Congressional Research Service
Informing the legislative debate since 1914

Overview of Constitutional Challenges to NSA Collection Activities

Edward C. Liu
Legislative Attorney

Andrew Nolan
Legislative Attorney

Richard M. Thompson II
Legislative Attorney

May 21, 2015

Congressional Research Service
7-5700
www.crs.gov
R43459

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Beginning in summer 2013, media reports of foreign intelligence activities conducted by the National Security Agency (NSA) have been widely published. The reports have focused on two main NSA collection activities approved by the Foreign Intelligence Surveillance Court (FISC) established under the Foreign Intelligence Surveillance Act (FISA) of 1978. The first is the bulk collection of telephony metadata for domestic and international telephone calls. The second involves the interception of Internet-based communications and is targeted at foreigners who are not within the United States, but may also inadvertently acquire the communications of U.S. persons. As public awareness of these programs grew, questions about the constitutionality of these programs were increasingly raised by Members of Congress and others. This report provides a brief overview of these two programs and the various constitutional challenges that have arisen in judicial forums with respect to each.

A handful of federal courts have addressed the Fourth Amendment issues raised by the NSA telephony metadata program. FISC opinions declassified in the wake of the public's awareness of the NSA telephony metadata program have found that the program does not violate the Fourth Amendment. Similarly, in *ACLU v. Clapper*, the federal District Court for the Southern District of New York held that a constitutional challenge to the telephony metadata program was not likely to be successful on the merits. On appeal, the U.S. Court of Appeals for the Second Circuit refrained from reaching the merits of this Fourth Amendment challenge, but instead resolved the case on statutory grounds, holding that the metadata program exceeded statutory authorization under Section 215 of the PATRIOT Act. However, the panel did engage in a general discussion about the Fourth Amendment principles implicated by this program, including the effect of modern technology on American's expectations of privacy. Both the district courts for the Southern District of California and the District of Idaho have found the bulk metadata program constitutional under existing Supreme Court precedent. In *Klayman v. Obama*, the federal District Court for the District of Columbia held that there is a significant likelihood that a challenge to the constitutionality of the NSA telephony metadata program would be successful.

Constitutional challenges to the NSA's acquisition of Internet communications of overseas targets under FISA have arisen in a number of different contexts. First, such challenges have arisen in both the FISC and the Foreign Intelligence Surveillance Court of Review as part of those courts' roles in approving the parameters of these collection activities. Secondly, constitutional challenges have been brought in traditional federal courts as civil actions by plaintiffs asserting an injury or in criminal proceedings by defendants who have been notified that evidence against them was obtained or derived from collection under Section 702. While the FISA courts have at times curbed the government's ability to engage in surveillance activity to ensure compliance with the Fourth Amendment, the one federal court to address the issue has upheld the program against constitutional challenge.

Contents

Contacts

Beginning in summer 2013, media reports of foreign intelligence activities conducted by the National Security Agency (NSA) have been published and are apparently based on unauthorized disclosures of classified information by Edward Snowden, a former NSA contractor. The reports have focused on two main NSA collection activities conducted under the auspices of the Foreign Intelligence Surveillance Act (FISA) of 1978.[1] The first is the bulk collection of telephony metadata for domestic and international telephone calls. The second involves the interception of Internet-based communications and is targeted at foreigners who are not within the United States, but may also inadvertently acquire the communications of U.S. persons.

This report provides a description of these two programs and the various constitutional challenges that have arisen in judicial forums with respect to each. Although a brief overview of the constitutional arguments and issues raised in the assorted cases is included, a detailed analysis or evaluation of those arguments is beyond the scope of this report.

Summary of the Foreign Intelligence Surveillance Act of 1978

As both programs make use of authorities provided under FISA, this section provides a brief description of that statute to help inform the subsequent discussion. FISA currently provides procedures for the approval of various types of investigative methods: (1) electronic surveillance,[2] (2) physical searches,[3] (3) pen register/trap and trace surveillance,[4] and (4) the use of orders compelling the production of tangible things.[5] The FISA Amendments Act (FAA) of 2008 added additional provisions for the foreign intelligence targeting of non-U.S. persons reasonably believed to be abroad[6] and the targeting of U.S. persons reasonably believed to be located abroad.[7] Although the requirements for each category of investigative tool differ significantly from one another, all make use of the Foreign Intelligence Surveillance Court (FISC), a specialized Article III court established under FISA to review and approve governmental applications seeking to use one of the aforementioned authorities.[8] FISA also establishes a Foreign Intelligence Surveillance Court of Review (FISCR) to provide appellate review of decisions made by the FISC.[9]

[1] 50 U.S.C. §1801 *et seq.*

[2] 50 U.S.C. §1803(a).

[3] *Id.* §1822(c).

[4] *Id.* §1842(a)(1). A pen register is a device which records all outgoing numbers dialed from a particular telephone line. A trap and trace device is akin to a "caller-ID" feature that records the telephone numbers from which incoming calls are being dialed.

[5] *Id.* §1861(b)(1).

[6] *Id.* §1881a.

[7] *Id.* §§1881b(a), 1881c(a). U.S. persons are defined in FISA to include U.S. citizens and legal permanent residents, as well as unincorporated associations comprised of a substantial number of U.S. persons and most domestically chartered corporations. 50 U.S.C. §1801(i).

[8] 50 U.S.C. §1803(a)(1). The FISC is composed of 11 district court judges selected by the Chief Justice of the Supreme Court.

[9] 50 U.S.C. §1803(b).

Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act

Following the terrorist attacks of September 11, 2001, the NSA began a program in which domestic telephony metadata was collected with the goal of helping to detect and identify individuals who were part of terrorist networks.[10] This program is frequently described as collecting telephony metadata "in bulk" to distinguish it from the narrower collection of metadata pertaining to an identified individual or group of individuals that is commonplace in both law enforcement and national security investigations. Since 2006,[11] the collection of telephony metadata in bulk has been sanctioned by orders of the FISC issued pursuant to Section 215 of the USA PATRIOT Act of 2001.[12] Under Section 215, the FBI may apply to the FISC for an order compelling a person to produce "any tangible thing" if there are reasonable grounds to believe that the things sought are "relevant" to an authorized foreign intelligence, international terrorism, or counter-espionage investigation.[13] An "authorized investigation" must be conducted under guidelines approved by the Attorney General under Executive Order 12333 and may not be conducted of a United States person solely upon the basis of activities protected by the First Amendment.[14]

Shortly after specific details about the NSA telephony metadata program were published in the media beginning in summer 2013, concerns about its constitutionality were quickly raised by commentators and lawmakers.[15] In particular, it has been argued that the collection of telephony metadata in bulk is an "unreasonable search[]" prohibited by the Fourth Amendment.[16] Before

[10] Unclassified Declaration of Frances J. Fleisch, National Security Agency, Schubert v. Obama, No. 07-cv-0693-JSW at ¶ 32 (N.D. Cal. December 20, 2013) available at http://icontherecord.tumblr.com.

