Id.*

51. Brandeisky, *supra* note 17 (noting a collection of lawsuits that have challenged NSA programs with date of filing summary and status).

52. Despite the ACLU representing clients held in Guantanamo Bay as terrorists, the U.S. Supreme Court ruled that they would not have a high enough level of apprehension to believe that their communications were being collected. Kopstein, *supra* note 5; *see* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1149-50 (2013).

53. State secrets is a privileged immunity, invoked only by the government, allowing for the protection of information from being divulged in evidence if it pertains to a matter of national security or reveals sensitive military intelligence. Lyons, *supra* note 3; *see also* Kopstein, *supra* note 5; Al-Haramain Islamic Found., Inc. v. Obama, 690 F.3d 1089, 1092 (9th Cir. 2012).

54. *Clapper*, 133 S. Ct. at 1141. Respondents assert that they suffered injury in fact and it is fairly traceable to Section 1881a of FISA Amendment Act of 2008 because there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted at some point. *Id.*; *see* FISA Amendments Act of 2008, Pub. L. No.110-261, § 122 Stat. 2436 (2008).

55. *Clapper*, 133 S. Ct. at 1140.

> authority—shows that respondents cannot satisfy the requirement that any injury in fact must be fairly traceable to § 1881a.[56]

Justice Alito's opinion focused primarily on the attenuated circumstances that the American Civil Liberty Union's plaintiffs used to show that they had been actively targeted.[57] The plaintiffs argued their interactions with, and legal support of, foreign clients are subjected to monitoring under Section 1881a.[58]

According to Jameel Jaffer, no plaintiffs can show that they have been monitored under this law because of an insuperable barrier to judicial review that requires disclosure of who the government targets—which the government refuses to do.[59] The dichotomy formed by this decision creates a catch-22, requiring plaintiffs to have the very information that they are seeking through the lawsuit. Currently, plaintiffs are required to show that they have been secretly wiretapped to establish that they were harmed.[60] But, plaintiffs wishing to challenge the FISA Amendment Act of 2008 have no way of establishing they have been secretly wiretapped because the programs are highly classified. Without satisfying the standing requirement, plaintiffs do not have the established legal ability to challenge a law. The plaintiffs in *Clapper* were seeking to compel the government to produce the documents detailing the secret wiretaps, which would establish the plaintiff's injury and satisfy the standing requirement.[61] However, in *Clapper*, the Supreme Court ruled that the plaintiffs lacked standing because they could not produce evidence of being secretly wiretapped.[62]

This roundabout reasoning is troubling for two specific reasons. First, Alito's decision relies on the provisions in Section 1881a(b)1-3,

---

56. In *Clapper*, the Court responded to plaintiff's argument, stating:

> 1) The government will decide to target the communications of non-U.S. persons with whom they communicate; 2) in doing so, the Government will choose to invoke its authority under §1881a rather than utilizing another method of surveillance; 3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy §1881a's many safeguards and are consistent with the Fourth Amendment; 4) the government will succeed in intercepting communications of respondents' contacts; and 5) respondents will be parties to the particular communications that the Government intercepts.

Id. at 1148.

57. *Id.*

58. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1140 (2013).

59. Jameel Jaffer argued before the Supreme Court as respondent's counsel. Amy Goodman & Juan Gonzalez, *ACLU Blasts Supreme Court Rejection of Challenge to Warrantless Spying without Proof of Surveillance*, DEMOCRACY NOW (Feb. 27, 2013), http://www.democracynow.org/2013/2/27/aclu_blasts_supreme_court_rejection_of.

60. *Id.*

61. *Clapper*, 133 S. Ct. at 1148.

62. *Id.* at 1148.

which lays out the parameters for targeting persons under FISA.[63] Although these provisions define the limits that U.S. citizens will not be "intentionally targeted," the inclusion of "a person reasonably believed to be outside of the United States" gives significant leeway for the vast collection of information and communications with U.S. citizens or entities.[64] Secondly, Alito stated, "even if respondents could demonstrate that the targeting of their foreign contacts is imminent, respondents can only speculate as to whether the Government will seek to use Section 1881 authorized surveillance (rather than other methods) to do so."[65] Alito reasoned that if there are any possible ways, other than through secret wiretaps, for the government to collect information on a target, the possibility of the secret surveillance was too attenuated for a plaintiff to establish standing.[66] Furthermore, Justice Alito refused to abandon the Supreme Court's reluctance to endorse standing theories that rest on speculation.[67]

Justice Alito next focused on respondent's assertion that the costs and burdens of ensuring that their communications were secure and protected from government monitoring established standing.[68] Justice Alito found that the Second Circuit's analysis improperly allowed respondents to establish standing by asserting present costs and burdens based on a fear of surveillance, so long as the fear is not "fanciful, paranoid, or otherwise unreasonable."[69] Alito was concerned that "an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a non-paranoid fear."[70] Justice Alito relied on the decision in *Laird v. Tatum*,[71] but found that "chilling effects arising merely from the individual's knowledge that a governmental agency was engaged in certain activities . . . armed with the fruits of those activities, the agency might in

63. *Id.* at 1148; FISA Amendments Act of 2008, Pub. L. No. 110-261, § 122 Stat. 2436 (2008); *see also* 154 CONG. REC. H 1707 (2008).

64. § 122 Stat. at 2436.

65. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) (focusing on the older provisions of FISA, which allowed for electronic surveillance of persons so long as probable cause is satisfied).

66. *Id.* at 1149.

67. *Id.* at 1150.

68. Respondents claimed that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations, to talk in generalities rather than specifics, or to travel so that they can have in-person conversations. *Id.* at 1151.

69. *Id.*

70. *Id.* (quoting Second Circuit Judge Raggi, Justice Alito stated "for the price of a plane ticket . . . transform their standing burden from one requiring a showing of actual or imminent . . . interception to one requiring a showing that their subjective fear of such interception is not fanciful, irrational, or clearly unreasonable").

71. Laird v. Tatum, 408 U.S. 1, 3 (1972).

the future take some other and additional action detrimental to that individual" were insufficient to establish the fear required for standing.[72] Justice Alito took a hard line in maintaining the requirements for plaintiffs to establish standing.[73] However, the reasoning based upon the theory that the FISA Amendment Act of 2008 created safeguards for protecting U.S. persons' civil liberties ignored what Justice Breyer called "commonsense inferences."[74]

In his dissent, Justice Breyer focused on how Section 1881a, added to the Foreign Intelligence Surveillance Act of 1978, changed the prior law in three specific ways.[75] First, the FAA "eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed."[76] Second, the FAA "eliminated the requirement that a target be a "foreign power or an agent of a foreign power."[77] Third, the FAA "diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion minimization procedures."[78] Justice Breyer rationalized:

> Thus, using the authority of § 1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that "a significant purpose of the acquisition is to obtain foreign intelligence information," and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved.[79]

Justice Breyer found that some of the respondents in *Clapper* were the kind of plaintiff that could reasonably expect to be monitored

---

72. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013) (mentioning that plaintiffs had a similar incentive to engage in many of the countermeasures that they are now taking under FISA prior to the adoption of the current FISA amendment undermines the ability to establish how much this new "chilling" effect has had on respondents).

