UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA,

- against - 11 Cr. 623 (JG)

AGRON HASBAJRAMI,

Defendant.

----------X

DEFENDANT AGRON HASBAJRAMI'S PRETRIAL OMNIBUS MOTIONS AND INCORPORATED MEMORANDUM OF LAW IN SUPPORT THEREOF

STEVE ZISSOU, ESQ.
42-40 Bell Blvd., Suite 302
Bayside, New York 11361
(718) 279-4500

MICHAEL K. BACHRACH, ESQ.
276 Fifth Avenue, Suite 501
New York, New York 10001
(212) 929-0592

Attorneys for Defendant Agron Hasbajrami

Also on the brief: Joshua L. Dratel, Esq.

Table of Contents

Table of Authorities

CASES

STATUTES AND OTHER AUTHORITIES

Press Release, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)* (Aug. 21, 2013) 78

DEFENDANT AGRON HASBAJRAMI'S
PRETRIAL OMNIBUS MOTIONS

I. Preliminary Statement

On October 2, 2014, this Court concluded, inter alia, that Defendant Agron Hasbajrami (hereinafter, "Hasbajrami") could "withdraw his plea of guilty because [this Court] conclude[d] that he was not sufficiently informed about the facts," namely, "a DOJ policy that transcended this case," which deprived him of the ability to make "an intelligent decision about whether to plead guilty" (Order, dated, October 2, 2014 [*ecf* #85], at 6).

Such policy, of course, was the Government's system-wide decision to omit reference to warrantless surveillance under the FISA Amendments Act (hereinafter, the "FAA") when providing notice of with-warrant surveillance under the Foreign Intelligence Surveillance Act (hereinafter, "FISA") (id. at 6).

While this Court's order "express[ed] no view whatsoever on the merits of a constitutional challenge to the FISA amendments" (id. at 7), this Court recognized that various per se and as applied challenges could be raised (id. at 8) and permit Hasbajrami to withdraw his plea so that he could be returned to a position to do so.

As such, Hasbajrami, by and through his attorneys, hereby moves to suppress the fruits of warrantless FAA surveillance related to his case and for other relief as detailed in the following motions:

1. Motion to suppress the fruits of FAA surveillance due to the per se unconstitutionality of the statute and its application herein;

2. Motion to suppress the fruits of FAA surveillance irrespective of the constitutionality of the statute;

3. Motion to suppress the fruits of FAA surveillance due to outrageous government conduct;

4. Motion to suppress Hasbajrami's post-arrest statements;

5. Motion for discovery of material and information necessary to determine whether the Government's specific conduct in this case violated the statutory requirements of FISA, the FAA, and/or any other surveillance statute or program relied upon during the investigation of this case, as well as to determine whether the Government's specific conduct violated Hasbajrami's right to Due Process under the Fifth Amendment;

6. Motion for an order directing the Government to identify any and all witnesses that it learned of during, or as a result of, the interrogation of the defendant;

7. Motion for an order directing the Government to specify all evidence that is subject to suppression and/or preclusion as a result of the interrogation of the defendant;

8. Motion for an order directing the Government to provide immediate notice of expert witnesses it intends to rely upon at trial;

9. Motion for immediate production of Brady/Giglio material;

10. Motion for early disclosure of 3500 material;

11. Motion for notice of evidence the Government intends to offer under Fed.R.Evid. 404(b); and

12. Motion for leave to submit further motions.

II. Background

Agron Hasbajrami was arrested on September 6, 2011, and ultimately charged with three counts of provision and attempted provision of material support to terrorists, and one count of attempt to provide material support to terrorists, all in violation of 18 U.S.C. §§ 2339A(a), 2. See Superseding Indictment, dated, January 26, 2012.

As described in Hasbajrami's Revised Pre-Sentence Report, dated, February 6, 2013 (hereinafter, "PSR"):

> An investigation by agents with the Federal Bureau of Investigation's Joint Terrorism Task Force ("JTTF") revealed that between April 2, 2011, and August 28, 2011, the defendant engaged in numerous email transactions with individual #1, utilizing different email accounts. Individual #1 (whose identity is known to the parties), is an individual the defendant believed was associated with a terrorism organization. During the course of their emails, the two arranged for the transfer of money from the defendant to individual #1, purportedly to support Islamic fundamentalist terrorism operations, and to arrange for the defendant's travel to the Federally Administered Tribal Areas ("FATA's") of Pakistan to join a jihadist fighting group. More specifically, the emails discussed and contained instructions and detailed descriptions of the smuggling route that the defendant was to take into the FATA, as well as contact instructions as to how the defendant would make contact with individual #1 once he arrived in the FATA, and how money should be sent to individual #1 from the United States, via a courier in Germany….
>
> Notwithstanding the emails discussed … above … there is information to suggest that Individual #1 was not in fact a

> terrorist, and that he solicited funds from the defendant for purposes unrelated to terrorism.
>
> Ultimately, the defendant was arrested by JTTF agents at John F. Kennedy International Airport in Jamaica, New York, on September 6, 2011, prior to boarding a flight bound for Istanbul, Turkey. A search of the defendant's luggage subsequent to his arrest revealed a tent, boots and cold-weather gear. The case agent advised that in a post-arrest statement, the defendant admitted to the entirety of the offense.

(PSR at ¶¶ 2-3) (footnotes omitted).

Upon information and belief, the Government's case against Hasbajrami will be based primarily upon the communications initially derived as a result of warrantless FAA surveillance (e.g., the emails described above) as well as the defendant's post-arrest statements. Although the Government will argue that the emails (and any other information not yet disclosed) were later obtained (or re-obtained) pursuant to Title I or Title III surveillance under FISA, the Government will be unable to avoid the conclusion that its FISA warrants were the derivate fruit of warrantless FAA surveillance.

As such, upon information and belief, all of the evidence against Hasbajrami will be shown to have been derived through warrantless surveillance, and it appears that none of it would have been inevitably discovered had the warrantless surveillance never occurred. What, if any, evidence survives the instant motions will then determine whether there exists sufficient admissible evidence to sustain

the charges against Hasbajrami.

III. Suppression Motions

First Motion

MOTION TO SUPPRESS THE FRUITS OF FAA SURVEILLANCE DUE TO THE PER SE UNCONSTITUTIONALITY OF THE STATUTE AND ITS APPLICATION HEREIN

A. Introduction

On February 24, 2014, the Government provided notice that it intended – and presumably still intends – "to offer into evidence or otherwise use or disclose in proceedings in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a [i.e., the FAA]" (Gov't letter [*ecf* #65] at 1).

Moreover, as explained by the Government, the "evidence and information, obtained or derived from Title I or III FISA collection, that the government intend[s] to offer into evidence or otherwise use or disclose in proceedings in this case was derived from acquisition of foreign intelligence information conducted pursuant to the FAA." Id.

As a result, Hasbajrami is an "aggrieved person" within the plain meaning of FISA and the FAA. See 50 U.S.C. § 1801(k) (" 'Aggrieved person' means a person who is the target of an electronic surveillance or any other person whose

communications or activities were subject to electronic surveillance.").

50 U.S.C. § 1881a, which is also known as Section 702 of FISA, was enacted in 2008 as part of the FISA Amendments Act (the FAA). Section 702, which is the element of the FAA referred to herein when we refer to the FAA, is viewed by many commentators, academics, and others, as an unprecedented degradation of the privacy rights of Americans, both U.S. citizens and U.S. lawful permanent residents, with none of the protections that the Fourth Amendment requires to limit governmental intrusions on privacy.

The statute violates the Fourth Amendment and is therefore unconstitutional because it:

- fails to provide judicial review of specific instances of searches and seizures of the personal communications of U.S. persons (i.e., U.S. citizens and U.S. lawful permanent residents, all of whom possess the same rights under the Fourth Amendment);

- fails to require probable cause, or any level of suspicion, before the Government can search, seize, retain, and later access those communications;

- fails to require specificity regarding the individual targeted by – or the facility to be accessed during – the electronic surveillance;

- limits the Foreign Intelligence Surveillance Court's authority to insist upon, and eliminates its authority to supervise, instance-specific privacy-intrusion minimization procedures; and

- fails to provide any accountability regarding the Government's surveillance of the electronic communications of U.S. persons while at the same time exceeding traditional constitutional and statutory

boundaries.

The following chart, initially created earlier this year by the Federal Defenders Office for its post-trial motions in United States v. Mohamed, 10 Cr. 475 (KI) (D.Oregon), demonstrates how the FAA differs from other electronic surveillance statutes – traditional FISA and Title III wiretaps – in terms of what information must be presented to a neutral and detached judicial officer in order to obtain authorization to execute specific search and seizures:

	Title III	Traditional FISA	FAA
Required level of suspicion of an individual	Probable cause the individual is committing, has committed, or is about to commit a criminal offense. See 18 U.S.C. § 2518(3)(a).	Probable cause the individual is a foreign power (including terrorist organizations) or an agent of a foreign power. See 50 U.S.C. § 1805(a)(2)(A).	None
Required level of suspicion regarding facility to be monitored	Probable cause communications concerning an offense will be obtained through interception. See 18 U.S.C. § 2518(3)(b).	Probable cause each targeted facility is being used, or is about to be used, by a foreign power or an agent of a foreign power. See 50 U.S.C. § 1805(a)(2)(B).	None
Particularity regarding individual to be monitored	Specify the identity, if known, of the person committing the offense or whose communications are to be intercepted. See 18 U.S.C. § 2518(1)(b).	Specify the identity, if known, or a description of the specific target of the surveillance. See 50 U.S.C. § 1805(c)(1)(A).	None

Particularity regarding location to be monitored	Specify the nature and location of the communications facilities as to which, or the place where, interception will occur. See 18 U.S.C. § 2518(1)(b).	Specify the nature and location of each of the facilities or places at which the surveillance will be directed. See 50 U.S.C. § 1805(c)(1)(B).	None
Particularity regarding types of communications to be intercepted	Particular description of the type of communication sought to be intercepted. See 18 U.S.C. § 2518(1)(b).	Designate the type of foreign intelligence information being sought and the type of communications or activities to be subjected to the surveillance. See 50 U.S.C. § 1805(c)(1)(C).	None

As will be discussed in further detail below, because the FAA does not provide sufficient Fourth Amendment protections to the private communications of U.S. persons the statute is unconstitutional. Consequently, and for the reasons that follow, we respectfully submit that the fruits of all warrantless FAA surveillance must be suppressed in this case and thus precluded from being introduced against Hasbajrami at trial.

This includes, inter alia: the following categories of evidence and information:

- all evidence and information derived as a result of Title VII warrantless FAA surveillance;
- all evidence and information "obtained or derived from Title I and Title III FISA collection … [that was] itself also derived from other

collection pursuant to Title VII" of the FAA (Gov't letter [*ecf* #65] at 1);

- Hasbajrami's custodial statements;
- and any other evidence and information that the Government could not have obtained in this case through an independent source, see Nardone v. United States, 308 U.S. 338, 341 (1939).

As such, and for the reasons that follow, we respectfully submit that suppression is warranted under the Fourth Amendment as fruit of the poisonous tree. See Murray v. United States, 487 U.S. 533, 536-37 (1988); see also 50 U.S.C. § 1806(g) ("If the United States district court … determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance….").

B. Background of Warrantless FAA Surveillance

Congress enacted FISA in 1978 in response to outcries over unlawful warrantless intrusions on the privacy of American citizens conducted in the name of national security. See Kris & Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, § 2:7 (2d ed. 2012). Congress found that the Government, in the name of national security, had "violated specific statutory prohibitions," "infringed the constitutional rights of American citizens," and "intentionally disregarded" legal limitations on surveillance, including pursuing "a 'vacuum cleaner' approach to intelligence collection" that sometimes intercepted

the content of Americans' communications under the pretext of targeting foreigners. Final Report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Book II, S.Rep.No. 94-755, at 137, 165 (1976), available at <http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf> (last accessed, November 24, 2014). While protecting the public was a central concern, the purpose of FISA was to rein in extra-legal activities by bringing Governmental surveillance within the rule of law.

In addition, the Supreme Court, in United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 313 (1972) (hereinafter, "Keith") ruled that domestic national security wiretapping was governed by the Fourth Amendment, and that as a result a warrant was required. The Court specifically left open the question of foreign intelligence information, and FISA represented an effort to codify the means for collecting foreign intelligence information within the United States.

In 2008, the FAA radically increased the Government's ability to search and seize the private electronic communications of U.S. citizens and all those protected by the Fourth Amendment. While FISA itself represented an innovation with respect to the concepts of probable cause and electronic eavesdropping warrants removing the requirement of probable cause of criminal activity and dispensing with many of other substantive and procedural requirements present in Title III, the FAA extended the distance from traditional Fourth Amendment warrant requirements

significantly further.

For example, the FAA allows the Government to target any "non-U.S. person" – which includes "any group, entity, association, corporation, or foreign power" (50 U.S.C. § 1801[m]) – that is located overseas so long as a "significant" purpose of that interception is related to foreign intelligence, which is broadly defined. See 50 U.S.C. § 1801(e). Thus, the statute authorizes wholesale surveillance against "non-U.S. persons" but even those broad parameters do not permit the targeting of "U.S persons", i.e., U.S. citizens and lawful permanent residents such as Hasbjarami, nor the interception of any communication to or from – in all or part – United States soil, which was also the case here.