[11] *Id.* at ¶ 21.

[12] P.L. 107-56, §215, codified as amended at 50 U.S.C. §1861. Section 215 replaced an existing FISA provision that contained a mechanism for the government to compel the production of records from only four types of businesses: (1) common carriers, (2) public accommodation facilities, (3) storage facilities, and (4) vehicle rental facilities. A court order compelling the production of these records was authorized if the FBI presented the FISC with "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. §1862 (2001). Originally subject to sunset on December 31, 2005, §215 has been reauthorized six times since it was originally enacted, and is currently set to expire on June 1, 2015. *See*, P.L. 109-160 (extension until February 3, 2006); P.L. 109-177 (extension until December 31, 2009); P.L. 111-118, §1004 (2009) (extension until February 28, 2010); P.L. 111-141 (extension until February 28, 2011); P.L. 112-3 (extension until May 27, 2011); P.L. 112-14 (extension until June 1, 2015).

[13] 50 U.S.C. §1861(b)(2)(A). Records are considered presumptively relevant if they pertain to a foreign power or an agent of a foreign power; the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. Additionally, if the records sought are "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the application must be approved by one of three high-ranking FBI officers, and cannot be further delegated.

[14] 50 U.S.C. §1861(a)(2).

[15] *See*, Senators Ron Wyden, Mark Udall, Martin Heinrich, *End the N.S.A. Dragnet, Now*, N.Y. TIMES, November 25, 2013; PCLOB Report, *supra* note 2.

[16] Jameel Jaffer, Testimony before the Senate Judiciary Committee, July 31, 2013, available at https://www.aclu.org/files/assets/testimony.sjc_.073113.final_.pdf. It has also been argued that the program is not consistent with the requirements of §215. *Id.* Because this report is limited to constitutional challenges, an evaluation of such arguments is beyond the scope of this report.

discussing these claims, this report will first provide a brief summary of the program's history and current status.

Description of Telephony Metadata Program

Generally, the telephony metadata program has operated by placing few limits on the government's ability to *collect and retain* large amounts of domestic and international telephone records while imposing more stringent restrictions on the government's capacity to *search or make further use* of the collected metadata. These restrictions are not explicitly required by the statutory text of Section 215. Instead, they are delineated as part of the orders the FISC issues pursuant to Section 215.

The program collects "metadata"—a term used in this context to refer to data about a phone call, but not the audio contents of a phone conversation itself.[17] Declassified FISC orders indicate that the data include the number that a call was dialed from; the number that a call was dialed to; and the date, time, and duration of the call.[18] The data do not include cell site location information. Intelligence officials have committed to alerting Members of Congress before collecting that location information, suggesting they currently have the authority to do so.[19]

The operation of this program has been altered significantly since its existence became widely known in June 2013.[20] Its current state of operations reflects changes to the program that were announced by President Obama on January 17, 2014.[21] Although the President directed the Attorney General and the intelligence community to recommend alternatives to the collection and retention of such metadata by the government, the announced changes did not immediately affect the ability of the NSA to collect or retain telephone records under this program. However, the changes did place additional restrictions on the ability to search the dataset as discussed below.

Metadata Queries Require Reasonable Articulable Suspicion

Telephone service providers that are served with orders issued under Section 215 are required to provide the NSA with telephony metadata pertaining to all domestic and international calls made on their networks, on an "ongoing daily" basis.[22] As this data is received by NSA, it is placed in a

[17] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-01, at n.2 (FISA Ct. January 3, 2014).

[18] *Id.*

[19] James Clapper, the Office of the Director of National Intelligence, letter to Senator Ron Wyden, July 26, 2013, available at http://www.wyden.senate.gov/news/press-releases/wyden-and-udall-important-surveillance-questions-unanswered

[20] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013.

[21] President Barack Obama, *Remarks by the President on Review of Signals Intelligence*, January 17, 2014, available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter "January 17 Remarks"].

[22] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-01, at 3 (FISA Ct. January 3, 2014). The orders last for 90 days and then must be renewed for the program to continue. *Id.* at 18.

database referred to as the "Collection Store."[23] The orders require metadata to be deleted no later than five years after they are initially collected.[24]

The FISC orders under which the telephony metadata program has operated have generally permitted searching the database for a particular number only if it can be demonstrated that there are facts giving rise to a reasonable articulable suspicion (RAS) that the telephone number in question, referred to as the "seed," is associated with one of the foreign intelligence targets referenced in the court order.[25] These targets are most commonly described as international terrorist organizations, although those portions of the FISC orders have not been declassified.[26] As used in other contexts, RAS is a less stringent standard than the "probable cause" standard that is required to be satisfied for criminal search warrants or traditional electronic surveillance under FISA.[27]

Although the RAS standard appears to have been a constant presence throughout the life of the program, the entity designated as responsible for making the RAS determination has varied over time. For most of the time between 2006 and 2014, a relatively small group of NSA personnel was charged with evaluating whether any particular query was supported by RAS.[28] However, on January 17, 2014, President Obama announced that he was directing the Department of Justice to seek a modification to the program that would require RAS determinations to be approved by the FISC prior to performing a query, except in cases of emergencies.[29] The FISC approved those modifications and assumed the RAS-determination role beginning on February 5, 2014.[30]

This arrangement was not unprecedented. Over the course of approximately six months in 2009, the FISC required RAS determinations to be made by the FISC on a case-by-case basis after instances of NSA non-compliance with the FISC's previous orders were discovered and reported to the FISC by the Department of Justice.[31] This pre-approval requirement was subsequently lifted after the FISC was satisfied that sufficient changes had been made to correct the earlier compliance violations.[32]

---

[23] *Id.* at 11.

[24] *Id.* at 14.

[25] *Id.* at 7.

[26] January 17 Remarks, *supra* note 22 (stating that "metadata that can be queried if and when we have a reasonable suspicion that a particular number is linked to a terrorist organization.").