73. *Id.* at 1151.

74. *Id.* at 1158 (Breyer, J., dissenting) (Justice Breyer wrote the dissent for which Justice Ginsburg, Justice Sotomayor and Justice Kagan joined).

75. *Id.* at 1156 (focusing on prior reading of the authorities granted under the FAA, Justice Breyer stated before the amendment, the Act authorized monitoring of private electronic communications if the government's purpose was to obtain foreign intelligence, targeting a foreign power or an agent of a foreign power, and designed to minimize the acquisition and retention and prohibit the dissemination of any private information acquired about Americans).

76. *Id.* (noting that this permitted surveillance on a programmatic, not necessarily individualized, basis).

77. *Id.*

78. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1156 (2013) (Breyer, J., dissenting) (noting that FAA removed the FISC authorization of monitoring and gave it a post facto supervisory role).

79. *Id.*

because they have a "strong motive to engage in, and the Government has a strong motive to listen to" the conversations they had with their foreign clients.[80] He insisted that the government's past behavior shows that it has sought, and will in all likelihood continue to seek, any and all information about alleged terrorists, which will include the surveillance of electronic communications conducted by U.S. persons.[81]

The initial litigation of the constitutional legitimacy of the FISA Amendment Act of 2008 was met with swift resistance from the executive branch and the Department of Justice.[82] *Clapper* is the controlling holding and has dealt a significant blow to what privacy advocates believe is an insurmountable hurdle.[83] These lawsuits did not address the balance of privacy and national security. The holding in *Clapper* stopped before discussing the constitutionality of the FAA, which has left fewer chances for subsequent litigation to be presented. The challenge for plaintiffs remains establishing an injury in fact to establish Article III standing.

III. ANALYSIS

In the wake of the terrorist attacks of September 11, 2001, the executive branch set out to bolster the abilities of the various clandestine surveillance organizations that fall under the umbrella of the NSA.[84] As earlier stated, the actions of the executive branch were to swiftly enlarge the breadth and capabilities of these surveillance agencies to collect, store, and seek out information or identify those involved with the terrorist groups or those who had a substantial part in planning or executing the attacks.[85] However, the impact of these newly granted powers has precipitated an extreme backlash from concerned citizens who feel that their liberties had been quickly ignored or abandoned.[86]

---

80. Several of the respondents represented by the ACLU were attorneys who represented persons acquitted of terrorism charges or have conducted research into human rights violations requiring communication by telephone and e-mail with former detainees, lawyers for detainees, journalists, and fixers all over the world. *Id.* at 1158.

81. *Id.* (noting plaintiff Scot McKay states that the Government under the authority of the pre-2008 law "intercepted some 10,000 telephone calls and 20,000 email communications involving his client").

82. *See* Kopstein, *supra* note 5.

83. *See id.* (discussing the recent setbacks privacy advocates have incurred in various lawsuits).

84. Schults, *supra* note 23.

85. *Id.*

86. Up until the Snowden information leaks, the public was relatively unaware of the extent of information gathering. Arik Hesseldahl, *Guardian Editors Debate a Former NSA Lawyer on PRISM, Snowden and Surveillance*, ALL THINGS D (Sept. 20, 2013, 6:43 AM), http://allthingsd.com/20130920/guardian-editors-debate-a-former-nsa-lawyer-on-prism-snowden-and-surveillance/#.

The conflict of these previously secret programs is deeply rooted in a catch-22 of how to ensure fundamental rights of privacy while maintaining national security.[87]

What is required to maintain the protection of privacy and the civil liberties of U.S. citizens is an open forum of debate and a clearly established legal framework for plaintiffs to challenge the substantive processes of NSA surveillance programs collection of information.[88] Public debate is necessary to uphold the nature of why these programs were created in the first place. As Stephen Baker, former general counsel at the NSA, states:

> Doing something through legislation requires that you have an open debate about exactly what limits you're imposing. But if you're going to have an open debate about what limits you're imposing, you're going to have to talk a lot about your capabilities. And the difficulty we have had engaging in intelligence under law has been that the debate has gradually revealed more and more of sources and methods, to the point that it's not clear that we have intelligence under law because we can't gather that much intelligence due to the loss of our sources and methods . . . you have to ask yourself, if I were a target of intelligence, what could I learn from the disclosures to this point? And almost every one of these disclosures allows you to avoid the intelligence-gathering if you're a target.[89]

Therefore, without a public debate or at least discussion of the policies of the various organizations conducting surveillance, the social and political backlash from these programs will undermine the reason for the programs' creation.

A. SUBSEQUENT INFORMATION LEAKS AND THE IMPACT ON ESTABLISHING INJURY IN FACT

In the months following *Clapper*, there has been a deluge of leaked court documents, memos, NSA documents, and other classified information that shows the extent of NSA surveillance programs under the FAA.[90] The leak of PowerPoint slides, detailing how the NSA uses its program PRISM to collect and store communications, by former NSA contractor Edward Snowden, has shown that the threat of U.S. persons being swept up in the broad drag net surveillance conducted is a highly

---

87. When *Clapper* was decided, many in the technology industry and privacy sectors believed that this was the final blow to privacy and that the decision would insulate NSA surveillance programs from further attacks. *Id.*

88. *Id.*

89. *Id.* (Baker defends the actions of the NSA during a debate with editors of *The Guardian* newspaper which has broken much of the Snowden leak and NSA stories).