Nonetheless, the FAA electronic surveillance program results in massive acquisition of individual telephone calls and emails with no individualized judicial supervision to limit or police the Government's ability to thereafter review all such intercepted communications, regardless of whether the intercepted individual is a U.S. or non-U.S. person. A recently declassified Foreign Intelligence Surveillance Court ("FISC") opinion from 2011 estimated that, in a single year, the programs implementing the FAA acquired more than 250 million communications. See [Case Name Redacted], [docket number redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011) (Bates, J.). Reportedly, the National Security Agency ("NSA") makes a copy of "nearly all cross-border text-based data," scans the content of each message

using its chosen keywords or "selectors," then saves any communication that contains a match for further analysis. Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013.

By ostensibly targeting foreign (i.e., "non-U.S.") persons, the Government nonetheless searches and seizes the private communications of "U.S. persons" – both U.S. citizens and lawful permanent residents – in contact with those foreign persons without complying with basic Fourth Amendment protections. Similarly, the seizure of communications of U.S. persons is by no means accidental or unexpected. Although the Government often describes the collection of American communications as "inadvertent" and "incidental," such ignores what any reasonable individual with knowledge of the surveillance could foresee: the intrusions on U.S. persons are as inevitable and expected as the Government's protestations to the contrary.[1]

[1] Cf. [Case Name Redacted], 2011 WL 10945618, at *16 ("The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction 'unintentional.'…. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the *time of acquisition* that matters, and the government conceded as much at the hearing in this matter…. Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection [a Section 702 surveillance program] with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions.") (emphasis in original and citations omitted).

C. The provisions of the FAA authorizing warrantless surveillance and interception (i.e., Section 702) are unconstitutional per se and as applied herein and as such require suppression of all evidence that was derived as a result

The Fourth Amendment to the United States Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."

This fundamental Constitutional requirement imbues U.S. persons with the freedom, security, and protection from warrantless surveillance and the collection of evidence resulting from such surveillance absent: (1) a neutral judicial determination of probable cause; (2) based on a sworn affidavit; (3) particularizing the place to be searched; and (4) particularizing the person or things to be seized. See Groh v. Ramirez, 540 U.S. 551, 554 (2004).

Searches undertaken without a warrant, as was the case here, "are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions," Katz v. United States, 389 U.S. 347, 357 (1967), none of which apply to this case. See also United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) ("The Fourth Amendment … prohibits 'unreasonable searches and seizures' whether or not the evidence is sought to be

used in a criminal trial, and a violation of the Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion."), citing, United States v. Calandra, 414 U.S. 338, 354 (1974), United States v. Leon, 468 U.S. 897, 906 (1984).

Notwithstanding the enactment of the FAA, the warrantless mass collection, retention, accessing, dissemination, and use of the contents of the electronic communications of U.S. persons has long been held to violate the Fourth Amendment. See Keith., 407 U.S. at 313 (warrantless domestic surveillance for national security purposes violates the Fourth Amendment); Berger v. New York, 388 U.S. 41, 64 (1967) (statute that authorized electronic surveillance under judicial supervision violated the Fourth Amendment because it "permits a trespassory invasion of the home or office, by general warrant, contrary to the command of the Fourth Amendment").

The enactment of the FAA is not the first time Congress has sought to test the bounds of the Constitution, and it will surely not be the last, but we respectfully submit that in this case of first impression this Court should uphold the sanctity of the Fourth Amendment and reject as unconstitutional the Congressional end-run attempted by the creation of the FAA.

To be clear, the FAA permits the widespread capture, retention, and later querying, dissemination, and use of the communications of U.S. persons (i.e., U.S.

citizens and lawful permanent residents, such as Hasbajrami) both outside *and within* the United States under the guise of targeting foreign actors, but without any of the protections required by the Fourth Amendment for those, like Hasbajrami, that reside in the United States and at all relevant times possess the rights bestowed upon them by the United States Constitution.

Indeed, the intrusions in this case also implicate the separation of powers doctrine, which inheres in the structure of checks and balances created by the first three Articles of the Constitution:

> The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government. The independent check upon executive discretion is not satisfied, as the Government argues, by 'extremely limited' post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.

Keith, 407 U.S. at 317-18 (emphasis added) (footnotes and citations omitted). See also Berger, 388 U.S. at 63 ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.").

Under well-established Fourth Amendment law, the FAA fails to meet Constitutional requirements for two primary reasons. First, since FAA surveillance

has not been confined to the collection of foreign communications by foreign actors abroad, the FAA is subject to the Warrants Clause of the Fourth Amendment, which, as will be discussed, contains fundamental requirements that FAA surveillance fails to meet. See, e.g. Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) ("[T]he most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment…' "), quoting, Katz v. United States, 389 U.S. 347, 357 (1967); accord Arizona v. Gant, 556 U.S. 332, 338 (2009).

And second, the warrantless searches and seizures in this case cannot pass constitutional muster because the Government will be unable to establish one of the "jealously and carefully drawn" exceptions to the warrant requirement. Georgia v. Randolph, 547 U.S. 103, 109 (2006), quoting, Jones v. United States, 357 U.S. 493, 499 (1958).

Notably, the contents of telephone calls and emails of U.S. persons are within the core zone of privacy protected from government intrusion in the absence of a warrant. See United States v. Alderman, 394 U.S. 165, 177 (1969); United States v. Katz, 389 U.S. 347, 353 (1967). Moreover, as has long been held, "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."

Keith, 407 U.S. at 313.

In United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010), the Sixth Circuit concluded that email "is the technological scion of tangible mail" and that it would "defy common sense to afford emails lesser Fourth Amendment protection." To that end, Hasbajrami's emails merit the same Fourth Amendment protection as any of his private communications.

Indeed, electronic surveillance requires compliance with the "basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded." Berger, 388 U.S. at 63. Just as letters and packages in the mail are treated as Fourth Amendment papers within the home, the content of electronic communications are protected against having police officers read them in the absence of a warrant:

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizure extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.

Walter v. United States, 447 U.S. 649, 655 (1980).

Importantly, the Fourth Amendment applies to international as well as

domestic communications. See United States v. Ramsey, 431 U.S. 606, 616-20 (1977); United States v. Peterson, 812 F.2d 486, 490-92 (9th Cir. 1987). The Fourth Amendment also applies beyond criminal investigations because it "guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, 613-14 (1989), "without regard to whether the government actor is investigating crime or performing another function," City of Ontario v. Quon, 130 S.Ct. 2619, 2630 (2010), including protecting national security, see Keith, 407 U.S. at 313-14.

The Fourth Amendment presupposes a number of measures that are missing from the search and seizure of electronic communications under the FAA: (1) a warrant authorizing the search and seizure; (2) based upon probable cause; (3) particularly describing the place to be searched and the items to be seized; (4) based at all times on an affidavit under oath or affirmation; (5) issued by a neutral and detached magistrate operating in a judicial capacity; (6) with a return or other procedure assuring compliance with the terms of the warrant in its execution.

The absence of any one of these critical features from FAA surveillance would be fatal to the statute because it would not adequately protect against the search and seizure of the private communications of persons who reasonably should be known to be U.S. persons. See, e.g., [Case Name Redacted], 2011 WL

10945618, at *16 (holding that the "NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications").

That none of them are present in the FAA compounds the statute's unconstitutionality immeasurably. The absence of these factors, either individually or collectively, violates the Fourth Amendment, and as such this Court should hold that the Government's warrantless collection, retention, and accessing are presumptively unreasonable under Coolidge and Gant, or, at a minimum, unreasonable *as applied* to the facts of this case.

1. The FAA is unconstitutional per se and as applied herein because it authorizes surveillance and interception without a warrant

The "warrant" of the Warrant Clause is distinct from the "authorization" and "certificate" by the Foreign Intelligence Surveillance Court (FISC) under 50 U.S.C. §§ 1881a(a), 1881a(g).

The issuance of a search warrant by a judge involves an individualized determination regarding the constitutionality of a specific invasion of privacy:

> In response to these abuses of power by the government, the Founders abolished general warrants, restricted the government's ability to search without warrants, and required individual authorization of specific warrants. Today, search warrants are specific instruments that restrict government, dictate who may conduct a search, what may be searched, and when it may be searched. Both the procurement of the search warrant and its

> execution must be done under the law; otherwise the search is an unconstitutional abuse of governmental power.

Swate v. Taylor, 12 F. Supp. 2d 591, 594 (S.D. Tex. 1998); see also United States v. Vilar, 530 F.Supp.2d 616, 630 (SDNY 2008) ("Subpoenas are not search warrants. They involve different levels of intrusion on a person's privacy."), quoting, In re Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 854 (9th Cir. 1991) (also explaining that "the person served [with a subpoena] determines whether he will surrender the items identified in the subpoena or challenge the validity of the subpoena prior to compliance," whereas "[t]he person to be searched has no lawful way to prevent the execution of the warrant" prior to its enforcement). In contrast, similar to a subpoena, the FAA only calls for an "authorization" that does not involve any of the specificity of a Fourth Amendment warrant.

Pursuant to 1881a(c)(2), the "authorization" requires "[a] determination … by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization … intelligence important to national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subjection (i)(3) prior to the implementation of such authorization."[2]

[2] Section 1881a(i)(3) discusses the judicial review of certifications and procedures specifically with respect to "orders" issued in accordance with the statute, but provides no reference to warrants.

However, the "certification" upon which all elements of FAA surveillance are predicated merely requires: (1) that the target of the surveillance "be located outside of the United States" and "attest" that the procedures sought to be utilized will "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located outside of the United States"; (2) that minimization procedures will be utilized; (3) that "a significant purpose of the acquisition is to obtain foreign intelligence information"; and (4) that other elements of the statute are followed.

However, nowhere does the FAA require that such certification establish the existence of "probable cause" or any other threshold level of proof. As a result, the certification requires barely more detail then would be required in support of a *so-ordered subpoena,* which is a far cry short of matching the quantum of evidence required for a warrant. See Dalia v. United States, 441 U.S. 238, 256 n.18 (1979) ("electronic surveillance undeniably is a Fourth Amendment intrusion requiring a warrant); United States v. Figueroa, 757 F.2d 466, 471 (2d Cir. 1985) ("even narrowly circumscribed electronic surveillance must have prior judicial sanction") (emphasis added).

As such, we respectfully submit that a statute authorizing the massive collection of – and access to – communications, without an individualized neutral determination that the electronic communications of U.S. persons can be seized, and

read, secretly, and without consent, by Government agents, is in no way consistent with the Fourth Amendment warrant requirement.

2. The FAA is unconstitutional per se and as applied herein because it permits surveillance and interception without probable cause

The Fourth Amendment's requirement of "probable cause" assures that "baseless searches shall not proceed." Keith, supra, 407 U.S. 297, 316 (1972). This fundamental norm for Government searches and seizures requires sworn facts sufficient for a judge to decide whether individualized suspicion justifies the Government's intrusion on privacy. See Gates v. Illinois, 462 U.S. 213, 239 (1983) ("An affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause, which is not met by wholly conclusory statements."). The Supreme Court has carefully guarded the probable cause standard against encroachment within core areas of privacy; even a minor intrusion beyond the boundary of the lawful Government action, where core rights are concerned, requires probable cause. See Arizona v. Hicks, 480 U.S. 321, 329 (1987).

In contrast, the FAA fails to require individualized suspicion or probable cause before engaging in electronic surveillance. Instead, the statute allows the Government to target any "persons reasonably believed to be located outside the United States to acquire foreign intelligence information," 50 U.S.C. § 1881a(a),

with the definition of "person" broadly defined to include "any group, entity, association, corporation, or foreign power," 50 U.S.C. § 1801(m). While the Foreign Intelligence Surveillance Court (hereinafter, "FISC") approves general programs and procedures under the FAA, it does not, contrary to the requirements of the Fourth Amendment, review or approve the Government's specific targeting decisions nor its later access and querying of any seized communications.

Given the broad definition of "person", see 50 U.S.C. § 1801(m), and the minimal requirement that the electronic surveillance have as "a significant purpose" the acquisition of foreign intelligence, see 50 U.S.C. § 1881a(g)(2)(A)(v), the statute broadly authorizes the Government to target entire geographical areas or groups of people. Thus, without court approval, the FAA could be relied upon to authorize the Government to intercept and read every communication to and/or within a country of interest – Afghanistan or Pakistan, for example – as long as the Government satisfies itself that such intercepts implicate foreign intelligence – even if the communications (in writing, orally, or by electronic or other means) originate within the United States and are created by U.S. persons, both of which are the case here.

For centuries leading up to and following the ratification of the Bill of Rights, the probable cause standard has been the fundamental bulwark protecting people from Governmental over-reaching into their private lives. See Carlo v. United

States, 286 F.2d 841, 843 (2d Cir. 1961) (describing the Warrant Clause as "one of the most fundamental and significant of the provisions of the Bill of Rights," and explaining that when warrantless searches are conducted the Court "must scrutinize the evidence with meticulous care to make sure that no determination … shall constitute any watering down or erosion of the rights guaranteed by the Fourth Amendment"); cf. Kyllo v. United States, 533 U.S. 27, 34 (2001) (requiring a warrant for use of a thermal imaging device outside the home because "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment").

We respectfully submit that the Government's surveillance and interception of electronic communications of U.S. persons is constitutional only if based on a judicial finding of probable cause – that's not merely the law, but also the just result. Under the FAA, no probable cause or other level of suspicion is required before communications are acquired, retained, and read, and as such we submit that the statute unquestionably violates the Fourth Amendment.

3. The FAA is unconstitutional per se and as applied herein because it permits generalized and programmatic acquisition, retention, and accessing of electronic communications of U.S. persons without requiring particularity regarding the places to be searched and the items to be seized

"The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched

and the persons or things to be seized.' " Maryland v. Garrison, 480 U.S. 79, 84 (1987). "The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement endures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Garrison, 480 U.S. at 84, citing, inter alia, Marron v. United States, 275 U.S. 192, 196 (1927).