[27] *See* U.S. v. Banks, 540 U.S. 31, 36 (2003) (forced entry into premises during execution of search warrant is permissible if there are reasonable grounds to expect futility of knocking, or if circumstances support a reasonable suspicion of exigency when the officers arrive at the door). Courts have eschewed using bright line rules to determine whether "reasonable suspicion" is warranted, and have required an examination of the totality of the circumstances instead. *See* U.S. v. Hensley, 469 U.S. 221, 227 (1985) (an informant's detailed statements implicating a third party in a bank robbery were sufficient to provide the reasonable suspicion necessary to justify a law enforcement stop of that third party); Terry v. Ohio, 392 U.S. 1, 27-28 (1968) (police officer's observation of individual repeatedly walking back and forth in front of storefronts and peering inside store windows provided reasonable belief that individuals were armed and about to engage in criminal activity justifying stop and frisk).

[28] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-01, at 7 (FISA Ct. January 3, 2014).

[29] January 17 Remarks, *supra* note 22.

[30] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things, No. BR 14-01 (FISA Ct. February 5, 2014).

[31] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 18-19 (FISA Ct. March 5, 2009).

[32] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 09-

(continued...)

Scope of Query Results Is Measured in "Hops"

Once a telephone number has been RAS-approved, it may be used as the seed of a query to the Collection Store. The response to such a query will include a list of all telephone numbers in the Collection Store that either called or were called by the seed. These telephone numbers are frequently referred to as representing the first "hop" away from the seed, because they include only telephone numbers with which the seed was in direct contact. However, the response to an RAS-approved query is not necessarily limited to first-hop results. After the program's existence was made public during the summer 2013, intelligence officials stated that responses to queries could include telephone numbers up to three hops away from the initial seed.[33] However, since the President's announcement on January 17, 2014, query results are limited to those telephone numbers that are within two hops of the initial seed.[34] All of the results that are returned from a query of the Collection Store are placed in a second database known as the "Corporate Store."[35] The FISC orders currently in effect do not require queries of the Corporate Store to satisfy the RAS standard.[36]

Fourth Amendment Challenges to Telephony Metadata Program

Upon public revelation of the NSA's bulk telephony metadata program, several lawsuits were filed in federal district courts challenging the constitutionality of this program under the Fourth Amendment's prohibition against unreasonable searches and seizures. In addition to publicly released FISC rulings on this issue,[37] four district courts have reached the merits of this Fourth Amendment question, and the U.S. Court of Appeals for the Second Circuit addressed, but did not resolve, the constitutional claims brought before it. The primary question presented to these courts is whether the bulk collection of telephone records constitutes a Fourth Amendment search, and if so, whether such a search is reasonable in light of the potential privacy interests involved and the federal government's interest in safeguarding the nation's security.[38] This question turns, in large part, on the applicability of the 1979 case *Smith v. Maryland* to the bulk collection

(...continued)

13, at 6-7 (September 3, 2009).

[33] PCLOB Report, *supra* note 2, at 31 (citing Declaration of Teresa H. Shea, Signals Intelligence Director, NSA, ACLU v. Clapper, No. 13-3994 at ¶ 24 (S.D.N.Y. Oct 1, 2013)); *see also In re* Application of the FBI for an Order Requiring the Production of Tangible Things, No. BR 14-01 at 3 (FISA Ct. February 5, 2014).

[34] January 17 Remarks, *supra* note 22.

[35] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-01, at 11 (FISA Ct. January 3, 2014).

[36] *Id.*

[37] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109 (FISA Ct. August 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf; *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-158 (FISA Ct. October 18, 2013).

[38] ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Klayman v. Obama, No. 13-0881, 2013 WL 6598728 (D.D.C. December 16, 2013). Neither the S.D.N.Y. nor D.D.C. courts addressed whether the metadata program exceeded the *statutory* authority granted by section 215's "any tangible things" provision, as both courts found that Congress impliedly precluded claims brought by third parties who may have been the subject of surveillance, but instead granted this right solely to the recipients of these orders, *i.e.*, the telephone service providers. *Clapper*, 959 F. Supp. 2d at 742; *Klayman*, 2013 WL 6598728, at *9.

program and the persuasiveness of more recent Supreme Court discussions about the effect of new technologies and prolonged government surveillance on the privacy interests of Americans.[39]

The Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]"[40] Central to the Fourth Amendment is determining whether the government has engaged in a "search," which occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable."[41] *Smith v. Maryland* was the starting point for the FISC and the federal district courts in determining whether accessing a telephone customer's phone records is a Fourth Amendment search.

In *Smith*, upon police request, the telephone company installed a pen register at its main office to determine whether Smith had called the victim of a recent robbery.[42] A pen register is simply a device for recording the outgoing numbers dialed from a telephone and does not record the content of the call.[43] The police had neither a warrant nor court order for installing this device. In a 5-3 decision, the Supreme Court held that Smith had no reasonable expectation of privacy in the telephone numbers he dialed, and, therefore, the installation of the pen register was not a Fourth Amendment search.[44] The Court grounded its holding in the proposition that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[45] Because Smith "voluntarily conveyed" the numbers he dialed to the company, he should have understood that the company would record that information as a matter of course.[46] This theory that individuals lose privacy protections when they share information with a third party (whether a private entity or the government) or where information is generated as part of a communication or transaction with a third party, has come to be known as "third-party doctrine."[47] Its application pre-dates *Smith* to a line of cases holding that the Fourth Amendment does not protect individuals from statements made to another person, even if that person turns out to be a government agent or is equipped with an electronic listening device.[48] In *Hoffa v. United States*, for example, the Court observed that the Fourth Amendment did not require the suppression of incriminating statements made by the defendant to a government informant while in a private hotel room.[49] In addition to these undercover agent cases, the third-party doctrine has been applied in various other instances of government requests for transactional records from private companies.[50] This theory has been

[39] Smith v. Maryland, 442 U.S. 735 (1979); *see generally* United States v. Jones, 132 S. Ct. 945 (2012).

[40] U.S. CONST. amend IV.

[41] Kyllo v. United States, 533 U.S. 27, 32-33 (2001).

[42] *Smith*, 442 U.S. at 737.

[43] *See* 18 U.S.C. §3127(3).

[44] *Smith*, 442 U.S. 745-46.

[45] *Id.* at 743-44.

[46] *Id.* at 744.

[47] United States v. Jones, 908 F. Supp. 2d 203, 211 (D.D.C. 2012); *see generally* CRS Report R43586, *The Fourth Amendment Third-Party Doctrine*, by Richard M. Thompson II.

[48] *See, e.g.*, On Lee v. United States, 343 U.S. 747, 748 (1952); Lopez v. United States, 373 U.S. 427, 430 (1963).

[49] Hoffa v. United States, 385 U.S. 293, 302 (1966).