90. *See* Gellman & Poitras, *supra* note 42.

likely scenario.[91] These leaks and the subsequent backlash since *The Guardian* published the PowerPoint slides have shown enough information for previous plaintiffs to reassert their claims of injury and rechallenge the constitutionality of the FAA.[92] The leaks by Snowden will not be directly addressed in this Comment, but they are important to understand the evolution of the discussion and the increase in public interest.[93]

Prior to the leaked information provided by Edward Snowden, there was information available that should have created enough doubt about the veracity of the government claims that the provisions adopted in the FAA were adequate at protecting U.S. citizens from an unconstitutional search.[94] In a letter sent from the Director of National Intelligence to Senator Ron Wyden on July 20, 2012, Kathleen Turner admitted that on at least one occasion the FISC court held that some collection carried out pursuant to the Section 702 minimization procedures was unreasonable under the Fourth Amendment.[95] The letter continued to state that although the information Senator Wyden wished to discuss was deemed important to national security, it was important to convey that the government "has remedied these concerns and the FISC has continued to approve the collection as consistent with the statute and reasonable under the Fourth Amendment."[96]

Furthermore, on June 5, 2013, *The Guardian* reported that a top secret FISC court order required Verizon Telecommunications to turn over all information on all telephone calls in its systems, both within the United States and between the United States and other countries.[97]

---

91. Seifert, *supra* note 46.

92. Adi Robertson, *The ACLU Wages a Long-shot Legal Battle Against NSA Surveillance*, VERGE (Aug. 30, 2013, 11:40 AM), http://www.theverge.com/2013/8/30/4675934/the-aclu-wages-a-long-shot-legal-battle-against-nsa-surveillance/in/4483763 (addressing the subsequent litigation filed in June 2013 that is trying to revive the case that *Clapper* lost).

93. An entire article can be written specifically on the impacts of Snowden leaking the confidential documents to *The Guardian* and *The Washington Post* but this is beyond the scope of this Comment.

94. Spencer Ackerman, *U.S. Admits Surveillance Violated Constitution at Least Once*, WIRED (July 20, 2012, 4:30 PM), http://www.wired.com/dangerroom/2012/07/surveillance-spirit-law/.

95. Although the letter did not describe how and why the surveillance was deemed unreasonable under the Fourth Amendment, this was the first instance in which a member of the Executive Branch admitted that there had been unreasonable searches done under the FISA programs. *Id.*

96. The statements in the letter describing the remedies taken by the government were a request by the Director of National Security that Sen. Wyden include in his statements to protect against an incomplete and potentially misleading understanding of what has transpired. *Id.*

97. The top secret court order obtained by *The Guardian* shows the first time, under

The order required Verizon to turn over for a period of three months all call detail records or "telephony metadata" and set out the comprehensive list of materials to be included in the metadata.[98] The "telephony metadata" would include the numbers of both parties on a call, location data, call duration, unique identifiers, and the time and duration of all calls that originated or transpired through Verizon's U.S. networks.[99] Also, the FISC court order expressly barred Verizon from disclosing to the public the request for customers' records or the FISC court order itself.[100]

Although under President George W. Bush officials in security agencies had disclosed to reporters the large-scale collection of call records, the leak of this FISC court order was the first time a significant and top-secret document had been revealed.[101] The revelatory nature of this leaked document was the first documented case that FISC orders shifted from the specific targets that had been championed in Justice Alito's majority holding in *Clapper*. As Justice Breyer described in the dissent,[102] FISA programs had evolved to amass as much communications as possible and were doing so indiscriminately targeting U.S. citizens. This shift in how FISA programs have been conducted was an often ignored consequence of giving sweeping abilities that allowed for unwarranted and limitless surveillance.

Proponents for FISA programs have vehemently declared that the information obtained under these FISC orders are vital to national security.[103] They point to the fact that metadata does not include the actual content of the conversations.[104] There has been a focus on the nature of metadata as a new age form of calling records. Proponents suggest

---

the Obama administration, an indiscriminate bulk collection of communication records. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

98. *Id.*

99. *Id.* (noting that the content of the conversations themselves were not included in the information handed over).

100. *Id. (*following the publication of this article, Greenwald and his accomplice were detained by British Intelligence officers that some felt was a direct action of intimidation for his work detailing the surveillance program and as Edward Snowden's contact).

101. *See id.*

102. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1156 (2013) (Breyer, J., dissenting) (stating that the intentional targeting of U.S. citizens lacked the previous protections that were included in the FISA programs prior to the 2008 amendment).

103. Carl Franzen, *President Obama on NSA Spying: Congress has Known about It and Approved for Years*, VERGE (June 7, 2013, 12:22 PM), http://www.theverge.com/2013/6/7/4406416/president-obama-on-nsa-spying-congress-has-known-about-it-and (publishing President Obama's statement that the NSA is not looking at people's names and they're not looking at content).

104. *See id.*

that the collection of location data, calling numbers, and other information that has been requested is not much different than several decades ago when a prosecutor would request the calling data used for in a criminal trial.[105] However, privacy advocates have grown concerned that metadata provides a more real time surveillance that allows a more intrusive invasion into privacy, as opposed to the stance that this is not a serious invasion of privacy.[106] Advocates are concerned because metadata can be quickly accessed and assimilated to give a more current location of targets within the United States that in the past was not possible.[107] The ability to track IP addresses in real time gives a pinpoint location that was never possible when using simple phone records in the past. The concerns are that metadata will be used as a surrogate for location tracking devices.

Also, the leaked Verizon FISC court order highlighted another problem that privacy experts had not expected. Telecommunication, email, and other companies that have been ordered to divulge customer information have also been subject to nondisclosure agreements.[108] Shortly after leaked documents revealed that private tech companies were involved in secret government surveillance programs, these companies sought to divulge to the public the interactions they have had with the NSA programs under FISA.[109] These private companies have come under increasing public pressure to ensure that information and data, vital for personal and business use, has been protected from overreaching government monitoring.[110] The inclusion of these nondisclosure agreements has placed a tenuous strain on the government and its largest supplier of communications and data. Private companies, such as Yahoo, had unsuccessfully fought to stay out of the controversial surveillance program PRISM but reluctantly joined.[111]

---

105. *Everything You Need to Know about PRISM*, *supra* note 8.

106. *Id.*

107. *Id.*

108. Adi Robertson, *Microsoft Moves Forward with NSA Surveillance Lawsuit after Government Negotiations Stall*, VERGE (Aug. 30, 2013, 2:29 PM), http://www.theverge.com/2013/8/30/4676538/microsoft-moves-forward-with-nsa-surveillance-lawsuit/in/4167369.

109. Adi Robertson, *Facebook and Yahoo Join Call for More Government Transparency in New Lawsuits*, VERGE (Sept. 9, 2013, 5:20 PM), http://www.theverge.com/2013/9/9/4712408/facebook-yahoo-file-suits-to-publish-more-fisa-data/in/4167369.

110. *Id.*

111. Sam Byford, *Yahoo Fought Back Against 'Unconstitutional' Government Order Before Joining PRISM: NYT,* VERGE (June 14, 2013, 12:33 AM), http://www.theverge.com/2013/6/14/4429008/before-prism-yahoo-fought-government-order-in-court/in/4167369.