As one court put it, wholesale seizure of documents is exactly "the kind of investigatory dragnet that the Fourth Amendment was designed to prevent." United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982). Instead, the purpose of the specificity requirement is to prevent general exploratory rummaging in a person's belongings. See Coolidge, 403 U.S. at 467. "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron, 275 U.S. at 196.

Indeed, as recently explained by the Supreme Court in Riley v. California, 134 S.Ct. 2473, 2494 (2014), the American colonists' viscerally negative reaction to the British practices of "general warrants" and "writs of assistance" provided an essential impetus for the Fourth Amendment, and even the American Revolution itself. For centuries now:

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled

> "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." 10 Works of John Adams 247–248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." Id., at 248 (quoted in Boyd v. United States, 116 U.S. 616, 625 [] (1886)).

Riley, 134 S.Ct. at 2494.

Notwithstanding the clear mandates of the Fourth Amendment, and similar to the electronic surveillance statute held unconstitutional in Berger v. New York, supra, 388 U.S. 41, 56 (1967), the FAA "lays down no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor 'the place to be searched,' or 'the persons or things to be seized.' "

To the contrary, the FAA specifically removed from FISA the previous specific requirement of particularity as to the facilities to be targeted. See 50 U.S.C. § 1881a(g)(4) ("A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.").

By doing so, the FAA created an exception to FISA that is incompatible with the Fourth Amendment. See United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("a failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary").

Analogous to the interception of email that occurred in this case, last year the Second Circuit held, "Where … the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance." United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013). The Court reached this conclusion reasoning that "because there is currently no way to ascertain the content of a file without opening it," there is a " 'serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.' " Galpin, 720 F.3d at 447, citing and quoting, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010). "This threat," the Second Circuit held, "demands a heightened sensitivity to the particularity requirement in the context of digital searches." Galpin, 720 F.2d at 447.

Certainly, there is no meaningful difference between the contents of a computer hard drive versus the contents of an email account. With the constant

advance of technology, both may be essentially limitless in size and content, and as such, "[t]he potential for privacy violations occasioned by an unbridled, exploratory search of [either] is enormous." Id.

Here, the FAA creates a mechanism that lacks any particularity of the places to be searched or the items to be seized; and contains no check on the Government's capacity to execute, in effect, a general warrant on all of a person's communications; no check, of course, except for the Fourth Amendment. We respectfully submit that this lack of particularity, particularly in the "heightened" realm of digital searches, cannot survive the scrutiny that the Fourth Amendment requires.

4. The FAA is also per se unconstitutional because it includes the participation of the Foreign Intelligence Surveillance Court in the construction of its surveillance programs, thereby blurring the role of the neutral and detached magistrate

The Fourth Amendment requires the participation of a neutral and detached magistrate to ensure that the Government does not overstep the Constitution while zealously attempting to "ferret[] out crime." Johnson v. United States, 333 U.S. 10, 14 (1948); see also McDonald v. United States, 335 U.S. 451, 455-56 (1948) (discussing the need for "an objective mind [to] weigh the need to invade" privacy to enforce the law); Steagald v United States, 451 U.S. 204, 212 (1981) (explaining that judicial approval of warrants ensures a "checkpoint between the Government

and the citizen").

When the role of the judge is reduced merely to ratifying Executive Branch decisions, and even participating in them as consultants (for all practical purposes), with no case or controversy involving an adversary, the court's input regarding the program morphs into an impermissible advisory opinion. See Chafin v. Chafin, 133 S.Ct. 1017, 1023 (2013) ("Federal courts may not … give 'opinion[s] advising what the law would be upon a hypothetical state of facts' ") (brackets in original), quoting, Lewis v. Continental Bank Corp., 449 U.S. 472, 477 (1990); see also Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979) (when magistrate participated in search, "the objective facts of record manifest an erosion of whatever neutral and detached posture existed at the outset"); Coolidge, 403 U.S. at 449 (State Attorney General who was actively in charge of criminal investigation and later was to be chief prosecutor at trial was per se disqualified from determining whether there was probable cause to issue search warrants).

Given the programmatic "approval" process performed by the Foreign Intelligence Surveillance Court under the FAA, the FISC no longer functions as neutral and detached judicial officers. Rather, the statutory function of the court under the FAA is not to issue a warrant based on probable cause but to authorize and certify a program. See 50 U.S.C. § 1881a(a).

In doing so, the FISC meets ex parte with the Government and assists in

formulating the program. See [Case Name Redacted], 2011 WL 10945618, at *1-3; see also id. at *1, *28-*30 (holding that one aspect of the Section 702 collection proposed therein, the " 'upstream collection' of Internet transcriptions containing multiple communications[,] is, in some respects deficient on statutory and constitutional grounds," and then identifying the deficiencies and ordering their correction or cessation if the corrections do not occur).

As such, rather than approve or disapprove of proposals, the Foreign Intelligence Surveillance Court has a role in designing and modifying them and advising how the programs may be fashioned in order to comply with the requirements of the Fourth Amendment *when applied* – exactly what the Supreme Court has clearly prohibited.

Given the blurred lines involved in FAA surveillance, we respectfully submit that the Foreign Intelligence Surveillance Court does not operate, in the context of Section 702, as the neutral and detached magistrate required by the Warrant Clause of the Fourth Amendment.

D. Conclusion

Defendant Agron Hasbajrami is a lawful permanent resident who at all times relevant to this motion resided within the United States. Each intercepted email was either sent or received by Hasbajrami while Hasbajrami was within the United States, and to the extent any telephone calls were intercepted that included

Hasbajrami, Hasbajrami's participation in those calls could have only occurred while he was within the United States.

Yet, the "authorization" permitting the surveillance and interception of Hasbjarami's communications was issued without a warrant, without a prior showing of probable cause, without requiring particularity regarding the places to be searched or the items to be seized, and without the supervision of an entirely neutral and detached magistrate.

Accordingly, for these and all other reasons discussed above, the defense respectfully submits that the FAA is both unconstitutional per se and as specifically applied against Hasbajrami. As a result, the defense further submits that the fruits of all FAA surveillance that aggrieved Hasbajrami must be suppressed in this case.

Second Motion

MOTION TO SUPPRESS THE FRUITS OF FAA SURVEILLANCE IRRESPECTIVE OF THE CONSTITUTIONALITY OF THE STATUTE

A. Introduction

Assuming *arguendo* that the FAA survives the constitutional challenges raised herein, see First Motion, supra, the statutory application of 50 U.S.C. § 1881a to the facts of this case also requires suppression of Hasbajrami's intercepted communications. As the Court noted in its October 2, 2014, Order permitting Hasbajrami to withdraw his guilty plea:

> [E]ven if Hasbajrami cannot make a facial challenge to the FAA, it is also possible that the revelation of the role FAA material played in the government's investigation will lead to new fact-specific challenges to the evidence that the government would have used in this case. Hasbajrami might seek to suppress the FISA-obtained evidence not because the FAA is unconstitutional in general, but because of some other infirmity in its application to this particular case.

Order, dated, October 2, 2014 (*ecf* #85), at 8. The instant motion addresses these statutory concerns.

Indeed, a fundamental rule of statutory construction is that a statute should be construed in a manner that preserves its constitutionality. See United States ex rel. Attorney General, v. Delaware & Hudson Co., 213 U.S. 366, 408 (1909) (when "a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, [a court's] duty is to adopt the latter"); see also Jones v. United States, 526 U.S. 227, 239-40 (1999); accord Triestman v. United States, 124 F.3d 361, 377 (2d Cir. 1997); United States v. Al-Arian, 329 F. Supp.2d 1294, 1298 & n. 11 (M.D. Fla. 2004) (relative to § 2339B); United States v. Khan, 309 F.Supp.2d 789, 822 (E.D.Va. 2004) (applying the same principle to "personnel" in the context of 18 U.S.C. § 2339A). That doctrine of "constitutional avoidance" therefore requires this Court to examine the application of 50 U.S.C. § 1881a to Hasbajrami in order to determine whether a purely *statutory* basis exists for suppression, thereby obviating

the need to decide the constitutional issues presented in the First Motion.

Here, while defense counsel (and Hasbajrami) have thus far been denied access to specific information that would verify a statutory violation of 50 U.S.C. § 1881a in this case, as discussed below, abundant public information exists to establish that during the very period in which Hasbajrami's communications were intercepted (April 2, 2011, through August 28, 2011),[3] and during which he, a "United States person," was located exclusively within the U.S., the NSA routinely exceeded the authority granted it by the FISC and violated 50 U.S.C. § 1881a as a matter of course.

We address in Defendant's Fifth Motion, infra, why such indisputable evidence of the general nature of the NSA's violations of the FAA requires disclosure to cleared defense counsel of materials and information specific to the electronic surveillance of Hasbajrami, or, at an absolute minimum, exacting scrutiny by this Court in camera. In the meantime, and absence of such discovery, the following motion outlines the violations of the FAA that we believe mostly likely occurred in this case. As such, we respectfully request that this Court weigh the instant arguments when reviewing any ex parte submissions provided to this Court by the Government, as well as when considering, based upon the public record,

[3] Defense counsel does not know the precise period during which such interceptions occurred (which may be longer), but refer to that which is public from the information provided in the Pre-Sentence Report. See Section II, supra.

whether Hasbajrami's rights under the FAA were violated in this case.

B. The requirements and limitations set forth in 50 U.S.C. § 1881a of the FAA

1. Background of the § 1881a program

As noted ante, in POINT I, the FAA was enacted in 2008. However, for seven years prior to the passage of the FAA, NSA had been conducting (at least) the very same electronic surveillance and interception ultimately authorized by the FAA. For example, "in 2001, the NSA [] 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." Edward C. Liu, Andrew Nolan, Richard M. Thompson II, *Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments, Congressional Research Service* (April 1, 2014) (hereinafter, "*CRS Report: Overview*"), at 9 (footnote omitted) available at <http://fas.org/sgp/crs/intel/R43459.pdf>, citing, December 20, 2013, Unclassified Declaration of Frances J. Flesch, National Security Agency, in Schubert v. Obama, 07 Civ. 693 (JSW) (N.D.Cal.), at ¶ 32 (available at <http://icontherecord.tumblr.com>).

Initially, such surveillance and interception, denominated the Terrorist Surveillance Program (hereinafter "TSP"), was performed without any legislative or court authorization. See James Risen & Eric Lichtblau, "Bush Let U.S. Spy on Callers Without Courts," *N.Y. Times*, December 16, 2005 (available at

<http://www.nytimes.com/2005/12/16/politics/16program.html?_r=0>). After the TSP's existence was disclosed in December 2005 in *N.Y. Times*, "[u]timately, new statutory authority for this type of acquisition was provided, at first, temporarily under the Protect America Act ('PAA') of 2007 [P.L. 110-55], and on a longer term basis by the FISA Amendments Act ('FAA') [P.L. 261]." *CRS Report: Overview*, at 10 (footnotes omitted).

The scope of the surveillance and interception has been breathtaking. The *CRS Report: Overview* noted:

> According to a partially declassified 2011 opinion from the FISC, NSA collected 250 million Internet communications per year under this program. Of these communications, 91% were acquired "directly from Internet Service Providers," referred to as "PRISM collection." 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.

CRS Report: Overview, at 10 (footnotes omitted), citing, In re Foreign Intelligence Surveillance Court (Redacted), Docket No. [Redacted], 2011 WL 10945618, at *9, *25 (FISC 2011).

In addition, as the *CRS Report: Overview*, again citing the 2011 FISC opinion, explains that:

> [The] 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.

Id. (footnotes omitted), citing, In re Foreign Intelligence Surveillance Court (Redacted), 2011 WL 10945618, at *5.

Moreover, according to the *CRS Report: Overview*, "The Obama Administration also acknowledged to the FISC that technical limitations in the 'upstream' collection result in the collection of some communications that are unrelated to the target or that may take place entirely between persons located in the United States." Id., at 10 (footnote omitted).[4]

2. The FAA's specific requirements and limitations

While the FAA codified the legal authority of the U.S. Attorney General and the Director of National Intelligence (hereinafter "DNI") to authorize jointly (through a certification process submitted to the FISC) the targeting of non-U.S. persons reasonably believed to be located outside the United States (and, once authorized, to acquire such communications for up to one year), the statute also

---

[4] The *CRS Report: Overview*, also explains:

> 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.

CRS Report: Overview, at 10.

imposed certain substantive and procedural restrictions upon electronic surveillance and interception pursuant to 50 U.S.C. § 1881a.

Summarizing those limitations, the *CRS Report: Overview* explained that acquisition of communications pursuant to § 1881a:

- may not intentionally target any person known at the time of acquisition to be located in the United States, see 50 U.S.C. § 1881a(b)(1);
- 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 (so-called "reverse targeting"), see 50 U.S.C. § 1881a(b)(2);
- may not intentionally target a U.S. person reasonably believed to be located outside the United States, see 50 U.S.C. § 1881a(b)(3); and
- 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, see 50 U.S.C. § 1881a(b)(4).

CRS Report: Overview, at 10-11.[5]

Thus, as Judge Bates enumerated in his 2011 FISC opinion, 50 U.S.C. § 1881a(d)(1) requires that "the targeting procedures must be 'reasonably designed' to 'ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States.' " In re Foreign Intelligence Surveillance Court (Redacted), 2011 WL 10945618, at *5.

[5] The FAA also requires that electronic surveillance pursuant to § 1881a be conducted in a manner consistent with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3(A); see also Defendant's First Motion, supra.

That subsection 1881a(d)(1) also requires that "the targeting procedures must be 'reasonably designed' to 'prevent the intentional acquisition of 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.' " Id.