[50] *See, e.g.*, Miller v. United States, 425 U.S. 435 (1976) (bank records); United States v. Starkweather, 972 F.2d 1347 (9th Cir. 1992) (utility records).

applied to non-content data, such as the to/from address line in an email,[51] but not to the content of communications, for example, the body of an email.[52]

Before the courts issued their rulings in *ACLU v. Clapper* and *Klayman*, the FISC was the first court to analyze the NSA's bulk metadata collection program under the Fourth Amendment. In conducting its review of one of the government's applications under Section 215, the FISC held that the Fourth Amendment provided no impediment to the proposed collection as *Smith* "squarely controlled" the "production of telephone service provider metadata."[53] Noting that Fourth Amendment interests are analyzed on an individual, and not group, basis, the FISC explained that "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[54]

In *ACLU v. Clapper*, Judge Pauley of the S.D.N.Y. agreed with the FISC that a constitutional analysis of Section 215 was controlled by *Smith*, that the collection of bulk records was not a search, and thus the NSA's metadata collection program did not violate the Fourth Amendment.[55] In its brief, the ACLU had argued that the bulk metadata collection amounted to the same type of privacy intrusion that led five Justices of the Supreme Court in *United States v. Jones* to suggest that long term location monitoring is a Fourth Amendment search.[56]

In *Jones*, the majority held that the physical attachment of a GPS device to an individual's car and the subsequent monitoring of information collected by that device was a Fourth Amendment search.[57] In two separate concurring opinions, five justices opined that although short term government monitoring may not exceed a person's expectation of privacy, longer term monitoring may do so, as aggregating information about a person can reflect a "wealth of detail," or mosaic, about his "familial, political, professional, religious, and sexual associations."[58] This is sometimes referred to as "mosaic theory" of the Fourth Amendment.

Like the FISC, Judge Pauley reasoned that the "collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[59] He noted that lower courts are bound to apply *Smith* unless it has been explicitly overruled by the Supreme Court itself, *Jones* notwithstanding.[60] The plaintiffs appealed this decision to the U.S. Court of Appeals for the Second Circuit.

---

[51] United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007).

[52] United States v. Warshak, 631 F.3d 266 (10th Cir. 2010).

[53] *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, at 6 (FISA Ct. 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[54] *Id.* at 9.

[55] ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

[56] Plaintiff's Memorandum of Law in Opposition to Defendant's Motion to Dismiss at 27-28, ACLU v. Clapper, No. 1:13-cv-03994 (S.D.N.Y. October 1, 2013), *available at* https://www.aclu.org/files/assets/60._pls._memo_of_law_in_opp._to_defs._mot._to_dismiss_2013.10.01.pdf.

[57] United States v. Jones, 132 S. Ct. 945, 949 (2012).

[58] 132 S. Ct. at 955 (Sotomayor, J., concurring); 132 S. Ct. at 964 (Alito, J. concurring).

[59] *Clapper*, 959 F. Supp. 2d at 752.

[60] *Id.*

On May 7, 2015, the Second Circuit held that the bulk telephone metadata program exceeded congressional authorization under Section 215 of the PATRIOT Act.[61] While the court refrained from ruling on the merits of the Fourth Amendment question raised by the plaintiffs, the opinion did note the "vexing issues" raised by such a challenge.[62] First, Judge Gerald Lynch, writing for a unanimous three-judge panel, noted the turmoil in the Supreme Court's third-party doctrine jurisprudence prompted, in part, by the concerns raised in the two *Jones* concurrences: notably, the ability of modern technology to alter traditional expectations of privacy. The court acknowledged that an expectation of privacy in an era where individuals share increasing amounts of information with both corporations and government "may seem quaint," but at the same time may become more threatened as "the extent of such information grows."[63] The court did not purport to resolve this dispute, but instead rested its decision solely on statutory grounds. Second, and perhaps, more importantly for a congressional audience, the court asserted that Congress, at least in the first instance, "is better positioned than the courts to understand and balance the intricacies and competing concerns involved in protecting our national security and to pass judgment on the value of the telephone metadata program as a counterterrorism tool."[64]

Interestingly, the Second Circuit panel observed that whether Congress has considered and authorized a program such as the telephone metadata program can be relevant to the judiciary's assessment of its constitutionality.[65] Based on this brief discussion, it is unclear whether the court was focusing on the threshold Fourth Amendment question, whether such a program constitutes a Fourth Amendment search, or the secondary issue, whether such a search was reasonable under the Fourth Amendment's general reasonableness balancing test. In any event, it was clear from the opinion that the court had kept a close eye on the legislative process surrounding FISA reform and will potentially look to Congress's action in the future in assessing the constitutionality of different iterations of this intelligence gathering program.

In a ruling on the merits mirroring that of the Southern District of New York, Chief Judge Winmill of the federal district court of Idaho upheld Section 215 against a Fourth Amendment challenge, noting that *Smith* and the third-party doctrine have not been overruled and continue to bind lower courts until the Supreme Court rules otherwise.[66] This case is currently on appeal before the U.S. Court of Appeals for the Ninth Circuit.[67] In a similar approach, but arising in a different procedural posture, the Southern District of California rejected several criminal defendants' motion for new trial after learning that data obtained under the bulk collection program may have been used in the federal government's investigation of them.[68] The district court denied their motion, observing that the use of pen registers, which the Supreme Court upheld in *Smith*, have pre-dated the digital revolution by about 150 years, negating the argument that the *Jones* concurrences' discussion of new technologies compelled a different result.[69]

[61] ACLU v. Clapper, No. 14-42-CV, 2015 WL 2097814, (2d Cir. 2015).

[62] *Id.* at *28.

[63] *Id.* at 29.

[64] *Id.* at *31.

[65] *Id.* at *31.

[66] Smith v. Obama, 24 F. Supp. 3d 1005, 1010 (D. Ida. 2014).

[67] Smith v. Obama, No. 14-35555 (9th Cir.).

[68] United States v. Moalin, No. 10-CR-4246, 2013 WL 6079518 (Nov. 18, 2013).

[69] *Id.* at *8.

In *Klayman*, Judge Leon from the DC District Court was receptive to the argument that the aggregation of telephone records can result in a Fourth Amendment search.[70] Judge Leon found that the bulk telephony metadata program was "so different from the simple pen register that *Smith* is of little value" in assessing whether the program resulted in a search.[71] Instead, the DC District Court judge found more persuasive the mosaic theory articulated in the *Jones* concurrences.[72] Acknowledging that "what metadata *is* has not changed over time," Judge Leon found that quantity of information collected and what that information can tell the government about people's lives required the court to look beyond *Smith* for its Fourth Amendment analysis.[73] Finding that this aggregation invaded a person's reasonable expectation of privacy, the court held that a Fourth Amendment search had occurred.