The confidential reports that have leaked since the *Clapper* decision have shown the breadth of personal information that telecom providers are compelled to divulge. This has created two specific problems when viewed through the holding in *Clapper*. First, the use of "reasonably expected" when describing a plaintiff's expectation of being monitored under a FISA program had not been designed to be implemented in a wide spread dragnet surveillance program.[112] Second, although the use of information collected under Section 1881(a) may not be used, the government insists that it maintain its capabilities that would not be present had these programs not been frequently used.[113]

The respondents in *Clapper* argued that their injury was related to the extenuating circumstances of being broadly swept up in the government's monitoring of international communications.[114] The plaintiffs were unsuccessful because these circumstances were deemed to be too remote to justify granting Article III standing and *Clapper* failed to address the constitutionality of the FAA.[115] The Supreme Court's dismissal of respondent's suit can now be viewed as short-sighted. Had the Supreme Court been presented with the information that was leaked or with the acknowledgement by the NSA of its secret spy orders,[116] would there have been a different outcome in *Clapper*?

Yes, there would likely have been a different outcome for *Clapper*, due to the slim majority opinion. But, whether the FISA court programs would have been dismantled or viewed as unconstitutional would still likely not have happened. The recent leaked documents are focused only on the likelihood of a plaintiff suffering an injury that would give the plaintiff Article III standing. However, Justice Alito's opinion declared that even if the plaintiffs in *Clapper* successfully showed that they could have been monitored, the government still had the capability to

---

112. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1156 (2013) (Breyer, J., dissenting).

113. *Id.*

114. The ACLU represented suspected terrorists that are still being held at Guantanamo Bay Cuba, who were detained during the wars in Iraq and Afghanistan. *Id.* at 1140 (Alito, J., majority opinion).

115. The ACLU is providing council to these terrorists in advance of being tried in either civilian or military courts and the communications that have been collected has caused concern that they will not be able to adequately represent their clients if information vital to trial preparation is recorded. *Id.* at 1156 (Breyer, J., dissenting).

116. James R. Clapper, head of the NSA, announced that the NSA would be unveiling the total number of orders issued over the course of the year and will release data annually. John Ribeiro, *US to Release Annual Figures on Spying Orders and People Affected,* COMPUTER WORLD (Aug. 29, 2013, 10:49 PM), http://www.computerworld.com/s/article/9242021/US_to_release_annual_figures_on_spying_orders_and_people_affected?source=rss_news_analysis&utm_source=feedburner&utm_medum=feed&utm_campaign=Feed%3A+computerworld%2Fs%2Ffeed%2Ftype%2Fnewsanalysis+%28Computer.

collect the information in other more traditional ways[117] and that there was no way of showing that information used by the government was collected through Section 1881(a) programs.[118] Assurances made by Senator Dianne Feinstein, chairwoman of the Intelligence Committee, promulgated the Justice Department's practices of notifying criminal defendants their communications were being monitored under the statute.[119] According to reports in the *New York Times*, national security prosecutors had not been informing defendants when the prosecutors used evidence from warrantless wiretaps.[120] This was in direct contradiction to what had been written in the FAA of 2008.[121] Internal leaks from the executive office have claimed that the solicitor general's office has been fighting since June 2013 to get the prosecutors to follow the safeguards established in the FAA.[122] This creates a paradox for the government in establishing the necessity for the warrantless collection of metadata.

While proponents for maintaining the current FISA programs have focused on the necessity of national security, this rationale places the government in a difficult position. If FISA programs have used information collected through a warrantless wiretap to convict a defendant, the government has yet to disclose to the defendant that he was in fact monitored, which is a violation of Section 1881a.[123] The inability for a

---

117. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1158 (2013) (Breyer, J., dissenting).

118. *Id.* (focusing on the restriction of using information for trial collected under a Section 1881a program without notifying the defendant where the information used was collected).

119. Sen. Feinstein gave a speech in 2012 that suggested several terrorism cases were successfully tried using warrantless wiretap programs and the lack of successful terrorist attacks was proof that the warrantless wiretap programs were working. Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013), http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=2&.

120. *Id.* (by not allowing criminal defendants the ability to address all evidence and accusers at trial, there is a high probability that convictions will be overturned or successful appeals for a new trial will be granted, because this information can establish Confrontation Clause violations).

121. FISA Amendments Act of 2008, 154 CONG. REC. H 1707-05 (2008) (showing Section 702 of the FAA outlines that all criminal defendants that have been prosecuted using information collected in programs utilizing warrantless wiretaps shall be promptly notified of the surveillance used).

122. Sean Hollister, *Warrantless Wiretapping Catch-22 Might Have Been Illegal*, VERGE (Oct. 17, 2013), http://www.theverge.com/2013/10/17/4850556/warrentless-wiretapping-catch-22-might-have-been-illegal (listing several anonymous sources in the Obama administration as giving the information to the *New York Times* that national security prosecutors have not been telling defendants when they are under surveillance because of inconsistent interpretations of the requirements in the statute).

123. *Id.*

criminal defendant to defend evidence that has been obtained through these programs violates the defendant's constitutional right to confront accusers.[124] This proves that the abilities for U.S. citizens to challenge the constitutionality of the FAA of 2008, by Justice Alito's standard,[125] can never be satisfied and that the FISA surveillance programs have violated constitutional protection of unreasonable search and seizure under the Fourth Amendment. However, if the government does not acknowledge the use of information obtained through these warrantless wiretapping programs, there is no proof that it "has worked" to stop future terrorist attacks.[126]

Following the standard created by Justice Alito in *Clapper*, a plaintiff must prove that an injury in fact is directly traceable to a surveillance program conducted under Section 1881a.[127] This requires that a plaintiff either shows that the government had no other possible way of obtaining the information on the target without using warrantless wiretaps or he has direct evidence of being wiretapped without warrant. This is an impossible standard for plaintiffs to reach because it is a continually moving goal. It allows for warrantless surveillance to be conducted whenever other alternative surveillance may be possible. The difference is the breadth and oversight with more traditional routes of gathering information that often requires a warrant, other than the programs set up in Section 1881a. Plaintiffs will also have to show that they are actively targeted by the warrantless wiretap programs. Reading Alito's decision, plaintiffs are unable to prove an injury in fact based upon the apprehension of possible surveillance or through collateral surveillance. This restricts plaintiffs' abilities to challenge the FISA programs because it narrowly reads Section 1881a "intentional targeting" parameters.[128] Plaintiffs will be hard-pressed to establish an intentional targeting from a collateral targeting when they have contacts with foreigners. This is primarily a cataloging or descriptor of how

---

124. U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed . . . to be informed of the nature and cause of the accusation; to be confronted with the witness against him; to have compulsory process for obtaining witnesses in his favor.").

125. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1158 (2013) (Breyer, J., dissenting).

126. Hollister, *supra* note 122 (quoting Sen. Diane Feinstein's testimony in December 2012 that warrantless wiretap programs had worked to successfully prosecute individuals convicted of terrorism related charges).

127. *Clapper*, 133 S. Ct. at 1148 (Alito, J., majority opinion).

128. "Intentional targeting" is no longer a viable option for plaintiffs to challenge the FAA of 2008, because Justice Alito's decision gives the government a broad range to somewhat create a scenario in which a U.S. person was not intentionally targeted, but rather simply absorbed in the targeting of some other non-U.S. person. *Id.*

surveillance has been conducted, and skirts the protections for U.S. citizens. Without meeting both of these standards, U.S. persons are unable to challenge FISA programs.

Beyond the current surveillance programs that have been approved by the FISA courts, the NSA has actively targeted loopholes in FISA targeting procedures to gain direct access to otherwise protected information.[129] According to leaked documents obtained by *The Guardian*, the NSA has tapped the communication links that connect Yahoo and Google data servers across four continents, allowing entire data flows to be copied.[130] This direct access is striking due to the secrecy, even from the companies that are being infiltrated, when approved FISA programs such as PRISM are readily available for secret surveillance.[131] Intercepting these communications overseas is a clear advantage for NSA programs as they operate outside many of the FISA minimization requirements. According to Senator Feinstein, Congress conducts little oversight of intelligence-gathering under the presidential authority of Executive Order 12333,[132] which covers all foreign intelligence gathering. By accessing the data links that are outside of the United States, the NSA is allowed to presume anyone using these foreign data links is a foreigner.[133]

By infiltrating the foreign links of both Yahoo and Google, the NSA can access what was once protected information without any FISA minimization procedures. The data centers are designed to synchronize large volumes of information about account holders in large data centers to maintain system speed and access.[134] The information is currently being collected and are stored in "cloud servers" as a redundancy to protect against data loss and system failure.[135] The indiscriminate

---

129. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say,* WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story_2.html (explaining the NSA's program MUSCULAR is a joint program implemented with British Intelligence to gather the information of users' content that is sifted between data centers and cloud storage of Yahoo and Google).

130. *Id*. (noting that the information is accessed by directly tapping the vast fiber optic networks that are required to connect cloud servers to data storage facilities, which are not encrypted).

131. *Id*.

132. *Id*. (noting that the provisions of Executive Order 12333 of Dec. 4, 1981, 46 FR 599941, 3 CFR, 1981 Comp. outline the need for and purpose of the collection of accurate and timely information in the areas of national defense and foreign relations, specifically sections 2.1, 2.2, and 2.3 address this need).

133. Gellman & Soltani, *supra* note 129.

134. *Id*.

135. Adi Robertson, *NSA Secretly Taps into Google, Yahoo Networks to Collect Information, Say Leaked Documents*, VERGE (Oct. 30, 2013),

collection of "foreign" information directed through these links will undoubtedly lead to the collection of U.S. citizen's information in the broad sweeping program. According to information disclosed on January 9, 2013, in a 30-day period, 181,280,466 records including metadata was processed and sent back as it was acquired through the information links.[136]

The release of this new information has led information companies to accelerate their encryption overhauls.[137] Overhauling and implementing vast encryption services for large companies has created an "arms race."[138] Although directed targeting cannot be completely protected, these companies are trying to make it harder for broad dragnet surveillance to become feasible, which adds an extra cost onto the operation of these companies. If these companies were able to display that they have suffered an injury by spending significant funds and resources on these new encryption techniques, they may satisfy standing to challenge the FISA programs.

Proponents of FISA may claim that the hardships incurred by telecommunication and internet providers increasing their security protocols would satisfy the standing requirement established in *Clapper*.[139] The theory would rest on the dramatic increase in security costs for these companies to implement encryption protocols throughout their redundancy networks. Supporters of the current FAA would suggest that there is no need to alter the Act due to the ability for certain parties to challenge the constitutionality of the FAA based on this theory. However, Justice Alito was reluctant to find economic hardship for plaintiffs in *Clapper* because securing their communications is an expected cost. The costs incurred for these information companies to increase their security measures will likely be considered an operating expense and therefore not create an economic hardship.

---

http://www.theverge.com/2013/10/30/5046958/nsa-secretly-taps-into-google-yahoo-networks-to-collect-information.

136. Gellman & Soltani, *supra* note 129 (indicating metadata includes who sent or received e-mails and when, as well as content such as text, audio, and video).

137. Craig Timberg, *Google Encrypts Data Amid Backlash against NSA Spying*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html.

138. *Id*. (quoting Google Vice President for security engineering Eric Grosse on encrypting services and competing against government surveillance programs to protect against both foreign and domestic threats to consumer privacy).

139. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013).

B. PROPOSED LEGISLATION

In July 2013, an unexpected and bipartisan effort to amend the NSA's domestic surveillance powers was narrowly defeated in the House of Representatives.[140] The amendment, attached to an annual defense budget bill, attempts to defund the NSA in order to limit the abilities of the NSA's surveillance programs.[141] Although the amendment failed to secure a majority, this was a step towards formal and open deliberation on FISA programs in Congress.[142]

The Intelligence Oversight and Surveillance Reform Act (ISOR) is a proposed legislation that will focus on improving oversight of the FISC court and provide for more transparency from government entities and the private sector.[143] Additional legislation, proposed in the House of Representatives and Senate, has also pushed for more stringent measures in maintaining the protection of U.S. persons' civil liberties and has been supported by private information companies.[144] This proposed legislation, Surveillance Order Reporting Act (SOR) and Surveillance Transparency Act of 2013 (STA), "seek to give companies more options for disclosing when and how often they received national security-related requests and provided data to the government."[145] These bills are currently in their respective intelligence committees and must be passed before moving on to the House and Senate floors for a vote.[146]

---

140. Joshua Kopstein, *House Narrowly Defeats NSA Amendment, Allowing Agency to Keep Spying on Americans,* VERGE (July 24, 2013), http://www.theverge.com/2013/7/24/4554420/nsa-amendment-defeated-allowing-agency-to-keep-spying/in/4167369 (noting that the actions of the House were particularly fast moving and caught most people off guard).

141. *Id*.

142. *Id*. (noting that this early House vote was actually an attempt to defund Section 215 of the Patriot Act which allows for the funding of programs that are reasonably expected to assist in the prosecution or the capture of individuals involved in terrorist plots).