As Judge Bates further noted, the FAA also "requires that the minimization procedures 'meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)…' " Id., citing, 50 U.S.C. § 1881a(e)(1). Elaborating, Judge Bates pointed out:

> Most notably, that definition requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

In re Foreign Intelligence Surveillance Court (Redacted), 2011 WL 10945618, at *5, quoting, 50 U.S.C. §§1801(h) & 1821(4).

The mechanics of authorization pursuant to § 1881a require the Attorney General and the DNI to make certain certifications with respect to the limitations built into § 1881a. As a result, the Attorney General and DNI must submit to the FISC an application for a "mass acquisition order," see 50 U.S.C. §§ 1881a(a), 1881a(c)(2), with "a written certification and supporting affidavit" attesting that the

FISC has approved, or that the Government has submitted to the FISC for approval, "targeting procedures" reasonably designed to (1) ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and (2) "prevent the intentional acquisition of 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." 50 U.S.C. § 1881a(g)(2)(A)(i).

The certification and supporting affidavit must also attest that the FISC has approved, or that the Government has submitted to the FISC for approval, minimization procedures that meet the definition of "minimization procedures" under 50 U.S.C. §§ 1801(h) or 1821(4). The certification and supporting affidavit must also attest, among other things, that the Attorney General has adopted "guidelines" to ensure: compliance with the limitations set out in 50 U.S.C. § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information." 50 U.C.C. § 1881a(g)(2)(A)(iii)-(vii).

However, in addition to the distinctions in the concept of "probable cause" – particularly the fact that individual targets of surveillance are not necessarily reviewed by the FISC prior to acquisition of their communications – between traditional FISA warrants and § 1881a surveillance and acquisition, the FISC's

oversight role with respect to the latter is "narrowly circumscribed." In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, Docket No. Misc. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008) (internal quotation marks omitted).

Instead, the FISC's role is essentially limited to reviewing the targeting and minimization procedures that the Government proposes to use to target and acquire communications prospectively. See *CRS Report: Overview*, at 11 (footnote omitted). The FISC 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. Id. (footnote omitted), citing, 50 U.S.C. § 1881a(e). However, the minimization procedures allow for the retention and dissemination of information – including U.S. person information, – that is evidence of a crime. Id.

Another limiting element that applies to FISA generally, and, it is respectfully submitted, applies to electronic surveillance and interception pursuant to the FAA as well, appears in 50 U.S.C. § 1805(a)(2)(A), which provides "that no United States person may be considered a foreign power or an agent of a foreign power … solely upon the basis of activities protected by the first amendment…."

Accordingly, if the target participated in First Amendment activities such as expressing support, urging others to express support, gathering information,

distributing information, raising money for political causes, or donating money for political causes, 50 U.S.C. § 1805(a)(2)(A) would preclude those activities from serving as the basis for FAA surveillance.

C. The implications of non-disclosure of the underlying FAA applications, affidavits, certifications and orders regarding the electronic surveillance of Hasbajrami

1. The vertical playing field created by ex parte FISA and FAA proceedings

Litigation of FISA-authorized electronic surveillance generally, and FAA-authorized electronic surveillance in particular in this case, represents a radical departure from the traditional and essential requirement of the adversary process.[6] While ordinary search and even electronic surveillance warrants (issued pursuant to Title III) are presented initially ex parte, once criminal charges are instituted defense counsel and the defendant are afforded access to the underlying submissions in support of those warrants. On the other hand, with only one exception known to defense counsel, FISA and FAA applications (and supporting documents) have

[6] As stated in the Congressional Research Service's Report, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate*:

> An underlying principle of the Anglo-American legal system is the adversarial process, whereby attorneys gather and present evidence to a generally passive and neutral decision maker. The basic assumption of the adversarial system is that a "sharp clash of proofs presented" by opposing advocates allows a neutral judge to best resolve difficult legal and factual questions.

Andrew Nolan, Richard M. Thompson II, and Vivian S. Chu, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate*, Congressional Research Service, March 21, 2014, at 2 (available at <http://fas.org/sgp/crs/intel/R43260.pdf>).

never been shared with the defendant or defense counsel – even defense counsel in possession of the requisite security clearance to review classified material. See United States v. Daoud, Docket No. 12 Cr. 723, 2014 WL 321384 (N.D.Ill. January 29, 2014), rev'd, 755 F.3d. 479 (7th Cir. 2014).

The entirely one-sided nature of FISA litigation, particularly in the context of determining whether the Government adhered to the restrictions set forth in 50 U.S.C. § 1881a, applies not only to the facts at issue, as only the Government knows the facts specific to the FAA electronic surveillance and interception with respect to Hasbajrami, but also to *the law* as well, as the Government has access to the entire body of FISC and FISCR opinions while defense counsel's access is limited to those few opinions the Government or the court has released publicly.

This decidedly unlevel playing field – indeed, it is vertical, with the Government at the apex and defense counsel at the bottom – has clear implications, not the least of which is the Government's undefeated (and unsurprising, in light of the advantages inherent in ex parte litigation) record in FISA litigation in the statute's 35-year history. Also, it imposes upon this Court a responsibility – review of the FISA or FAA submissions as, in effect, surrogate defense counsel – to which courts have acknowledged they are not sufficiently suited to fulfill. See Alderman v. United States, 394 U.S. 65, 184 (1969); Franks v. Delaware, 438 U.S. 154, 169 (1978); United States v. Marzook, 412 F. Supp.2d 913, 921 (N.D.Ill. 2006).

Here, declassified opinions of the Foreign Intelligence Surveillance Court have provided evidence of systemic non-compliance with the court's authorizations. In the absence of the disclosure of the classified material requested in Defendant's Fifth Motion, infra, which we submit is necessary for defense counsel to present a full and complete picture of the Government's violations of its obligations under the FAA, Hasbajrami's burden of establishing specific statutory non-compliance should be relaxed accordingly.

As such, we respectfully submit that the Government should shoulder the burden of proving compliance – indeed, the doctrine of *res ipsa loquitor* makes sense here under the circumstances the Government alone has created. Certainly in this context, in which the FISC's approval was based on a general application, and not on specific information related to Hasbajrami, it would be appropriate to judge the Government on its lack of general compliance with the FISC's authorization.

2. Criticism of the FISC's ability to perform its necessary oversight function

Compounding the problem of ex parte review of FISA and FAA materials once a criminal prosecution is commenced is the fact that the FISC's capacity for oversight of FAA electronic surveillance and acquisition at the initial application phase is so narrowly defined by statute, as well as the FISC's historical institutional limitations as an independent factor in reining in abuse of FISA and FAA authority.

Regarding the latter, unlike the judiciary's traditional threshold Fourth

Amendment role as a gatekeeper for particular acts of surveillance, the FISC's role in FAA electronic surveillance is simply to ratify in advance the vaguest parameters pursuant to which the Government is then free to conduct acquisition of communications for up to one year.

Nor, unlike courts discharging their requisite Fourth Amendment responsibilities, does the FISC consider individualized and particularized surveillance applications, or make individualized probable cause determinations, or supervise the implementation of the Government's targeting or minimization procedures.[7]

Consequently, in the wake of the disclosures of the NSA's vast and unprecedented dragnet approach to electronic surveillance, the FISC has been the subject of much criticism and reconsideration.[8] As the Congressional Research

---

[7] Nor are judicial rulings from the FISC precedential, as they have not been issued in the context of "Cases" or "Controversies" within the constitutional meaning of Article III because only one party was involved. See Camreta v. Greene, 131 S. Ct. 2020, 2028 (2011) (authority to adjudicate legal disputes requires adverse litigants with the "concrete adverseness which sharpens the presentation of issues"), quoting, Los Angeles v. Lyons, 461 U.S. 95, 101 (1983).

[8] In addition to the sources discussed in POINT I, supra, and the text above, see also, e.g., *Report on the FISA Amendments Act of 2008*, The Constitution Project, Liberty and Security Committee, September 6, 2012, available at <http://www.constitutionproject.org/wp-content/uploads/2012/10/fisaamendmentsactreport_9612.pdf>; *PCLOB Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act*, July 9, 2013, available at <http://www.pclob.gov/library/20130709-Transcript.pdf>; *Remarks prepared for the Oct. 2, 2013 Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Senate Committee on the Judiciary*, Professor Laura K. Donohue, Georgetown Law School, available at <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1117&context=cong> (arguing that the "rather remarkable success rate" raises a "serious question about the extent to

Service notes, "[r]ecent controversies over the nature of the government's foreign surveillance activity have prompted some to argue that the judiciary's review of government surveillance requests under the Foreign Intelligence Surveillance Act of 1978 (FISA) should be far more exacting." Andrew Nolan, Richard M. Thompson II, and Vivian S. Chu, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate*, Congressional Research Service, March 21, 2014, at 2 (available at <http://fas.org/sgp/crs/intel/R43260.pdf>).

In fact, proposed reforms have focused on the absence of adversarial proceedings:

> [L]awmakers and others have suggested transforming FISA proceedings such that the process is more adversarial in nature. Critics of the current FISA proceedings have cited the infrequency of the FISC's rejections of government surveillance request as evidence that the lack of an adversarial process has prevented the court from fully and properly scrutinizing the government's position. While some reject this line of reasoning, those who have found the ex parte nature of FISA proceedings troubling have argued that allowing another attorney to argue in opposition to the requests of the Department of Justice (DOJ) to conduct foreign intelligence activity would allow the FISC to better protect civil liberty interests.

---

which FISC and [the Foreign Intelligence Surveillance Court of Review] perform the function they were envisioned to serve"); Stephen I. Vladeck, "It's Time To Fix the FISA Court (the Way Congress Intended)", MSNBC (Aug. 1, 2013), available at <http://www.msnbc.com/msnbc/its-time-fix-the-fisa-court-the-way>; http://www.uscourts.gov/uscourts/courts/fisc/honorable-patrick-leahy.pdf; and http://www.stanfordlawreview.org/online/foreign-intelligence-surveillance-court-really-rubber-stamp-ex-parte-proceedings-and-fisc-win#footnote_2.

Id., at 2-3; see also id. at Preamble ("[i]n response to concerns that the ex parte nature of many of the proceedings before the FISA courts prevents an adequate review of the government's legal positions, some have proposed establishing an office led by an attorney or 'public advocate' who would represent the civil liberties interests of the general public and oppose the government's applications for foreign surveillance").[9]

While Congress and others debate whether adversarial proceedings should be instituted in the FISC at *front end* of the FISA and FAA process, there remains no good rationale for continuing ex parte proceedings at the *back end*, in the Federal courts in the context of criminal prosecutions when, as here, a defendant's liberty is at stake and the evidence the Government seeks to use either consists of or is derived from FISA or FAA surveillance and acquisition.

[9] Regarding the FISC's *ex parte* proceedings, *N.Y. Times* reported that Geoffrey R. Stone, professor of constitutional law at the University of Chicago, and co-author of *Liberty and Security In a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013 (available at <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>), "said he was troubled by the idea that the court is creating a significant body of law without hearing from anyone outside the government, forgoing the adversarial system that is a staple of the American justice system. 'That whole notion is missing in this process,' [Prof. Stone] said." Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *N.Y. Times*, July 6, 2013, available at <http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all>.

D. The history of non-compliance with both FAA and FISA restrictions

Certainly the public record compels a presumption that during the time period at issue herein – 2010-2011 – NSA was *not* in compliance with FAA or FISA in a number of critical and relevant aspects. Following the disclosures made by Edward Snowden, in August 2013 the Government released declassified versions of a series of FISC opinions that catalog the abuses and transgressions – exceeding the authority granted by the FISC – NSA committed in the course of implementing FAA programs and surveillance/acquisition.

In one such FISC opinion, In re Foreign Intelligence Surveillance Court (Redacted), supra, 2011 WL 10945618, at *5, n.14 (FISC 2011), District Judge John D. Bates, Chief Judge of the FISC at the time, excoriated the NSA for exceeding its acquisition authority and making repeated misrepresentations to the FISC regarding the NSA's activities during the period in which Hasbajrami's communications were monitored and intercepted pursuant to 50 U.S.C. § 1881a. As described in the *CRS Report: Overview*, Judge Bates was evaluating "the targeting and minimization procedures proposed by the government to address new information regarding the scope of upstream collection." *CRS Report: Overview*, at 13 (footnotes omitted).

The *CRS Report: Overview* explained that "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." Id. (footnotes omitted). In response, Judge Bates "found the proposed minimization procedures to be deficient on statutory and constitutional grounds." Id. (footnotes omitted).

According to the *CRS Report: Overview*,

> [w]ith 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 retained for up to five years so long as the government was not seeking to use that information.

Id. (footnote omitted).

The *CRS Report: Overview* noted that Judge Bates concluded 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." Id. (footnote omitted).

In his opinion, and discussed in POINT I, supra, Judge Bates noted the pervasive nature of the violations: "The court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program." In re Foreign Intelligence Surveillance Court (Redacted), 2011 WL 10945618, at *5, n.14.

Judge Bates further noted that the Government's submissions in that proceeding made it clear that the NSA had been acquiring Internet transactions even before the FISC's first approval thereof, id. at *17, n.45, adding that:

- "[t]he Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet 'transactions,' which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities, June 1 Submission at 1–2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals." Id. at *5;

- "for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different than what the Court had been led to believe." Id. at 9;

- "the Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCT's [multi-communication transactions], are consistent with the Fourth Amendment." Id. at 9;

- "NSA's minimization procedures, as the government proposes to apply them to MCT's as to which the 'active user' is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention[.]" Id. at 28;

- "[t]he sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of transactions is not feasible." Id. at 10;

- "the Court cannot know for certain the exact number of wholly

domestic communications acquired through this collection, nor can it know the number of non-target communications acquired or the extent to which those communications are to or from United States persons or persons in the United States." Id. at 10;

- "[e]ven if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection . . . it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future." Id. at 10;

- "the actual number of wholly domestic communications acquired may still be higher in view of NSA's inability conclusively to determine whether a significant portion of the MCT's within its sample contained wholly domestic communications." Id. at 11; and

- "the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year." Id. at 15.[10]

As a result, Judge Bates required further briefing by the Government because "it appeared to the Court that the acquisitions described in [a recent Government letter to the Court] exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702." Id. at *2.