Finding that this metadata collection was a search, Judge Leon of the DC District Court then assessed whether that search was "reasonable" under the Fourth Amendment.[74] Noting that searches must generally be accompanied by a warrant based upon probable cause, the court assessed whether the "special needs" exception to the warrant requirement might apply to the bulk metadata program, because, again, collection under Section 215 requires neither a warrant nor probable cause. The special needs exception applies "when special needs, beyond the normal need for law enforcement, make the warrant requirement and probable-cause requirement impracticable."[75] Some examples of special needs cases include suspicionless drug testing of high school students[76] and railroad personnel,[77] automobile checkpoints for illegal immigrants[78] and drunk drivers,[79] and the search of airplane,[80] subway,[81] and train passengers' carry-on bags.[82] In each, the government's interest went beyond a general interest in law enforcement to broader governmental needs. Even where the government can claim a special need beyond ordinary law enforcement interests, a reviewing court must balance the privacy interests of the individual with the government's interest to determine whether a warrant or individualized suspicion is required.[83] In making this determination, a court must consider (1) "the nature of the privacy interest upon which the search [] at issue intrudes"; (2) "the character of the intrusion that is complained of"; and (3) "the nature and immediacy of the governmental concern, ... and the efficacy of this means for meeting it."[84] Judge Leon accepted that the plaintiffs had significant privacy interests in the aggregation of their telephone data and that the government's interest in identifying unknown terrorists was of the "highest order."[85] Turning to the efficacy of the

[70] Klayman v. Obama, No. 13-0881, 2013 WL 6598728, *18 (D.D.C. December 16, 2013).

[71] *Id.* at *19.

[72] *Id.* at 955 (Sotomayor, J., concurring); *Id.* at 964 (Alito, J. concurring).

[73] *Klayman*, 2013 WL 6598728, at *21

[74] *Id.* at *22.

[75] Vernonia Sch. Dist. 47J v. Acton, 515 U.S 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

[76] *Id.* at 664-665.

[77] Skinner v. Railway Labor Executives' Assoc., 489 U.S. 602, 633 (1989).

[78] United States v. Martinez-Fuerte, 428 U.S. 543, 556-57 (1976).

[79] Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

[80] United States v. Edwards, 498 F. 2d 496, 500 (2d Cir. 1974).

[81] MacWade v. Kelly, 460 F.3d 260, 275 (2d. Cir. 2006).

[82] Cassidy v. Chertoff, 471 F.3d 67, 87 (2d. Cir. 2006) (Sotomayor, J.).

[83] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 664-66 (1989).

[84] *Vernonia Sch. Dist. 47J*, 515 U.S at 656-60.

[85] *Klayman*, 2013 WL 6598728, at *23.

program, the court questioned whether the program has "actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time sensitive in nature."[86] Doubting the metadata program has significantly aided the government in conducting time-sensitive terrorism investigations, and in light of the serious privacy intrusions found, the court concluded that the bulk metadata program was unreasonable under the Fourth Amendment.[87] The government appealed this decision, which is currently pending before the U.S. Court of Appeals for the District of Columbia Circuit.[88]

Section 215 of the PATRIOT Act is set to expire on June 1, 2015.[89] Depending on whether Section 215 lapses or is modified, pending cases challenging the telephone metadata program could be rendered moot.

PRISM and Upstream Acquisition of Internet Communications

Contemporaneously with the origination of the telephony metadata program in 2001, the NSA also began acquiring Internet-based communications of overseas targets without the use of a traditional law enforcement warrant or an electronic surveillance order under Title I of FISA.[90] Ultimately, new statutory authority for this type of acquisition was provided, at first, temporarily under the Protect America Act (PAA) of 2007;[91] and on a longer term basis by the FAA.[92]

According to a partially declassified 2011 opinion from the FISC, NSA collected 250 million Internet communications per year under this program.[93] Of these communications, 91% were acquired "directly from Internet Service Providers," referred to as "PRISM collection."[94] The other 9% were acquired through what NSA calls "upstream collection," meaning acquisition while Internet traffic is in transit from one unspecified location to another.[95] NSA also has two methods for collecting information about a specific target: "to/from" communications collection, in which the target is the sender or receiver of the Internet communications; and "about" communications collection, in which the target is only mentioned in communications between non-targets.[96] The Obama Administration also acknowledged to the FISC that technical limitations in the "upstream" collection result in the collection of some communications that are

[86] *Id.* at *24.

[87] *Id.*

[88] *See* Klayman v. Obama, No. 14-5004 (D.C. Cir.).

[89] *See supra* note 12.

[90] Unclassified Declaration of Frances J. Fleisch, National Security Agency, Schubert v. Obama, No. 07-cv-0693-JSW at ¶ 32 (N.D. Cal. December 20, 2013) available at http://icontherecord.tumblr.com.

[91] P.L. 110-55.

[92] P.L. 110-261.

[93] Foreign Intelligence Surveillance Court Memorandum Opinion, at 29 (FISA Ct. October 3, 2011) (Bates, J.).

[94] *Id.* at 29-30.

[95] *Id*. at n.24.

[96] *Id*., at 15.

unrelated to the target or that may take place entirely between persons located in the United States.[97]

The PRISM and upstream collections differ from the telephony metadata program in two key respects. First, the PRISM and upstream collections acquire the contents of those communications. Second, as this program targets the "to/from" and "about" communications of foreigners who are abroad, the collection of Internet-based communications may be considered by some to be more discriminating than the bulk collection of telephony metadata.

Overview of Section 702

Section 702 of FISA, as added by the FAA, permits the Attorney General (AG) and the DNI to jointly authorize targeting of non-U.S. persons reasonably believed to be located outside the United States.[98] Once authorized, such acquisitions may last for periods of up to one year. Under Subsection 702(b) of FISA, such an acquisition is also subject to several limitations. Specifically, an acquisition

- may not intentionally target any person known at the time of acquisition to be located in the United States;
- may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- may not intentionally target a U.S. person reasonably believed to be located outside the United States;
- may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.[99]

Traditional FISA orders authorizing electronic surveillance generally require the FISC to find, *inter alia*, that probable cause exists to believe that the particular target of the proposed surveillance is a foreign power or an agent of a foreign power.[100] In contrast, under Section 702, individual targets of surveillance are not necessarily reviewed by the FISC prior to acquisition of their communications. Instead, the FISC's role is largely limited to reviewing the targeting and minimization[101] procedures that the government proposes to use to target and acquire communications prospectively. In order to be approved, Section 702 requires the targeting procedures be reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States and to prevent the intentional

[97] *Id.* at 5, 29-33.