143. Hollister, *supra* note 19 (stating that the proposed legislation has not fully been written yet, but the bill's sponsors Sen. Ron Wyden, Sen. Mark Udall, Sen. Richard Blumenthal, and Sen. Rand Paul provided a summary and held a press conference outlining the legislation that will be presented shortly).

144. Robertson, *supra* note 135. These bills have been supported by the Center for Democracy and Technology and have received letters of support from over two dozen companies and a number of trade groups, requesting that more details of the government's secret information requests be published for public dissection. *Id*.

145. These bills act as a combination of the current legislation that has been proposed and the petitions that Apple, Google, and other technology companies have been waging to allow for more open discussion and the ability to divulge what information they have offered to the government. *Id*.

146. These bills that are financially backed and publicly supported by technology companies will have the higher likelihood of success because the amount of money that is involved, developing security and securing customer's trust, has leveraged intense pressure on the legislature to get a bill completed. *Id*.

There are some distinct differences in how these bills are attempting to change the current use of NSA surveillance programs. First, the ISOR Act is trying to add government oversight into the FISC court system of approving targeting orders; whereas the SOR Act and STA Act target corporate gag orders. The SOR Act and STA Act would accomplish this by allowing the publishing of detailed reports which outline the information companies have disclosed to government surveillance programs and give their customers a more defined scope of government data collection.[147] Despite these differences, what each of these proposed bills seeks is to target specific areas of FISA in an attempt to control either the acquisition of information or the dissemination of acquisition policies, none of these fully encapsulate a plan that will significantly affect how surveillance is currently conducted. Analyzing the proposed legislation reveals several shortcomings that are specific to each act.

Analyzing ISOR first, the focus of this act is mainly on reforming the duties of the FISC court, as well as creating a new form of "judicial constraint."[148] The shortcoming of ISOR is the significant changes to the FAA of 2008 that are required for it to be implemented.[149] The bulk of ISOR seeks to reform the FISC court by implementing a "Constitutional Advocate to argue against the government when the FISC is considering significant legal and constitutional questions."[150] This would require the creation of a new pseudo regulatory agency tailored specifically to the FISC court. Creating this regulatory agency would create several issues including budget and authority, specifically which branch of the federal government would the agency be under. ISOR would also declassify significant FISC opinions, which contain specific interpretations of the law or the Constitution and permit constitutional challenges for law-abiding Americans who have been professionally impacted by the U.S. government's collection of communications.[151] Although this would provide a framework for constitutional challenges by private

147. Currently, companies are barred from disclosing what type of information they have produced which has caused a lot of concern from their customers who have used their services for data storage as well as transmission of sensitive materials. *Id.*

148. Hollister, *supra* note 19.

149. *Id.* The biggest issue with implementing ISOR is that it is overly ambitious and the elements included within it would require significant support in both houses of the federal government and both major parties because it will require significant rewrites to the FAA of 2008 as well as the creation of significant oversight committees as well as increased budget concerns. *Id.*

150. *Id.*

151. The bill does not give a clear definition or understanding to who are law-abiding Americans and it has a caveat of only including those Americans that have been professionally impacted while ignoring the privacy concerns of citizens that use services for their personal use. *Id.*

citizens, this does not address the inabilities for plaintiffs to prove that they were in fact targeted by NSA surveillance programs.

Minimization procedures are also a significant part of ISOR's attempt at regaining control over how surveillance is conducted. ISOR would focus on reasserting the minimization procedures that have been subverted by the FAA of 2008. The hope under the original FISA scheme was that a judge would act upon his own volition to minimize the possibility of a U.S. citizen being directly targeted by surveillance programs.[152] However, minimization techniques have been impeded through the assured anonymity that current FISC court judges have and the FAA of 2008's elimination of the FISC judge's power to challenge the factual predicates of the government's application.[153]

Currently under the FAA of 2008, minimization receives its power through Section 703.[154] Judicial, as well as other minimization procedures, are to be conducted pursuant to the definitions of intentional targeting of the communications of a U.S. person and are subject to judicial review.[155] Although these procedures have been delineated under the FAA of 2008, information that has been leaked shows that the authority of the FISC court to protect these minimization procedures has effectively been subverted by the FAA of 2008.

The notion of the FISC court as a rubberstamp on government surveillance via these current limited minimization procedures is likely very accurate and is a problem in and of itself. However, this Comment is not an indictment of the FISC court to view content of surveillance requests subjectively. The purpose of this information is to describe how minimization has been removed from the FAA of 2008 and in so doing, has removed the only judicial body that has the clearest oversight over the surveillance programs.

Next, analyzing the SOR Act and STA Act, the focus of these Acts are to push for a more immediate resolution to some of the concerns that U.S. persons have regarding private companies turning over their

---

152. Owen Fiss, *Even in a Time of Terror,* 31 YALE L. & POL'Y REV. 1, 18 (2012) (placing the onus on FISC court judges to make decisions of whether private citizens' privacy concerns would trump national security concerns is an undue burden, that even without new capabilities allowing for easy dragnet surveillance, it would be a difficult task that is almost certainly doomed to fail).

153. *Id*. (suggesting the troubling issue is the perception that FISC judges now rubberstamp all applications without needing a specific articulation of the target or reason for permitting the monitoring targets).

154. FISA Amendments Act of 2008, 154 CONG. REC. H 1707-05 (2008).

155. *Id*. (discussing that although private citizens cannot be intentionally targeted by NSA surveillance programs under the FAA of 2008, information has been revealed showing that these programs have collected vast amounts of information from U.S. citizens by collecting the information as it has been transmitted through international transmission hubs).

private information to government surveillance programs. However, these legislative pushes run far shorter than the proposed legislation under the aforementioned ISOR Act. Currently, companies can only report on the amount of data requests.[156] While these requests can be reported in blocks of 1,000, a single request could encompass millions of users.[157] The SOR and STA Acts would focus on refining the language used in the FAA of 2008 to allow private companies to give more detailed reports regarding the frequency and amount of user data that has been requested under FISC court orders.

All of the above being considered, the SOR and STA Acts are more likely to be passed in Congress and moving onto the next stage of the legislation process, due to the substantial lobbying of the technology industry and that these acts will not alter any significant parts of the FAA of 2008. Lobbying by several large technology companies has increased support in the legislation that would give the companies more ability to inform their customers and future users about information requests.[158] These companies hope that more transparency will alleviate customer's concerns about information security. Endorsement by technology companies also provides more persuasive support to the SOR and ACT Acts by showcasing the private sector backing of these acts. However, both the SOR and STA Acts still fall short of offering a substantive solution to the problems of implementing FISA programs because they do not halt or change any of the policies currently used to collect information.