Subsequently, the Government presented the FISC revised minimization standards that were deemed acceptable under statutory and Fourth Amendment standards. However, those modifications were submitted November 30, 2011, well

[10] See also Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.," *N.Y. Times*, August 8, 2013, available at <http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all> (analyzing a document of internal NSA rules disclosed by Mr. Snowden).

after the electronic surveillance and acquisition of Hasbajrami's communications occurred in this case. Those changes provide further strong indication that the NSA's prior means of surveillance and acquisition, *which were applied to Hasbajrami*, violated 50 U.S.C. § 1881a.

Other recently declassified FISC opinions include additional examples of the NSA's persistent and diverse non-compliance with FISC orders and restrictions:

- the "NSA exceeded the scope of authorized acquisition continuously during the more than [redacted] years of acquisition[.]" [(Case Name Redacted)], PR/TT No. [docket redacted], at 3, (FISC [date redacted]) (declassified Nov. 18, 2013) (available at <http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf>) (last accessed, November 24, 2014);

- "the NSA has on a daily basis, accessed the BR [business records] metadata for purposes of comparing thousands of non-RAS [reasonable articulable suspicion] approved telephone identifiers on its alert list against the BR metadata in order to identify any matches," which was a violation of the earlier court order that was compounded by the government's repeated inaccurate descriptions to the FISC. In re Production of Tangible Things from [redacted], Docket No. BR 08-13, 2009 WL 9150913, at *2-8 (FISC Mar. 2, 2009) (declassified Sept. 10, 2013);

- "NSA's placement of unminimized metadata [redacted] into databases accessible by outside agencies, which, as the government has acknowledged, violates not only the Court's orders, but also NSA's minimization and dissemination procedures set forth in [United States Signal Intelligence Directive]," (In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], Docket No. BR 09-06, at 6-7 (FISC June 22, 2009) (order requiring government to report and explain instances of unauthorized sharing of metadata) (declassified Sep. 10, 2013) (order requiring government to report and explain instances of unauthorized sharing of metadata) (declassified Sep. 10, 2013) (available at

<http://www.clearinghouse.net/chDocs/public/NS-DC-0013-0001.pdf>) (last accessed, November 24, 2014);

- the Court was "deeply troubled" by previous non-compliance incidents that occurred shortly after the completion of NSA's "end to end review" of the processes for handling BR ["Business Records"] metadata "and its submission of a report intended to assure the court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems" (In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], Docket No. BR 09-13, 2009 WL 9150896, at *2 (FISC Sept. 25, 2009) (declassified Sep. 10, 2013)).

See also In re Production of Tangible Things from [redacted], Docket No. BR 08-13, 2009 WL 9157881, at *2 (FISC Jan. 28, 2009) (declassified Sept. 10, 2013) ("The Court is exceptionally concerned about what appears to be a flagrant violation of its Order in this matter.").

Judge Bates's 2011 FISC opinion also referred to a 2009 FISC Opinion that was subsequently released to the public. That opinion, by FISC Judge Reggie B. Walton (who also sits as a District Judge in the District for the District of Columbia) provides further and compelling proof that NSA persistently lies to, conceals from, and misleads (affirmatively and by silence) the FISC, that NSA cannot be trusted even to train its own employees adequately, or even be able to determine for itself the limits on its surveillance activities consistent with statute or FISC Orders. See In re Production of Tangible Things From [Redacted], Docket No. BR 08-13, 2009 WL 9150913 (FISC March 2, 2009).

Judge Walton's FISC opinion demonstrates the plethora of statutory

violations that pervade the NSA's electronic surveillance programs, including those at issue herein. For example, Judge Walton's March 2009 FISC opinion includes the following passages:

- "[t]he government's submission suggests that its non-compliance with the Court's orders resulted from a belief by some personnel within the NSA that some of the Court's restrictions on access to the BR [Business Records] metadata applied only to "archived data".… That interpretation strains credulity … such an illogical interpretation of the Court's Orders renders compliance with the RAS [Reasonable, Articulable Suspicion] requirement merely optional." Id. at *2;

- "[t]he government compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC." Id. at *3;

- "[r]egardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect [REDACTED] call detail records pertaining to telephone communications of US persons located within the United States who are not the subject of any FBI investigation and whose call detail information could not otherwise have been legally captured in bulk." Id. at *4;

- "[i]n summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. *The minimization procedures proposed by the government in each*

successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systematically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively." Id. at *5 (emphasis added);

- "[t]he record before the Court strongly suggests that, from the inception of this FISA BR program, the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures." Id. at *7; and

- "[u]nder these circumstances, *no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures*. In fact, the government acknowledges that, *as of August 2006, "there was no single person who had a complete understanding of the BR FISA system architecture*." Id. at *7 (emphasis added). See also Scott Shane, "Court Upbraided N.S.A. on Its Use of Call-Log Data," *N.Y. Times*, September 10, 2013, available at <http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html?pagewanted=all&_r=0> (noting that, according to a senior U.S. intelligence official who briefed reporters just prior to release of the 2009 FISC opinion, "only about 10 percent of 17,800 phone numbers on the alert list in 2009 had met [the RAS] test," and that "[t]here was nobody at N.S.A. who really had a full understanding of how the program was operating at the time").

Judge Walton also recognized the FISC's limitations as a watchdog, pointing out that "in light of the scale of this bulk collection program, the Court must rely heavily on the Government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of US persons as required by applicable minimization procedures." Id. at *6.

Elaborating, Judge Walton noted that "[t]o approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that

those responsible for implementation fully comply with the Court's orders." Id. Yet, he concluded, "The Court no longer has such confidence." Id.

Judge Walton's lack of confidence was well-founded, and validated by the NSA's continued non-compliance. As if Judge Bates's 2011 FISC opinion and Judge Walton's 2009 FISC opinion (and the three others cited above) were insufficient to demonstrate NSA's abject inability – whether deliberate or simply through inexcusably irresponsible negligence or cavalier incompetence – to comply, a subsequent August 13, 2009, report the Government submitted to the FISC revealed even more non-compliance issues beyond the myriad enumerated in Judge Walton's opinion, and which were discovered after issuance of that Opinion. See Report of the United States, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 09-09, August 13, 2009, (hereinafter "US Report, Docket BR 09-09").

Further violations of the FISC's Orders included, for example: (a) permitting employees of other government agencies to have external and unsupervised access to the NSA database; (b) failing to audit for compliance issues – at any point over the lifespan of the program – a database used to store information retrieved from NSA databases; and (c) use of software with a feature permitting analysts to pull more information than NSA was authorized to retrieve. Id.

The NSA's continued non-compliance and recidivism, even through 2011 as

described in Judge Bates's FISC opinion, establishes that the FISC's complaints, and even its attempts at remedial measures, are ineffectual as long as the process remains secret. The public record – and who knows (certainly not defense counsel) what still remains classified – compels but one conclusion: the NSA cannot be trusted to comply with its statutory and constitutional obligations, despite repeated chances, and one of the principal reasons is the absence of any accountability.

The repeated misrepresentations cited by Judge Bates in October 2011 and Judge Walton in 2009 constitute simply a constant and continued feature of NSA practice with respect to FISA surveillance generally. Indeed, they are reminiscent of those divulged in the FISC's 2002 opinion in In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F.Supp.2d 611, 620-21 (FISC), rev'd on other grounds sub nom., In re Sealed Case, 310 F.3d 717 (FISCR 2002),[11] in which the FISC, in its first opinion ever, reported that beginning in March 2000, the Department of Justice had come "forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States."

Those errors related to misstatements and omissions of material facts," including:

- "75 FISA applications related to major terrorist attacks directed against the United States" contained "misstatements and omissions of material

[11] "FISCR" refers to the Foreign Intelligence Court of Review, which is the appellate court for the FISC, and is comprised of three Federal Circuit judges. The FISCR's 2002 decision in In re Sealed Case marked its first case since enactment of FISA in 1978.

facts." In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F.Supp.2d at 620-21;

- the government's failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance. Id.; and

- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. Id.

According to the FISC, "In March of 2001, the government reported similar misstatements in another series of FISA applications…." Id. at 621. Those problems, however, were not isolated or resolved by those revelations. Instead, they proved persistent. A report issued March 8, 2006, by the DOJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other intelligence-gathering procedures more than 100 times in the preceding two years, and problems appear to have grown more frequent in some crucial respects. See Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March 8, 2006 (hereinafter "DOJ IG Report") (available at <http://www.usdoj.gov/oig/special/s0603/final.pdf>).

The report characterized some violations as "significant," including wiretaps that were much broader in scope than authorized by a court ("over-collection"), and others that continued for weeks and months longer than authorized ("overruns"). Id.

at 24-25.[12] FISA-related over-collection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. See DOJ IG Report, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, although the amount of time "over-collection" and "overruns" were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. Id. at 25, 29.

The lack of veracity catalogued in the declassified FISC opinions publicly disclosed is inevitable in a system in which there is no opponent to dispute facts or hold opponents accountable for misrepresenting facts, and in which the court lacks investigative authority or any practical, meaningful means of oversight over the collection/storage/interception process. Indeed, an internal May 2012 audit of NSA's surveillance programs – among the documents recently disclosed by Mr. Snowden – found that NSA violated privacy rules protecting domestic U.S. communications 2,776 times in a one-year period. See *SID Oversight & Compliance*, Quarterly Report, First Quarter Calendar Year 2012, May 3, 2012, available at <http://www.documentcloud.org/documents/758651-1qcy12-violations.html#document/p12>.

[12] The DOJ Inspector General's report was not instigated by the Government itself. Rather, the publication of documents released to the Electronic Privacy Information Center (hereinafter "EPIC") in Freedom of Information Act litigation prompted the DOJ IG to use those and other documents as a basis for the report. In preparing the report the IG reviewed only those 108 instances in which the FBI itself reported violations to the Intelligence Oversight Board – a four-member Executive Branch body that ordinarily does *not* submit its reports to Congress.

Unfortunately, in a system in which NSA and other intelligence organs are free to misrepresent without challenge or accountability, little has changed except perhaps NSA's enhanced dexterity in abusing and manipulating the FISC and the FISA system as a whole.

Here, even on just the public record, the FISC opinions establish that during the time frame relevant to this case, when Hasbarajmi, undeniably a "U.S. person," was located exclusively in the United States, the NSA was regularly and materially violating § 1881a and exceeding the authority granted it by the Foreign Intelligence Surveillance Court.

In addition, the First Amendment limitations on FISA surveillance also merit consideration, particularly since the conduct that led to the FISA surveillance could very well have been limited to protected First Amendment activity. See Humanitarian Law Project v. Holder, 130 S. Ct. 2705, 2710 (2010) (material support does not include independent advocacy, or even mere membership in a proscribed organization).

Judged by its general and wholly unsatisfactory level of non-compliance, the Government's violation of 50 U.S.C. § 1881a in this case is manifest even from the public record alone. Consideration of such non-compliance would be an appropriate standard in this instance since the general program of surveillance and acquisition (rather than a particularized application specifically to Hasbajrami) is

what the FISC approved, reviewed, and initially found incompatible with the FAA (and the Fourth Amendment) before ultimately approving modifications made *after* the interception of Hasbajrami's communications.

Moreover, even the Foreign Surveillance Intelligence Court concluded that the Government's capture of domestic U.S. communications – during the time frame of the surveillance and acquisition of Hasbajrami's communications – was *intentional*, and therefore beyond the boundaries set by the FISC and the FAA. See In re Foreign Intelligence Surveillance Court (Redacted), supra, 2011 WL 10945618, at *16 (FISC 2011).

In addition, as discussed in Defendant's Fifth Motion, infra, the DNI has informed a U.S. Senator that in at least one instance the minimization standards employed by NSA were "unreasonable" under the Fourth Amendment, and that the agency believed "the government's implementation of Section 702 of FISA has sometimes circumvented the spirit of the law, and on at least one occasion the FISA Court has reached this same conclusion." Letter from the Office of the DNI to Senator Ron Wyden, dated, July 20, 2012, available at <http://www.wired.com/images_blogs/dangerroom/2012/07/2012-07-20-OLA-Ltr-to-Senator-Wyden-ref-Declassification-Request.pdf> (last accessed, November 23, 2014).

E. Conclusion

Accordingly, for all of the reasons discussed above, we respectfully submit that the Government's electronic surveillance and acquisition of Hasbajrami's electronic communications were conducted in violation of 50 U.S.C. § 1881a, and must therefore be suppressed along with any and all of fruits derived therefrom.

Third Motion

MOTION TO SUPPRESS THE FRUITS OF FAA SURVEILLANCE DUE TO OUTRAGEOUS GOVERNMENT CONDUCT

This Court ruled that the Government's intentional decision to provide Hasbajrami with "FISA notice without FAA notice," notwithstanding the statutory requirements to the contrary (i.e., 50 U.S.C. § 1881e[a]), intentionally "misled [Hasbajrami] about an important aspect of his case" (Order, dated, October 2, 2014 [*ecf* #85], at 6). This Court then permitted Hasbajrami to withdraw his guilty plea as a result (id. at 7-8).