[98] 50 U.S.C. §1881a.

[99] 50 U.S.C. §1881a(b).

[100] 50 U.S.C. §1805(a)(2). As defined by FISA, the term "foreign power" includes international terrorist organizations. 50 U.S.C. §1801(a)(4).

[101] Minimization procedures generally provide standards governing the circumstances under which particular communications may be acquired, used, and shared.

acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States.[102] The court must also find that the minimization procedures are reasonably designed to minimize the retention, and prohibit the dissemination, of information that is about a U.S. person or that could identify a U.S. person.[103] However, the minimization procedures may allow for the retention and dissemination of information, including U.S. person information, that is evidence of a crime.[104]

Constitutional Challenges to Acquisition of Internet Communications

Constitutional challenges to the NSA's acquisition of Internet communications of overseas targets under FISA have arisen in a number of different contexts. First, such challenges have arisen in the FISC and FISCR as part of those courts' roles in approving the parameters of these collection activities. Secondly, constitutional challenges have been brought in traditional federal courts as civil actions by plaintiffs asserting an injury or in criminal proceedings by defendants who have been notified that evidence against them was obtained or derived from collection under Section 702.

FISCR Protect America Act Litigation

Prior to the enactment of Section 702, a similar joint authorization procedure created under the PAA was upheld by the FISCR in 2008.[105] This suit arose out of the objection of an Internet service provider (ISP) to a directive the company had received ordering it to assist in surveillance activities under the PAA. Under a theory of third-party standing, the ISP was able to raise the Fourth Amendment privacy rights of its customers.[106] Under Fourth Amendment case law, unless an exception applies, the government must obtain a warrant to conduct electronic surveillance, as this type of investigation invades an individual's reasonable expectation of privacy.[107] Although the Supreme Court has declined to address whether there is a foreign intelligence exception to the Fourth Amendment that would permit the executive to engage in warrantless electronic surveillance,[108] the FISCR had previously suggested that such an exception applied to surveillance conducted under traditional FISA authorities.[109]

When this question was presented to the FISCR in the context of the PAA, the court formally recognized a foreign intelligence exception based upon principles supporting the "special needs" exception that has been developed in other contexts.[110] Generally, the special needs exception

[102] 50 U.S.C. §1881a(d) The certification must also attest that guidelines have been adopted to ensure that the specifically prohibited types of surveillance activities listed in §702(b), such as reverse targeting, are not conducted.

[103] 50 U.S.C. §1881a(e).

[104] *Id.*

[105] In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009-1016 (FISA Ct. Rev. 2008) (upholding similar joint authorization procedure under the Protect America Act in the face of a Fourth Amendment challenge brought by telecommunications provider).

[106] *Id.* at 1009.

[107] *See* Berger v. New York, 388 U.S. 41 (1967); United States v. Warshak, 631 F.3d 266 (10th Cir. 2010).

[108] *See* United States v. United States District Court (Keith Case), 407 U.S. 297 (1972).

[109] *In re* Sealed Case, 310 F.3d 717, 721 (FISA Ct. Rev. 2002).

[110] The special needs exception is also discussed in the context of the telephone metadata program *supra*, at "Fourth (continued...)

may excuse the warrant requirement when the purpose behind governmental action goes beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose.[111]

As applied to the joint authorization procedure in the PAA, the court found that the acquisition of foreign intelligence information went "well beyond garden-variety law enforcement" purposes.[112] Furthermore, the court found a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and that this would impede the vital national security interests at stake.[113]

Although no warrant was required by the Fourth Amendment, the court did hold that the Fourth Amendment still required the surveillance to be reasonable, based on the totality of the circumstances.[114] Finding the government's interest in national security to be of the highest order, the court held that protections contained in the PAA, in light of this very important government interest, reasonably offset the lack of particularity or prior judicial review of the authorized surveillance.[115]

2011 FISC Opinions

In August 2013, the Obama Administration partially declassified several opinions of the FISC regarding collection activities under Section 702.[116] The first of these opinions, dated October 3, 2011, evaluated the targeting and minimization procedures proposed by the government to deal with new information regarding the scope of upstream collection. Specifically, the government had recently discovered that its upstream collection activities had acquired unrelated international communications as well as wholly domestic communications due to technological limitations.

After being presented with this new information, the FISC found the proposed minimization procedures to be deficient on statutory[117] and constitutional[118] grounds. With respect to the statutory requirements, the FISC noted that the government's proposed minimization procedures were focused "almost exclusively" on information that an analyst wished to use and not on the larger set of information that had been acquired. Consequently, communications that were known to be unrelated to a target, including those that were potentially wholly domestic, could be

(...continued)

Amendment Challenges to Telephony Metadata Program."

[111] *Vernonia*, 515 U.S at 653, *supra* note 67.

[112] *In re* Directives, 551 F.3d at 1011.

[113] *Id.*

[114] *Id.* at 1012.

[115] *Id.* at 1016.

[116] *See* Office of the DNI, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, August 21, 2013, available at http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

[117] Foreign Intelligence Surveillance Court Memorandum Opinion, at 59-63, 67-80 (October 3, 2011).

[118] *Id*, at 67-79 (October 3, 2011). The FISC upheld the targeting provisions, even though the government acknowledged that its upstream collection activities were known to acquire some wholly domestic communications. The FISC found that this was not a violation of §702, since the government could not determine "at the time of acquisition" whether a particular communication was wholly domestic. Foreign Intelligence Surveillance Court Memorandum Opinion, at 46-47 (October 3, 2011).

retained for up to five years so long as the government was not seeking to use that information. The court found that this had the effect of maximizing the retention of such information, and was not consistent with FISA's mandate to minimize the retention of U.S. person information.[119]

The FISC also held that the proposed minimization procedures did not satisfy the Fourth Amendment.[120] Notably, it applied the same analysis used by the FISCR in the PAA litigation, but found that, under the facts before it, the balance required under the Fourth Amendment's reasonableness test did not favor the government, particularly in light of the statutory deficiencies.[121]

Following the FISC's determination that the Fourth Amendment had been violated, the government presented revised minimization procedures to the FISC, and the court approved those procedures on November 30, 2011.[122] The revised minimization procedures addressed the court's concerns by requiring the segregation of those communications most likely to involve unrelated or wholly domestic communications; requiring special handling and markings for those communications which could not be segregated; and reducing the retention period of upstream collection from five years to two.[123] With these modifications, the court found that the balancing test required under the Fourth Amendment supported the conclusion that the search was constitutionally permissible.[124]

Clapper v. Amnesty International[125]

Upon enactment of Section 702, a number of non-profit organizations brought suit challenging the joint authorization procedure for surveillance of non-U.S. persons reasonably believed to be abroad. The suit centrally alleged that this authority violated the Fourth Amendment's prohibition against unreasonable searches. In order to establish legal standing to challenge Title VII, the plaintiffs had argued that the financial costs they incurred in order to avoid their fear of being subject to surveillance constituted a legally cognizable injury. However, on February 26, 2013, in *Clapper v. Amnesty International*, the U.S. Supreme Court held that the plaintiffs had not suffered a sufficiently concrete injury to have legal standing to challenge Title VII.[126] Specifically, the Court held that in order to obtain injunctive relief from a federal court a plaintiff must prove with "specific facts" that he had been injured or that his injury would be "certainly impending" because of the challenged action.[127] The High Court reasoned that because the non-profit organizations could not prove with specificity that it was "certainly impending" that the United

[119] *Id.* at 59.