The reason that these aforementioned bills still fall short is because of the dilemma presented to Congress in tackling this problem. The dilemma is in creating legislation that has the substantive power to affect change to the FAA of 2008 while still being a bill that is reasonably expected to pass through both the House of Representatives and Senate. ISOR as it is currently expected to be presented would provide the most effective reform to the FAA of 2008. But, ISOR has the significant challenge of maintaining a bipartisan support and it requires drastic alterations to the FAA of 2008 which the SOR and STA Acts do not require any drastic alterations. ISOR is a predominantly Democrat supported bill and could pass through the Senate but would likely see a significant pushback in the Republican-dominated House of

---

156. Russell Brandom, *Can a New Round of NSA Transparency Bills Make it Through Congress?*, VERGE (Oct. 1, 2013), http://www.theverge.com/2013/10/1/4790484/can-the-nsa-transparency-bills-make-it-through-congress/in/4483763.

157. *Id*. (noting that this use of a single request to obtain millions of users' data is misleading and deceptive by giving the perception of only a few users being affected).

158. *Id*.

Representatives.[159]

Pushback to ISOR is anticipated because the necessary alterations would require significant debate on balancing privacy and national security.[160] President Obama has made the balance between national security and privacy clear when he addressed the growing concerns of how information has been collected:

> But I think it's important to recognize that you can't have 100 percent security, and also then have 100 percent privacy, and zero inconvenience. You know, we're going to have to make some choices as a society. What I can say is that in evaluating these programs, they make a difference in our capacity to anticipate and prevent possible terrorist activity.[161]

President Obama addressed the nation and ensured that the surveillance conducted by the NSA had been passed through bipartisan majorities and that Congress has been properly informed on how surveillance had been conducted.[162] However, President Obama's insistence that "these programs have been authorized by broad bipartisan majorities . . . and your duly elected representatives have been consistently informed on exactly what we're doing" was not entirely accurate.[163] According to Representative Justin Amash, the 2011 letter sent to both the House Intelligence Committee and the Senate Intelligence Committee was held confidential within this small circle.[164] Rep. Amash's statements cast doubts upon how much information Congress was given outside of the select few that sat on intelligence committees.[165] Rep. Amash found that the letter would not have been seen by members of Congress elected after 2010 and therefore would not have had a sound opinion on the Patriot Act nor the FISA Amendments Act.[166]

This lack of overall understanding by Congress, as well as by the American public, allowed the creation of a very powerful surveillance

---

159. *Id*.

160. *Id*. (noting that bills that are deemed to be overly ambitious are often dead on arrival when presented to the floor of either the House of Representatives or Senate because few members will be willing to vote for and be associated with legislation that does not pass).

161. Franzen, *supra* note 103.

162. *Id*.

163. *Id*. (noting the importance of understanding how surveillance is collected is different than arguing whether or not the surveillance has been conducted; for several years the American public has been kept in the dark about what information has been collected).

164. Robertson, *supra* note 135 (Representative Amash posted a declassified document noting that the letter was intended to be presented to all members of congress as an effective way to inform the legislative debate).

165. *Id*.

166. *Id*.

program. And now, although there is much outrage and want to create substantial change as to how surveillance is conducted, it is quite clear after the recent government shutdown that bipartisan support of any legislation would be wishful thinking. ISOR would provide the substantial change that many are requesting, but it is overly ambitious and the significant change it requires makes it an impractical solution. This fact has allowed the SOR and STA Acts to exist as they seek to make smaller, incremental changes that, although less successful in executing change, are more likely to receive bipartisan support. Addressing the issues presented by the FAA of 2008 requires legislation that is both pragmatic and capable of challenging the constitutionality of the NSA surveillance programs.

C. THE CREATION OF STANDING BY REDEFINING FISA INJURY IN FACT

There is a clearer way of redefining the actions of the NSA under the FAA of 2008, which would be to give plaintiffs a greater chance of challenging the constitutionality of FAA of 2008. Currently under *Clapper*, plaintiffs have yet to establish an injury in fact that would supersede the Supreme Court majority's apprehension of giving extenuating circumstances enough merit to justify standing.[167] If a congressional amendment to the current FAA of 2008 inserted a new definition for protected information, then standing to challenge the acquisition of communications can be satisfied and there would be a significant increase in surveillance oversight. This bill would avoid the messiness of trying to restructure the currently secretive FISC court operations. Rather than attempting to create a new form of judicial review[168] or the creation of a new authority for Congressional oversight board,[169] a more constructive attempt at addressing the need for a clearer balance would be to give the constitutional challenge back to the people. Rather than trying to legislate it into firmly rooted governmental bodies, let the private section, the plaintiffs of the United States, fight this battle as they are the ones who are "injured in fact."

This proposed legislation combines the pragmatic approach of the SOR and STA Acts by avoiding any drastic rewrite of the FAA of 2008 while still achieving the goals of affecting significant change to NSA surveillance programs found in ISOR. Since this legislation only

---

167. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013).

168. Hollister, *supra* note 19 (stating that the currently presented legislation calls for the creation of a completely new regulatory body to act as an independent defense counsel that would challenge the government's reasons and assertions when asking for FISC court approval to request information).

169. The bill gives the Privacy and Civil Liberties Oversight Board the authority to issue subpoenas to ensure that government policies are not breaching constitutional liberties and compel testimony with the force of law. *Id*.

requires creating a new section of protected information, it does not require significant alterations to the FAA of 2008 that could block bipartisan support. Creating a new definition for protected information will likely receive broad support and lobbying from the technology industry, because it would restrict what information they would be required to relinquish.

The aforementioned legislation does not address the entirety of FISA programs nor does it attempt to solve every issue in FISA. The goal of this proposed legislation is instead to create an avenue for plaintiffs to get into court by satisfying standing. Unlike proposed legislation like ISOR or SOR/STA, this proposed solution will give plaintiffs a method to actually challenge the constitutionality of FISA. Creating a clear method for plaintiffs to assert challenges to FISA is the most practical solution to these convoluted problems. So far, the U.S. Supreme Court has been able to avoid ruling on FISA. This legislation will alleviate the burdens upon the legislature to address FISA on its own and will compel all branches of the federal government to work towards a solution.