While the result fashioned by this Court permitted Hasbajrami to be returned procedurally to the position he would have been in if not for the Government's violation of its notice obligations under the FAA, the defense respectfully submits that additional sanctions are necessary to dissuade the Government from repeating its misconduct in future cases. Specifically, the defense submits that suppression

here of the fruits of the Government's warrantless FAA surveillance would satisfy this goal.

In Hampton v. United States, 425 U.S. 484, 495 n.7 (1976), the Supreme Court ruled that Government misconduct could invalidate a conviction on due process grounds if the misconduct reaches a "demonstrable level of outrageousness." Similarly, the Second Circuit has acknowledged that "Government involvement in a crime may in theory become so excessive that it violates due process and requires the dismissal of charges against a defendant even if the defendant was not entrapped." United States v. Al Kassar, 660 F.3d 108, 121 (2d Cir. 2011).

Because the sanction of dismissal is so severe, the Second Circuit has observed that outrageous Government conduct is "an issue frequently raised that seldom succeeds." United States v. Schmidt, 105 F.3d 82, 91 (2d Cir. 1997). However, the Court has also made clear that it accepts the legal principle that governmental conduct can be so beyond the pale that it constitutes a Due Process violation requiring sanction. See United States v. Cromitie, 727 F.3d 194, 217-221 (2d Cir. 2013); Al Kassar, 660 F.3d at 121.

Here, while the Government's misconduct might not warrant the ultimate sanction of dismissal, some meaningful sanction in nevertheless necessary to avoid

a toothless result that provides Hasbajrami no relief and leaves the Government unaccountable.

As this Court recognized in United States v. Simels, Docket No. 08 Cr. 640 (JG), 2009 WL 1924746, at *13-15 (EDNY July 2, 2009), in the context of the failure to minimize interception of legitimate attorney-client conversations recorded pursuant to a defective Title III electronic eavesdropping warrant, the wholesale failure to minimize required wholesale suppression. Further, as this Court also recognized in Simels, there would be little incentive for the Government to act properly in the future if, in the worst case scenario, after the failure to minimize was discovered, only the improperly intercepted communications – which the Government never had a right to collect – were suppressed. That is, in tactical and strategic terms, a "no lose" proposition for the prospective wrongdoer.

Here, the Government's misconduct was deliberate, calculating, and *designed* to mislead (by omitting reference to the FAA in its original FISA notice). Failing to impose some sanction would not just fail to punish misconduct, it would, conversely, reward it.

Hasbajrami has been allowed to withdraw his guilty plea and to therefore challenge the warrantless surveillance that took place in this case. However, by withdrawing his guilty plea Hasbajrami faces the potential for a lengthier sentence now than he had been facing prior to learning that the Government had violated his

Due Process rights. Specifically the defendant now faces a potential sentence of 60 years imprisonment upon a conviction post-trial, whereas he had previously received a 15-year sentence pursuant to his plea agreement.

As such, should the defendant's suppression motions fail, the Government will be in a better position vis-à-vis Hasbajrami's potential sentence then it would have been in had Hasbajrami never learned of the Government's misconduct in the first place. Although this Court's order fulfilled the good intention of returning the defendant to the procedural position he was in prior to his guilty plea, this Court's order also returned the Government to the unscathed – and advantageous – position *it was in* prior to unlawfully failing to comply with its notice obligations under the FAA.

We respectfully submit that a just result requires a more significant sanction than simply returning the parties to the position they had been in prior to the Government's unlawful action. While outright dismissal would constitute an extreme sanction, suppression of the fruits of the warrantless surveillance is certainly appropriate and would make clear that when the Government willfully evades its discovery obligations significant consequences will follow.

As such, we respectfully submit that the Government's intentional decision to mislead the defendant into entering a guilty plea by withholding information critical to his decision-making with respect to that plea, is *so outrageous* that it requires a

sanction beyond simply permitting the defendant to withdraw his guilty plea. We respectfully submit that it requires the tempered and appropriate sanction of suppression as well.

Fourth Motion

MOTION TO SUPPRESS HASBAJRAMI'S POST-ARREST STATEMENTS

On September 6, 2011, Defendant Agron Hasbajrami was arrested, handcuffed, and interrogated by the FBI. The interrogation lasted for three days and was not completed until September 8, 2011. During that interrogation, Hasbajrami waived his Miranda rights and made incriminating statements that the Government intends to introduce at trial. See Miranda v. Arizona, 384 U.S. 436, 460-63 (1966).

Nonetheless, because Hasbajrami's arrest and statements were a direct result of the surveillance challenged in Motions One through Four, above, and because Hasbajrami's arrest and statements would not have been produced through an independent source, to the extent Hasbjarami's suppression motions were not already clear, we hereby also specifically move to suppress his post-arrest statements as fruit of the poisonous tree. See Murray v. United States, 487 U.S. 533, 536-37 (1988); Silverthorne v. United States, 251 U.S. 385, 392 (1920); Nardone v. United States, 308 U.S. 338, 342 (1939); Wong Sun v. United States, 371 U.S. 471, 488 (1963).

IV. Discovery Motions

Fifth Motion

MOTION FOR DISCOVERY OF MATERIAL AND INFORMATION NECESSARY TO DETERMINE WHETHER THE GOVERNMENT'S SPECIFIC CONDUCT IN THIS CASE VIOLATED THE STATUTORY REQUIREMENTS OF FISA, THE FAA, AND/OR ANY OTHER SURVEILLANCE STATUTE OR PROGRAM RELIED UPON DURING THE INVESTIGATION OF THIS CASE, AS WELL AS TO DETERMINE WHETHER THE GOVERNMENT'S SPECIFIC CONDUCT VIOLATED HASBAJRAMI'S RIGHT TO DUE PROCESS UNDER THE FIFTH AMENDMENT

A. Introduction

As previously stated, Hasbajrami is an "aggrieved person" within the plain meaning of FISA and the FAA. See 50 U.S.C. § 1801(k) (" 'Aggrieved person' means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."). The "electronic surveillance" under "this subchapter" refers to subchapter I of the FISA, which is entitled "Electronic Surveillance" and codified at 50 U.S.C.§§ 1801-1812. The statute broadly defines electronic surveillance in 50 U.S.C. § 1801(f).

As also previously discussed, when evidence is "derived" from surveillance that was "not lawfully authorized or conducted" the Court must suppress the evidence, see 50 U.S.C. § 1806(g), and derivative evidence includes statements and tangible evidence that are the fruit of the poisonous tree, see Murray v. United

States, supra, 487 U.S. 533, 536-37 (1988).

As such, so that the defense may effectively establish whether Hasbajrami has any further basis to challenge the Government's surveillance programs in this case, the defense requests from the Government – including all Federal, State, and local law enforcement, intelligence, diplomatic, military, and other agencies and departments, as well as from foreign governments with which the U.S. has acted jointly or cooperatively in this investigation – the following pursuant to 50 U.S.C. § 1881a, Rule 16 of the Federal Rule of Criminal Procedure, 18 U.S.C. § 3504,[13] Brady v. Maryland, 373 U.S. 83 (1963), and its progeny:

1. To the extent there exists any "foreign intelligence information" relevant to this case that has not been previously disclosed to the defense, provide any remaining undisclosed information at this time;

2. Disclose whether the FAA surveillance relied upon against Hasbajrami intentionally targeted the defendant (see 50 U.S.C. §§ 1881a[b][1],

[13] 18 U.S.C. § 3504 provides, in relevant, part:

> (a) In any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority of the United States … (1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act;
>
> X X X
>
> (b) As used in this section, "unlawful act" means any act the use of any electronic, mechanical, or other device (as defined in section 2501[5] of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto.

1881a[b][2]), and/or whether he was the subject of "reverse targeting" (i.e., targeting someone oversees in order to capture communications with a U.S. person or in order to capture communications involving a U.S. component);

3. Disclose whether the FAA surveillance relied upon against Hasbajrami intentionally targeted "a United States person reasonably believed to be located outside of the United States" (50 U.S.C. § 1881a[b][3]);

4. Disclose whether the FAA surveillance relied upon against Hasbajrami "intentionally acquire[d] any communication as to which the sender and all intended recipients [were] known at the time of the acquisition to be located in the United States" (50 U.S.C. § 1881a[b][4]);

5. Disclose whether the Government has any reason to believe that the FAA surveillance relied upon against Hasbajrami were not "conducted in a manner consistent with the fourth amendment to the Constitution of the United States" (50 U.S.C. § 1881a[b][5]);

6. Provide copies of all FISA warrants and FISA warrant applications not previously disclosed to the defense in this case;

7. Provide material documenting what minimization and targeting procedures and interpretive instructions were in effect at the time any foreign intelligence evidence or information was gathered, and how those procedures were implemented (i.e., who was being targeted, what was the basis for that targeting, and what minimization procedures were used during that targeting);

8. Provide what information, if anything, was told to was the Foreign Intelligence Surveillance Court (FISC) about FAA surveillance relative to Hasbajrami (or other persons relevant to this case) in approving any FISA warrants in this case;

9. Provide notice of whether any other surveillance programs were relied upon during the investigation of this case and aggrieved Hasbajrami; and

10. Provide notice whether any "programmatic analytics" were utilized, or whether cross-referencing or searching or analysis occurred with respect to the information derived from FAA and FISA surveillance and

interception, and/or any other surveillance, interception, collection, and/or retention program.

It is requested that compliance with each of the above discovery demands be made by providing the requested information directly to cleared defense counsel. However, should the Government believe that cleared defense counsel are prohibited from receiving any or all of the above information, then it is requested that, at a minimum, the information be provided to this Court for *in camera* review (pursuant to the provisions of the Classified Information Procedures Act and any appropriate protective order), and that after such review this Court disclose to the defense any such information that this Court determines the defense is entitled.

B. Disclosure will level the uneven vertical playing field created by ex parte FISA and FAA Proceedings

As discussed in Defendant's Second Motion**,** supra, litigation of FISA-authorized electronic surveillance generally, and FAA-authorized electronic surveillance in particular in this case, represents a radical departure from the traditional and essential requirement of the adversary process. The entirely one-sided nature of FISA litigation, can be evened however if this Court determines that defense input will assist this Court's review of the FISA and FAA-related information. See 50 U.S.C. § 1806(f) (authorizing courts to "disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance …

where such disclosure is necessary to make an accurate determination of the legality of the surveillance").

As the Supreme Court recognized in Alderman v. United States, 394 U.S. 65, 184 (1969) – a case involving electronic surveillance – "[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate." See also Franks v. Delaware, 438 U.S. 154, 169 (1978) (permitting adversarial proceeding on showing of intentional falsehood in warrant affidavit because the magistrate who approves a warrant ex parte "has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations").[14]

Ex parte proceedings impair the integrity of the adversary process and the criminal justice system. As the Supreme Court has recognized, "[F]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights…. No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it."

[14] As explained by the court in United States v. Marzook, a case also involving terrorism-related charges, and in the context of deciding whether to close a suppression hearing to the public because of the potential revelation of classified information thereat:

> It is a matter of conjecture whether the court performs any real judicial function when it reviews classified documents in camera. Without the illumination provided by adversarial challenge and with no expertness in the field of national security, the court has no basis on which to test the accuracy of the government's claims.

United States v. Marzook, 412 F. Supp.2d 913, 921 (N.D.Ill. 2006), quoting, Stein v. Department of Justice & Federal Bureau of Investigation, 662 F.2d 1245, 1259 (7th Cir. 1981).

United States v. James Daniel Good Real Property, et. al., 510 U.S. 43, at 55 (1993), quoting, Joint Anti-Fascist Refugee Committee v. McGrath, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring); see also United States v. Madori, 419 F.3d 159, 171 (2d Cir. 2005), citing, United States v. Arroyo-Angulo, 580 F.2d 1137, 1145 (2d Cir. 1978) (closed proceedings "are fraught with the potential of abuse and, absent compelling necessity, must be avoided") (other citations omitted).[15]

In United States v. Abuhamra, 389 F.3d 309 (2d Cir. 2004), the Second Circuit reemphasized the importance of open, adversary proceedings, declaring that "[p]articularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other." Abuhamra, 389 F.3d at 322-23, citing, McGrath, 341 U.S. at 171 n.17 (Frankfurter, J., concurring) (which noted that "the duty lying upon every one who decides anything to act in good faith and fairly listen to both sides … always giving a fair opportunity to those who are parties in the controversy for correcting or contradicting any relevant statement prejudicial to their view") (citation and internal quotation marks omitted).[16]

---

[15] Conversely, as Judge Learned Hand stated in United States v. Coplon, 185 F.2d 629, 638 (2d Cir. 1950), "Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which is seeks to forfeit the liberty of its citizens."

[16] As the Ninth Circuit observed in the closely analogous context of a secret evidence case, " 'One would be hard pressed to design a procedure more likely to result in erroneous

Similarly, in the Fourth Amendment context, including in relationship to electronic surveillance, the Supreme Court has twice rejected the use of ex parte proceedings on grounds that apply equally here. In Alderman v. United States, the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to the prosecution case against the defendants.

The Court rejected the Government's suggestion that the District Court make that determination in camera and/or ex parte, and observed:

> An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Id. at 182.

In ordering disclosure of improperly recorded conversations, the Court declared:

> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge,

---

deprivations.'…. [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." American-Arab Anti-Discrimination Committee v. Reno, 70 F.3d 1045, 1069 (9th Cir. 1995) (quoting District Court); see, e.g., id. at 1070 (noting "enormous risk of error" in use of secret evidence); Kiareldeen v. Reno, 71 F.Supp.2d 402, 412-14 (D.N.J. 1999) (same).