[120] *Id.* at 67-79.

[121] *Id.* at 68, 75-78.

[122] Foreign Intelligence Surveillance Court Memorandum Opinion, at 11-15 (November 30, 2011).

[123] *Id.* at 7-11.

[124] *Id.* at 14-15. A third declassified order from September of 2012 addressed the question of what to do with the information that had been acquired through upstream collection prior to the October 2011 opinion. In this third opinion, the FISC acknowledged that the NSA had made a "corporate decision" to purge all data identified as originating from upstream collection before October 31, 2011 (the date that the revised minimization procedures went into effect). Foreign Intelligence Surveillance Court Memorandum Opinion, at 11-15 (September 2012).

[125] For a more in depth discussion of *Clapper v. Amnesty International*, *see* CRS Report R43107, *Foreign Surveillance and the Future of Standing to Sue Post-Clapper*, by Andrew Nolan.

[126] Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013).

[127] *Id.*at 1149, n.4.

States would utilize Section 702 to intercept the plaintiffs' conversations, the plaintiffs lacked standing to bring their case.[128] Because the Court did not have jurisdiction to proceed to the merits of the plaintiffs' claims, the Court did not decide the Fourth Amendment question.

Criminal Defendants

The litigation in *Clapper*, while preventing a facial challenge to Section 702 by a group of non-profit organizations that allegedly worked with clients who could have been subject to surveillance done pursuant to Title VII, may have resulted in a new series of challenges to the FAA by certain criminal defendants. In October 2012, during oral argument before the High Court in *Clapper*, the Solicitor General, in responding to a question posed by Justice Sotomayor, stated that the government was providing notice to criminal defendants that evidence derived from Section 702 surveillance would be used in the criminal case, allowing the defendant to challenge the lawfulness of that provision.[129] The Solicitor General's response appears to have been prompted by a provision in FISA requiring the government, whenever it "intends to enter into evidence or otherwise use or disclose ... any information obtained or derived from an electronic surveillance ... [done] pursuant to" FISA, to "notify the aggrieved person and the court" "that the Government intends to so disclose or use such information."[130] In turn, once a criminal defendant is provided with such a notification, the defendant has the opportunity to ask a court to suppress the evidence that was "unlawfully acquired."[131] While the *Clapper* Court dismissed the case on standing grounds, the Supreme Court did so in part relying on the fact that a criminal defendant could potentially have standing to challenge Section 702 because of the notification provision.[132] In the wake of *Clapper*, the Solicitor General reportedly examined the Justice Department's notification policy and discovered that the policy required telling criminal defendants that incriminating evidence was gathered pursuant to surveillance conducted under FISA, but did not specifically mention that the surveillance was conducted under Title VII.[133] As a result of this discovery, the Department of Justice reportedly altered its disclosure policy,[134] resulting in the filing of several notifications to criminal defendants that the government intends to utilize inculpatory evidence that was obtained or derived pursuant to the authority provided under Section 702.[135] In three cases, a criminal defendant has responded to the government's

[128] *Id.* at 1148 ("[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.").

[129] *See* Transcript of Oral Argument at 4, Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2012).

[130] 50 U.S.C. §1806(c).

[131] *Id.*

[132] 133 S. Ct. at 1154 ("[O]ur holding today by no means insulates §1881a from judicial review ... if the Government intends to use or disclose information obtained or derived from a §1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition.").

[133] *See* Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, October 26, 2013, *available at* http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?hp&_r=0.

[134] *Id.*

[135] *See generally* Patrick C. Toomey, In Reversal, DOJ Poised to Give Notice of Warrantless Wiretapping, ACLU BLOG OF RIGHTS (October 18, 2013, 5:01 PM), *available at* https://www.aclu.org/blog/national-security/reversal-doj-poised-give-notice-warrantless-wiretapping; *see, e.g.,* United States v. Hasbarjrami, Case No. 1:11-cr-0623, Docket #65, (E.D.N.Y. Feb. 24, 2104); United States v. Mihalik, Case No. 2:11-cr-00833, Docket #145 (C.D. Cal. April, 4, 2014); United States v. Khan, Case No. 3:12-cr-00659, Docket #59 (D. Ore. April, 3, 2014); United States v. Mohamud, Case. No. 3:10-cr-00475, Docket #486 (D. Ore. Nov. 19, 2013); United States v. Muhtorov, 1:12-cr-00033, (continued...)

notification, utilizing FISA's provision allowing the suppression of any evidence "unlawfully acquired" under statute, by challenging the constitutionality of Section 702.[136]

Unlike the litigation in the FISA Courts over the constitutionality of the PAA and the FAA, the litigation resulting over the suppression of evidence derived from Section 702 authorities is not isolated to the Fourth Amendment issue. In addition to the question of whether Section 702 violates the Fourth Amendment's prohibition on unreasonable searches and seizures, criminal litigation over Title VII also challenges whether Section 702 violates Article III of the Constitution.[137] Article III of the Constitution vests the "judicial power" of the United States in the Supreme Court and any inferior courts established by Congress,[138] including the FISC.[139] The Constitution limits the exercise of the "judicial power" to the adjudication of "cases" or "controversies,"[140] and the case-or-controversy limitation has been the impetus of several rules of justiciability that restrict the court's power and curb Congress's ability to regulate federal courts.[141] With respect to an Article III challenge to Section 702, relying on case law holding that the constitutional case-or-controversy requirement restricts a federal court to adjudicating live disputes that are "definite and concrete"[142] and prevents an Article III court from issuing "advisory opinions,"[143] critics of Section 702 argue that Title VII requires a federal court to "evaluat[e] in a vacuum" the legal propriety of the government's targeting and minimization procedures without regard to how the government would be utilizing their FAA authorities in a specific surveillance action.[144] Whether such an abstract assessment of the government's surveillance procedures is a constitutionally appropriate role for a federal court may largely depend on how broadly Supreme Court decisions allowing Article III courts to "perform a variety of functions not necessarily or directly connected to adversarial proceedings in a trial or appellate

(...continued)

Docket #457 (D. Colo. Oct. 25, 2013).