Although this solution is a roundabout way of addressing the plaintiff's shortcomings in *Clapper*, it satisfies the issues that Justice Alito had presented in his majority holding.[170] Justice Alito's opinion established that plaintiffs must be able to show an injury in fact and more than a speculation that the government used Section 1881a authorized surveillance to target their clients.[171] Furthermore, giving plaintiffs the opportunity to satisfy standing will allow the Supreme Court to adjudicate the constitutionality of the FAA of 2008. There does not need to be a drastic Congressional bill that will likely not pass both houses of Congress for there to be a significant change to the legal rights of plaintiffs to challenge the constitutionality of FAA of 2008.

Although attacking the present issues in a very different way than ISOR or SOR/STA Acts, this proposed solution could actually be successful in asserting a change to the current dilemma both Congress and the American public face. First, a new amendment to the FAA of 2008 should insert limitations on the acquisition of metadata. Currently under Section 703, any intentional targeting of a known or reasonably believed target that is a U.S. person is restricted.[172] The collection of U.S. persons' metadata information is an intentional targeting of U.S.

---

170. *Clapper*, 133 S. Ct. at 1151.

171. *Id*. (providing three reasons for not granting Article III standing, but the third reason is not the controlling language of the decision but merely sets out the reluctance of the Supreme Court to find standing based on assumptions).

172. FISA Amendments Act of 2008, 154 CONG. REC. H 1707-05 (2008) (section 703(b) sets out the parameters of targeting persons while section 703(d) and 703(e) set out the targeting procedures and minimization procedures respectively).

persons that was limited directly by Section 703. Although this collection targets U.S. persons, courts have yet to find that metadata is the type of information or communication that is protected under the Fourth Amendment.[173] Metadata should be presented as a new point under Section 703 limitations. This will give plaintiffs the ability to point directly at a statutory limitation that they can base their injury in fact off of. This will likely be sufficient to establish that plaintiffs have standing to challenge the constitutionality of the FAA of 2008. Justice Alito determined that the simple fear of having information collected was not enough for plaintiffs to achieve Article III standing. Contrary to Justice Alito's apprehension of plaintiff's fear, leaked documents show that U.S. persons have been intentionally targeted through the dragnet collection of all Verizon communications.[174]

Secondly, although these challenges may not be able to satisfy the second crux of Justice Alito's opinion, they provide a basis for this to be achieved in the future. Justice Alito found that if there was some other possible way for the government to have conducted the surveillance, there should not be a rush to judgment or finding that the government had certainly conducted warrantless surveillance.[175] While the proposed legislation cannot achieve this on its own, the importance of allowing the potential success of it, is that it at least plaintiffs can establish that they have been targeted in dragnet surveillance programs. Establishing direct evidence of dragnet surveillance programs will limit the need to address other possible ways surveillance could have been conducted and set a firm basis for a constitutional challenge of FISA program legality.

The goal of this new legislation is not to take on the bear of a problem that is the FAA of 2008, but merely to establish the framework for this Act to at least be challenged on a constitutional basis. So far, the legislation that has been proposed has only looked at creating a new subset of judicial control in the FISC court or has catered only to the dissemination side of producing user information. The larger goal, of any congressional act that wishes to address the issue of guaranteeing U.S. persons' privacy rights are secured, is to allow a plaintiff into federal court to challenge the constitutionality of the FAA of 2008.

The respondents in *Clapper* have already refiled a petition to have their case reviewed after more information had been leaked following their case's dismissal.[176] Since under the current FAA of 2008 plaintiffs

---

173. Hesseldahl, *supra* note 86 (according to Stephen Baker, the state department has relied on the reluctance of courts to increase the privacy concerns of metadata to the levels of it being protected under the Fourteenth Amendment, which would protect the collection of the information similar to that of simple wiretaps).

174. Hollister, *supra* note 19.

175. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013).

176. Brandeisky, *supra* note 17 (having joined in the Electronic Privacy Information

cannot petition the surveillance court directly, The Electronic Privacy Information Center (EPIC) has petitioned straight to the U.S. Supreme Court.[177] The Justice Department has responded that EPIC lacks standing and a mandamus review is unwarranted because EPIC can still file a challenge in a federal district court.[178]

This current petition is a clear example of why there needs to be additions made to the FAA of 2008 that allow for plaintiffs to satisfy the standing requirements to be heard in front of the Supreme Court. It is highly unlikely that legislation will be passed that restricts the activities of the FISC court, or that will give plaintiffs enough authority to challenge the FISC court decisions. Currently under the FAA of 2008, FISC court decisions are not challengeable by U.S. persons. Without creating a way for U.S. persons to establish standing, there will be no legal remedy available to protect civil liberties. Absent a new found commonality among the differing parties in Congress, there is little to no chance that a substantial bill will be passed that drastically changes how the FISC court is structured or how FISA surveillance programs are implemented. The most successful challenge to these rigid ideas will come from the most unlikely source, and that is why there needs to be a reliance on plaintiffs getting into the Supreme Court to challenge the constitutionality of FAA of 2008.

IV. CONCLUSION

Balancing the needs of national security, while maintaining privacy for U.S. citizens, cannot be easily quantified or diagramed. The need of an open democratic republic requires that both be openly discussed and debated. The issues involved strain the common bond that is so often looked for in a free and open society that to not have any discourse is the biggest hurdle to overcome. Since the adoption of more stringent and often over-zealous collection of communications following the terrorist attacks on September 11, 2001, there has been significant public apathy towards civil liberties. The current model of allowing secret courts to allocate and protect the rights of all U.S. citizens has created a strain on trust in the government when it was most needed. The use of metadata by FISA surveillance programs satisfies the injury in fact issue for plaintiffs to establish Article III standing. The reluctance of the Supreme Court to grant Article III standing in *Clapper* was based on the notion that the extenuating circumstances of possibly being swept

---

Center petition for writ of mandamus, respondents in *Clapper* argued that the FISC court exceeded its authority when it interpreted the word "relevant" to encompass all the metadata that Verizon possesses).

177. *Id*.

178. *Id*.

up in the dragnet surveillance by the NSA was too remote. The Supreme Court was justified in being cautious of allowing plaintiffs to create standing, by fear of surveillance alone. However, there is a greater need to allow plaintiffs to bring a case challenging the constitutionality of FAA.

Forcing FISC court orders into the public domain, by allowing plaintiffs to petition them directly for the evidence of being monitored by government agencies, will be the first step in securing that trust in the government will be reformed. Although legislation can establish new parameters and set out more stringent guidelines for how communications are collected and stored, without the ability to challenge the constitutionality of the program in the legal system, these problems will persist. Although there may seem to be easier ways of achieving a constitutional challenge to the FAA of 2008, these paths are all likely dead ends. Legislation that does not try to give plaintiffs a larger platform or a more defined Article III standing will fail at achieving any real end result. The likelihood of another change to the actual legislation will be too low.