> through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

Id. at 184.

Likewise, the Court held in Franks v. Delaware, 438 U.S. 154 (1978), that a defendant, upon a preliminary showing of an intentional or reckless material falsehood in an affidavit underlying a search warrant, must be permitted to attack the veracity of that affidavit. The Court rested its decision in significant part on the inherent inadequacies of the ex parte nature of the procedure for issuing a search warrant, and the contrasting enhanced value of adversarial proceedings:

> the hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily *ex parte*, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an ex parte inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

Franks, 438 U.S. at 169.

The same considerations that the Supreme Court found compelling in

Alderman and Franks militate against ex parte procedures in the FISA context. After all, denying an adversary access to the facts constitutes an advantage as powerful and insurmountable as exists in litigation.

Conversely, the lack of access to specific facts categorically impairs the ability of a defendant (or his counsel, even cleared counsel) to establish non-compliance with the strictures of 50 U.S.C. § 1881a. For example, the factual background of this pleading can only be based on assumptions from the public record, including a heavily redacted 2011 FISC opinion and testimony before the Privacy and Civil Liberties Oversight Board (hereinafter "PCLOB") at a March 19, 2014, public hearing.[17]

However, courts have recognized that when defense counsel is compelled to argue in a vacuum devoid of a factual context to which only the Government and

[17] The PCLOB is an independent, bipartisan agency within the executive branch whose members are appointed by the President and confirmed by the Senate. PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 2 (Jan. 23, 2014). The PCLOB conducted a public hearing March 19, 2014, at which the General Counsels of the Federal Bureau of Investigation, the National Security Agency, and the Director of National Intelligence, as well as the Deputy Assistant Attorney General for the Department of Justice's National Security Division, provided testimony about programs operated under § 1881a. See *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act Before The PCLOB* (2014) (transcript available at <http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf>).

Nonetheless, even the PCLOB information is of limited value because, *inter alia*: the witnesses did not purport to provide information regarding the protocols and practices in effect at the time of the surveillance in this case, which was probably from 2010-2011; the information provided was limited to declassified material; and the testimony was not under oath, not from individuals with first hand knowledge, and not subject to more than very limited questioning.

the court have access, a defendant's burden must be alleviated. As the Fourth Circuit has recognized in a closely analogous context – discerning what exculpatory evidence a witness solely within the Government's control, and to whom the defense is denied access, can provide – when a defendant is deprived of such access, the burden to be specific with respect to the material in question must be relaxed accordingly. See United States v. Moussaoui, 382 F.3d 453, 472 (4th Cir. 2004), citing, United States v. Valenzuela-Bernal, 458 U.S. 858, 870-71, 873 (1982).

Here, that adjustment applies, as Hasbajrami and his cleared counsel are compelled to operate in a system in which the admissibility of evidence at the core of the Government's case – in this case, in effect the *entirety* of the Government's case – is decided on the basis of a secret body of facts *and* law to which even cleared defense counsel is denied access.

Also, with respect to justification for disclosure of FISA and FAA materials to defense counsel in this case, the NSA's non-compliance clearly rises to level described in United States v. Duggan, 743 F.2d 59, 79 (2d Cir. 1984), in which the Second Circuit, relying on FISA's legislative history, explained that the need for disclosure:

> might arise if the judge's initial review revealed potential irregularities such as possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards

contained in the order[.]

Duggan, 743 F.2d at 79; see also United States v. Belfield, 692 F.2d 141, 147 (D.C.Cir. 1982) (quoting S. Rep. No. 701, 95th Cong., 2d Sess. 64 [1979]); United States v. Ott, 827 F.2d 473, 476 (9th Cir. 1987) (same).

Here, as previously discussed, the FISC opinions have provided that very catalog of "irregularities." Accordingly, it is respectfully submitted that the Court should order disclosure to cleared defense counsel the FISA and FAA applications and supporting materials, which will enable the Court to render its decisions with full participation by defense counsel consistent with the principles of the adversary system.[18]

C. The details of the FAA electronic surveillance should be produced because motions based on the FAA's unconstitutionality and application against Hasbajrami require full factual development

As discussed in Defendant's June 30, 2014 motion for discovery (*ecf* #76), which had been raised at the time in the context of Hasbajrami's since-realized desire to withdraw his guilty plea, the Government's notice that it intended to use the products of 50 U.S.C. § 1881a surveillance in proceedings in this case was merely the starting point for consideration of the appropriate remedy that should be ordered after the means, methods, and extent of the Government's surveillance of

[18] See Hon. James G. Carr, Op-Ed, "A Better Secret Court," *N.Y. Times*, July 23, 2013, available at <http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html?ref=opinion&_r=1&>.

Hasbajrami are fully developed in this case.

The present case involves the surveillance of an individual "located in the United States" – Hasbajrami – notwithstanding the limitation against surveilling such an individual under 50 U.S.C. § 1881a(b):

> An acquisition authorized under subsection (a) –
>
> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) 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;
>
> * * *
>
> (4) 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
>
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

Discovery regarding the targeting, scope, manner, authorizations, limitations, and mitigation of the intrusions (or lack thereof) are needed to effectively complete the arguments regarding the legality and derivative use of the surveillance in this case. As such, we respectfully submit that the defense should have full access to the relevant facts to inform – and if necessary, supplement – legal arguments

challenging the fruits of the surveillance undertaken here.

The discovery order should also include all targeting and minimization procedures, including interpretive instructions, that were in effect at all times the Government conducted surveillance of Hasbajrami. The disclosures by Edward Snowden include purported FAA targeting and minimization procedures under FISA and the FAA See 50 U.S.C. §§ 1801(h)(1), 1881a(d), 1881a(e); see also Glenn Greenwald & James Ball, *The top secret rules that allow NSA to use US data without a warrant*, The Guardian, June 20, 2013.

Since those initial revelations, some of the disclosed rules have been declassified, while others remain classified, and still others are likely classified but not publicly disclosed or released. See Press Release, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)* (Aug. 21, 2013).

As such, this Court's order should require specification of which procedures were in effect on all dates that Hasbajrami was subject to surveillance because the Director of National Intelligence ("DNI") has acknowledged that rules during that rough time frame violated the Fourth Amendment.

In a letter from the Director's office to Senator Wyden, the DNI included the admissions that

- "on at least one occasion the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the Section 702

minimization procedures used by the government was unreasonable under the Fourth Amendment," and

- the agency believed "the government's implementation of Section 702 of FISA has sometimes circumvented the spirit of the law, and on at least one occasion the FISA Court has reached this same conclusion."

Letter from the Office of the DNI to Senator Ron Wyden, dated, July 20, 2012, available at <http://www.wired.com/images_blogs/dangerroom/2012/07/2012-07-20-OLA-Ltr-to-Senator-Wyden-ref-Declassification-Request.pdf> (last accessed, November 23, 2014); see also [Case Name Redacted], supra, 2011 WL 10945618, at *16, *28 (FISC Oct. 3, 2011) (the case referenced by the DNI in its July 20, 2012 letter to Senator Wyden); Charlie Savage, *N.S.A. Said to Search Content of Messages To and From U.S.*, N.Y. Times, Aug. 8, 2013.

The Government should be compelled to state whether the DNI's response to Senator Wyden relates in any way to the investigation of Hasbajrami and/or this case.

Further, because recent declassified FISC decisions have found that historical government conduct from the outset of the FAA was unlawful, this Court should order that the defense have access to all decisions, classified or not, that find problems with the conduct of surveillance under the procedures in effect from 2010-2011, or earlier if any of the FAA surveillance referenced in the Government's February 24, 2014 notice (*ecf* #65) was surveillance that occurred *prior to* the offense conduct alleged in Hasbajrami's Indictment.

Aside from facial and as-applied constitutional challenges to the statute, as well as the purely statutory claims, factual development and access to the relevant protocols will enable the defense to present arguments regarding the second half of the statutory suppression standard: whether the Government acted within the scope of the authorizations and orders. Even assuming the FAA is valid, suppression is warranted if the "surveillance was not made in conformity with an order of authorization or approval." 50 U.S.C. §§ 1806(e)(2), 1806(g).

As set forth in Defendant's Second Motion, supra, recently declassified FISC opinions reveal that the relevant agencies have a long and persistent history of violating the limitations of FISC orders. Without discovery regarding all of the surrounding factual circumstances of the surveillance, the defense here cannot effectively complete our arguments for suppression based on lack of compliance with the required authorizations.

D. The complexity and the need for accurate factual determinations strongly support full defense access to surveillance material and advocacy regarding its significance

The scope of appropriate disclosure to the defense corresponds to the depth and complexity of the potential motions to suppress as well as to the potential for disclosing Brady material. The statute provides for an aggrieved person to file a motion for suppression where the information was either unlawfully acquired or acquisition was conducted outside the scope of an order of authorization or

approval. See 50 U.S.C. § 1806(f).

To be certain, information is unlawfully acquired if the statute is unlawfully applied or if the statute itself is unconstitutional. See ACLU Found. of S.Cal. v. Barr, 952 F.2d 457, 465 (D.C.Cir. 1991) ("Section 1806[f] requires the court to decide whether the surveillance was 'lawfully authorized and conducted.' The Constitution is law.").

The Government's failure to adhere to the limitations on the scope of surveillance would therefore support Hasbajrami's motions to suppress both direct and derivative evidence:

> If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person.

50 U.S.C. § 1806(g).

Even if the suppression motions are denied, this Court must review the information to determine whether material considered in relation to the motion, assuming it was reviewed ex parte, requires production as Brady material: "If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." Id.

The statute confers authority on this Court to order disclosure to defense counsel "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). In this provision, Congress intended to strike "a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information." S.Rep.No. 95-701 at 64 (1978).

The developments since the Snowden disclosures and the institutionalized suppression of notice revealed after Clapper establish that this case fits exactly what Congress thought should trigger full defense participation: disclosure may be "necessary" when there are "indications of possible misrepresentation of fact" and other problems indicating the need for adversarial review. Id.

Courts have explained that disclosure to the defense is warranted if the legal and factual issues involved in reviewing the surveillance are "complex," and where "the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards contained in the order.' " United States v. Belfield, 692 F.2d 141, 147 (D.C.Cir. 1982) (quoting S.Rep.No. 95-701 at 64 [1978]); accord United

States v. Ott, 827 F.2d 473, 476 (9th Cir. 1987).

These factors must be assessed in light of the Supreme Court's recognition that valuable defense input is lost when review of the legality of electronic surveillance is conducted ex parte. See Alderman v. United States, supra, 394 U.S. 165, 184 (1969); see also United States v. Abu-Jihaad, supra, 630 F.3d 102, 141 (2d Cir. 2010) ("Although applicable in criminal cases, the state-secrets privilege must – under some circumstances – 'give way … to a criminal defendant's right to present a meaningful defense.' "), quoting, United States v. Stewart, 590 F.3d 93, 131 (2d Cir. 2009).

We note that if the Government asserts the "state-secrets" privilege as a basis for its continued refusal to disclose the material under dispute, the Second Circuit has held that the test announced in Roviaro v. United States, 353 U.S. 53 (1957), should be applied. See Abu-Jihaad, 630 F.3d at 141. As the Second Circuit explained, the first question is "whether the material in dispute is discoverable, and if so, whether the state-secrets privilege applies," and the second question is, if the privilege applies, "whether the information is helpful or material to the defense, i.e., useful to counter the government's case or to bolster a defense." Id., quoting Stewart, 590 F.3d at 131 (citing Roviaro).

The Second Circuit also observed, however, "Information that is helpful or material to the defense 'need not rise to the level that would trigger the

Government's obligation under Brady v. Maryland … to disclose exculpatory information.' " Abu-Jihaad, 630 F.3d at 141 n.33, quoting, United States v. Aref, supra, 533 F.3d 72, 80 (2d Cir. 2008), and citing, United States v. Mejia, 448 F.3d 436, 457 (D.C.Cir. 2006) (observing that, for purposes of the analogous provisions of the Classified Information Procedures Act, "information can be helpful without being 'favorable' in the Brady sense").

E. The balance of the factors this Court considers in determining defense participation requires full defense access and advocacy

Under the present circumstances, the balance strongly favors disclosure: the need for government secrecy has been radically reduced by the public disclosures of previously secret programs; the need for adversary proceedings has been recognized by a presidential study group; the legal and factual complexity of the issues in this case favor full defense participation; and there are reasonable grounds to question the candor and completeness of the security apparatus's representations.

1. The need for secrecy has been reduced by the Edward Snowden disclosures

The Government has either publicly acknowledged or failed to deny the broad range of electronic surveillance now attributed to it. Prior to Hasbajrami's guilty plea, the mass collection of telephone and Internet content and metadata was speculative; now it is fact. As a result of the Snowden disclosures and other revelations, there are no longer compelling reasons for secrecy, or to the extent they

remain, cleared defense counsel should be allowed look under the veil. The gathering of all of Hasbajrami's telephone call and Internet metadata (along with everyone else's metadata) was not previously known, but now the secret is out. The Government likely has records of every one of Hasbajrami's calls and Internet communications prior to any FISA warrant.

The only questions remaining are whether and under what circumstances the Government obtained and accessed surveillance, the lawfulness of the authority or conduct of the surveillance, and how the patterns of communication can be helpful to the defense. The Government need for ex parte proceedings has collapsed now that the secrets this Court was balancing against disclosure are part of general public discourse.

2. The benefits of adversarial proceedings are recognized by the President's Review Group

The public debate surrounding the Snowden disclosures has exposed the serious flaws that ex parte proceedings import into the structure of our country's legal system. President Obama's national security review recognized that our adversary system is compromised, and the benefits of defense advocacy are lost, in a system that does not include an advocate for individual privacy. See The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, Recommendation 28 (Dec. 12, 2013) (recommending, inter alia, "Congress should create the position of Public Interest

Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court," and "the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards") (available at <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>)(last accessed, November 24, 2014).