[136] *See* United States v. Hasbarjrami, Case No. 1:11-cr-0623, Docket #92, (E.D.N.Y. Nov. 26, 2014); United States v. Muhtorov, Case No. 12-CR-00033, Docket #520 (D. Colo. January 29, 2014); United States v. Mohamud, Case. No. 3:10-cr-00475, Docket #503 (D. Ore. April 4, 2014).

[137] *Id.* at 44.

[138] *See* U.S. CONST. art. III, §1.

[139] Case law uniformly agrees that the FISA courts are courts established under Article III of the Constitution. *See* United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) (Kennedy, J.) ("[Appellant] ... appears to suggest that the FISA court is not properly constituted under [A]rticle III because the statute does not provide for life tenure on the FISA court. This argument has been raised in a number of cases and has been rejected by the courts. We reject it as well."); *In re* Kevork, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985) ("The FISA court is wholly composed of United States District Court judges, who have been appointed for life by the President, with the advice and consent of the Senate, and whose salaries cannot be reduced. The defendants' contentions that because of their limited term on the FISA court, these judges lose their Article III status, has no merit."); United States v. Megahey, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1180) (same); United States v. Falvey, 540 F. Supp. 1306, 1313 n.16 (E.D.N.Y. 1982) (same); *In re* Release of Court Records, 526 F. Supp. 2d 484, 486 (FISA Ct. 2007) ("Notwithstanding the esoteric nature of its caseload, the FISC is an inferior federal court established under Article III.").

[140] U.S. CONST. art. III, §2; *see* United States v. Morton Salt Co., 338 U.S. 632, 641-42 (1950) ("Federal judicial power itself extends only to adjudication of cases and controversies.... ").

[141] *See generally* CRS Report R43362, *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes*, by Andrew Nolan and Richard M. Thompson II, at pp. 6-9.

[142] *See* Aetna Life Ins. Co. v. Haworth, 300 U.S. 227, 240-41 (1937).

[143] *See* Chi. & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 113 (1948).

[144] *See* Defendant's Motion to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act and Motion for Discovery, United States v. Muhtorov, Case No. 12-CR-00033-JLK-1, at *45 (D. Colo. January 29, 2014).

court" are read.[145] Moreover, while case law rejecting an Article III case-or-controversy challenge with respect to traditional FISA electronic surveillance orders did so because the *ex parte* review of a foreign surveillance application was viewed as presenting the court with "concrete questions" in a form that a judge was "capable of acting on,"[146] it remains to be seen whether the Supreme Court would find judicial review of the government's targeting and minimization procedures under the FAA equally untroubling.[147]

To date, one federal court has issued a written opinion[148] with respect to a suppression motion challenging the constitutionality of the FAA. Specifically, in *United States v. Mohamud,* a district court denied the suppression motion of a criminal defendant against whom the government intended to use evidence obtained under the FAA in a prosecution for violating 18 U.S.C. §2332a(a)(2)(A), attempting to use a weapon of mass destruction.[149]

With regard to the constitutionality of Section 702 vis-à-vis Article III, the Oregon court concluded that Congress, in the FAA, provided an "intelligible principle" by which the FISA court could evaluate the legality of the government's targeting and minimization procedures,[150] making Article III review procedures under the FAA akin to other traditional non-adjudicative functions of federal courts, like the review of wiretap applications, where a "neutral and detached" federal judge evaluates whether the government's conduct comports with the Constitution.[151]

With regard to the defendant's Fourth Amendment challenge, the district court held that the warrant requirement does not apply to the incidental interception of U.S. persons' communications as part of electronic surveillance targeting non-U.S. persons overseas to obtain foreign intelligence information.[152] Alternatively, the court held, like the FISCR in its 2008 decision, that the foreign intelligence exception permitted the government to conduct surveillance under the FAA without a warrant.[153] Applying a similar balancing test as the FISCR, the district court found that the privacy interests implicated by the incidental collection of U.S. persons'

[145] *See* Mistretta v. United States, 488 U.S. 361, 389 n.16 (1989).

[146] *See* United States v. Megahey, 553 F. Supp. 1180, 1196 (E.D.N.Y. 1982) (citing *In re* Summers, 325 U.S. 561, 567 (1945)).

[147] There may be other arguments as to why §702 raises Article III questions. For example, pursuant to §702, if a certification filed in order to obtain foreign intelligence surveillance information is rejected by the FISC, the government can automatically continue the acquisition of such material pending an appeal to the FISCR, 50 U.S.C. §1881a(i)(4)(B), potentially calling into question whether Title VII allows the FISC to issue "dispositive" "final" judgments in line with Article III's requirements. *See* Plaut v. Spendthrift Farm, 514 U.S. 211, 219 (1995) (holding that the judicial power is "to render dispositive judgments"); *but see* Miller v. French, 530 U.S. 327, 346-49 (2000) (upholding automatic stay provision in the Prison Litigation Reform Act against Article III challenge). For an extended discussion on whether automatic stays violates Article III, *see* CRS Report R43260, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate*, by Andrew Nolan, Richard M. Thompson II, and Vivian S. Chu, at pp. 46-47.

[148] A court in the Eastern District of New York appears to have issued an oral decision with respect to the constitutionality of section 702, denying a suppression motion challenging the constitutionality of section 702. *See* United States v. Hasbarjrami, Case No. 1:11-cr-0623, Docket #116 (E.D.N.Y. Mar. 20, 2015). As of the date of this report, the transcript of the oral decision is not available to the public. *Id.*

[149] *See* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *1 (D. Or. June 24, 2014)

[150] *Id.* at *10.

[151] *Id.* at *11.

[152] *Id.* at *15.

[153] *Id.* at *18.

communications did not outweigh the government's interest in protecting the nation's security. Further, the court observed that the "numerous safeguards built into the statute," most importantly the minimization and targeting procedures required by the FAA, bolstered the reasonableness of the surveillance program.[154] The defendant in *Mohamud* appealed his judgment in October 2014, and the appeal is currently pending before the Ninth Circuit Court of Appeals.[155]

Author Contact Information

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

Andrew Nolan
Legislative Attorney
anolan@crs.loc.gov, 7-0602

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

[154] *Id.* at

[155] *See* United States v. Mohumud, No. 14-30217 (9th Cir.).