The rationale for an advocate before the Foreign Intelligence Surveillance Court applies equally to the need for security-cleared counsel in this case to provide technological and legal perspectives to balance against the Government's one-sided presentations in proceedings before the District Court:

> Our legal tradition is committed to the adversary system. When the government initiates a proceeding against a person, that person is usually entitled to representation by an advocate who is committed to protecting her interests. If it is functioning well, the adversary system is an engine of truth. It is built on the assumption that judges are in a better position to find the right answer on questions of law and fact when they hear competing views. When the FISC was created, it was assumed that it would resolve routine and individualized questions of fact, akin to those involved when the government seeks a search warrant. It was not anticipated that the FISC would address the kinds of questions that benefit from, or require, an adversary presentation. When the government applies for a warrant, it must establish "probable cause," but an adversary proceeding is not involved. As both technology and the law have evolved over time, however, the FISC is sometimes presented with novel and complex issues of law. The resolution of such issues would benefit from an adversary proceeding.

> In our system of justice, defense counsel standing for the rights of the accused traditionally provides competing arguments needed by a neutral decision-maker.
>
> We have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts.

United States v. Nixon, 418 U.S. 683, 709 (1974) (citation omitted).

While recognizing that secrecy is sometimes permissible, this Court acts in the best traditions of our justice system by recognizing the benefits of full adversary participation where, as here, the circumstances call for careful scrutiny of complex legal issues based on voluminous material.

3. The complexity of the legal issues warrants defense participation

Substantial issues exist regarding the constitutionality of the FAA as well as the application of the FAA and other surveillance programs to Hasbajrami. These concerns were readily evident from the colloquies between Respondent's lawyer and several of the Justices during the Clapper oral argument. Justice Kagan noted that the FAA "greatly expands the government's surveillance power. Nobody denies that." Transcript of Oral Argument at 17, Clapper, 133 S.Ct. 1138 (2013). Similarly, Justice Ginsburg noted that certain checks required for traditional FISA

surveillance do not exist in the FAA:

> JUSTICE GINSBURG: Mr. Jaffer, could you be clear on the expanded authority under the FAA? As I understood it, it's not like in [FISA], where a target was identified and … the court decided whether there was probable cause. Under this new statute, the government doesn't say who the particular person or the particular location. So, there isn't that check. There isn't that check.
>
> MR. JAFFER: That's absolutely right, Justice Ginsburg … the whole point of the statute was to remove those tests, to remove the probable cause requirement, and to remove … the requirement that the government identify to the court the facilities to be monitored. So those are gone.
>
> That's why we use the phrase "dragnet surveillance." I know the government doesn't accept that label, but it concedes that the statute allows what it calls categorical surveillance, which … is essentially the surveillance the plaintiffs here are concerned about.

Id. at 32-33.

Justice Breyer stated that the program is not limited to wiretapping alleged terrorists or foreign agents, noting that any conversation touching on "foreign intelligence" information could be implicated: "the definition of foreign intelligence information … defines it to include information with respect to a foreign power or foreign territory that relates to the conduct of foreign affairs. It's very general." Id. at 43.

The competing interests of privacy and national security are also the subject of a current judicial debate regarding whether the defense perspective is essential to

a fair disposition. Compare Klayman v. Obama, Docket No. 13-0851, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (the metadata collection program likely unconstitutional) with ACLU v. Clapper, Docket No. 13 Civ. 3994, 2013 WL 6819708 (SDNY Dec. 27, 2013) (upholding the metadata collection program).

Similarly, the President's Review Group used collection of telephone metadata under section 215 of FISA as a "good example" of the "serious and difficult questions of statutory and constitutional interpretation about which reasonable lawyers and judges could certainly differ," finding that better decisions result from adversary presentations:

> On such a question, an adversary presentation of the competing arguments is likely to result in a better decision. Hearing only the government's side of the question leaves the judge without a researched and informed presentation of an opposing view.

Review Group Report at 203-04.

In addition to debating the scope and lawfulness of surveillance, a defense advocate is necessary to present the legal arguments on the inclusion of false statements or material omissions within the meaning of Franks v. Delaware, 438 U.S. 154 (1978), on the use of evidence derived from earlier unlawful surveillance to make decisions under Murray v. United States, supra, 487 U.S. 533, 542-43 (1988), and to held determine whether the use of any such derivative evidence in subsequent FISA applications requires suppression as the "fruit of the poisonous

tree" under Silverthorne v. United States, supra, 251 U.S. 385, 392 (1920), Nardone v. United States, supra, 308 U.S. 338, 342 (1939), and/or Wong Sun v. United States, supra, 371 U.S. 471, 488 (1963).

Further, compliance with complicated statutes upon which there is little precedent militates in favor of defense participation. The simple determination of probable cause in the standard FISA case is often "relatively straightforward and not complex." United States v. Abu-Jihaad, supra, 630 F.3d 102, 129 (2d Cir. 2010).

Although the FISA issues in the present case have their own share of novelty and complexity, the complicated legal and factual issues under the FAA receive little guidance from the Circuit Courts or other Districts about how to evaluate the constitutionality of orders granting applications for FAA surveillance or actual execution of the surveillance. Indeed, this is the first case in this Circuit to address this issue.

As such, defense advocacy is reasonable and necessary given the serious and difficult questions this case presents, as well as the importance and effect any precedent will create. In addition, the Government's previous non-disclosure further demonstrates the need for defense counsel participation in the process of adjudicating all aspects of Hasbajrami's motions.

4. Congress anticipated that evidence of misrepresentation and other over-reaching would favor disclosure and defense participation

The legislative history of FISA specifically stated that "indications of possible misrepresentation of fact" could establish the necessity for defense participation in discovery and suppression proceedings. S.Rep. 95-701 at 64. Congress set an intentionally low bar for favoring defense participation: "indications" and "possible". Here, of course, this Court has already concluded that "[w]hen the government provided FISA notice without FAA notice, Hasbajrami was misled about an important aspect of his case," misrepresentation which resulted from "a DOJ policy that transcended this case" (Order, dated, October 2, 2014, at 6 [*ecf* #85]).

As a result, the intentionally misleading FISA notice that the Government originally filed in this case, which misled Hasbajrami but also presented a fraud upon defense counsel and this Court, provides a legitimate basis to view any ex parte Government submission with great suspicion in this case; such, we submit, supports the need to permit adversarial testing *in all aspects* of the defendant's suppression motions.

We respectfully submit that Hasbajrami, or, at a minimum this Court, is entitled to know, for example, if the Government misled the FISC when it sought authorization to conduct FAA surveillance, assuming the Government did in fact

request such authorization, as well as whether the Government misled the FISC when it subsequently applied for FISA warrants in this case. Failure to provide such notice to the FISC would be relevant to the Constitutional issues presented in this case.

It is worth noting that it cannot be presumed that the Government understood and/or followed its obligations when interacting with the FISC in association with its investigation of Hasbajrami and others related to this case. On August 21, 2013, the Government declassified the opinion of District Judge John Bates holding that aspects of the surveillance authorized by 50 U.S.C. § 1881a (i.e., Section 702 of the FAA) was unconstitutional. See [Case Name Redacted], supra, No. [docket number redacted], 2011 WL 10945618 (FISC Oct. 3, 2011). While ultimately continuing surveillance authorizations after insisting on modification of the minimization protocols, Judge Bates made a record of serious concerns regarding the legal authority and agency actions in carrying out that authority.

The opinion detailed the Government's May 2011 disclosure to the Foreign Intelligence Surveillance Court that, contrary to previous statements, the NSA was relying on the FAA to collect Internet communications that are "wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection," and that the NSA "might lack confidence in the effectiveness" of procedures for ensuring that persons

targeted with FAA surveillance of their Internet transactions are actually located overseas. Id. at *2.

In other words, at the very same time it was conducting electronic surveillance and interception of Hasbajrami's communications, the Government "advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court had been led to believe." Id. at *9. These disclosures "fundamentally alter[ed] the Court's understanding of the scope of the collection conducted pursuant to Section 702," which had previously been based on erroneous representations that "acquisition of Internet communications under Section 702 would be limited to discrete 'to/from' communications between or among individual account users and to 'about' communications falling within [redacted] specific categories that had been first described to the Court in prior proceedings." Id. at *5.

The Government's applications for authorization to conduct FAA surveillance in that instance therefore contained all of the problems that justify disclosure: "misrepresentation of fact, vague identification of the persons to be surveilled, [and collection of] surveillance records which include a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards" contained in past orders. United States v. Belfield, 692 F.2d 141, 147 (D.C.Cir. 1982). These problems also appear to

coincide temporally with the period of FAA surveillance related to Hasbajrami's prosecution.

The errors in the Government's applications to the FISC, including its applications for FAA surveillance authorization, are not merely "typographical or clerical in nature." United States v. El-Mezain, 664 F.3d 467, 566 (5th Cir. 2011) (internal quotation marks omitted). Rather, "the errors [are] . . . pervasive enough to confuse the court as to the quantity or quality of the evidence described in the applications," such that "disclosing the applications and related materials to defense counsel would assist the court in making an accurate determination of the legality of the surveillance." Id. at 567 (internal quotation marks omitted).

Notably, in a separate disclosure, it has been revealed that Government agents have been laundering intelligence from NSA electronic intercepts to disguise their origins: "[L]aw enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges." John Shiffman & Kristina Cooke, *U.S. directs agents to cover up program used to investigate Americans*, Reuters, Aug. 5, 2013.

The governmental agencies that distributed information include the FBI, the CIA, and the NSA, all of which were likely involved in the present case. Although the Reuters documents are undated, they "show that federal agents are trained to 'recreate' the investigative trail to effectively cover up where information

originated." Id. Interviews with law enforcement personnel showed the practice, denominated "parallel construction," is widespread to protect sources, but "employing the practice as a means of disguising how an investigation began may violate pretrial discovery rules by burying evidence that could prove useful to criminal defendants." Id.

Given the record of affirmative misrepresentations and omissions made by the Government in its applications for 50 U.S.C. § 1881a authorizations (as well as its misrepresentations and omissions in applications for orders authorizing other forms of FISA surveillance), discovery is warranted so that the defense and this Court may effectively assess whether the fruits of those authorizations must now be suppressed.

Indeed, because numerous FISC opinions – including opinions authorizing FAA surveillance – remain classified, the defense has no way to know the extent of the Government's misrepresentations to the FISC and noncompliance with its orders. As such, for all of these reasons, we respectfully submit that disclosure under 50 U.S.C. § 1806(f) is necessary to permit the adversarial testing that accurate review of these issues requires.

F. This Court should grant discovery because litigation regarding the lawfulness of Government surveillance accomplishes important societal purposes of transparency and deterrence

Meaningful review regarding the Government's compliance, or lack of

compliance, with the FAA and thereafter with FISA, accomplishes essential societal functions beyond protection of the defendant's individual rights. Constitutions and statutes are merely a collection of toothless platitudes in some countries. In the United States, transparency and deterrence of governmental misconduct are essential to the rule of law that sets us apart by giving the promise of justice meaning in the real world.

50 U.S.C. § 1881a specifically protects not merely United States citizens, but anyone located within the United States at the time of the surveillance – such should be particularly true here where the defendant was a legal immigrant living in the United States on a permanent visa, not someone who entered this country illegally or with an unlawful purpose in mind.[19] As such, the public interest strongly favors discovery and defense participation in all proceedings.

G. This Court should also require the Government to provide the defense with notice of any other surveillance statutes and/or programs it used and/or relied upon during the investigation of this case to which Hasbajrami was aggrieved

Finally, given the number of surveillance programs that the Government has concealed for years, it is possible that the Government relied on other, still-secret surveillance techniques in its investigations of Hasbajrami. Discovery thus far suggests that the Government tracked Hasbajrami's location, financial activities,

[19] There is no dispute that Hasbajrami immigrated to the United States to pursue the American dream, and that he was only first exposed to radical Islam after he had moved to Brooklyn.

and communications. However, the Government belated FAA notice also indicates that the Government has been less than candid in complying with its notice obligations.

Thus, to ensure that Hasbajrami's right to Due Process is not still being infringed upon in manners simply not yet revealed, Hasbajrami's motion for discovery, including notice of undisclosed surveillance, is not limited to the surveillance programs described above nor even those methods publicly acknowledged to date. See, e.g., Charlie Savage & Mark Mazzetti, *C.I.A. Collects Global Data on Transfers of Money*, N.Y. Times, Nov. 13, 2013, http://nyti.ms/1lbhseL ("Several officials also said more than one other bulk collection program has yet to come to light."). Indeed, with respect to monitoring financial transactions, during Hasbajrami's first encounter with FBI agents he was asked by them (prior to any relevant discussion) whether he had ever sent any money overseas.

As such, Hasbajrami's request for notice encompasses any surveillance program or technique that the Government relied upon to monitor Hasbajrami's communications or activities as part of its investigation related to this case. See 18 U.S.C. § 3504; see also 50 U.S.C. § 1845; Due Process Clause, Fifth Amend., U.S. Const.

H. Conclusion

Accordingly, for all of the reasons discussed above, the defense respectfully requests that the Government be directed to disclose the following, either directly to counsel, or, at a minimum, to this Court for *in camera* review:

1. Any "foreign intelligence information" relevant to this case that has not been previously disclosed to the defense;

2. Whether the FAA surveillance relied upon against Hasbajrami intentionally targeted the defendant (see 50 U.S.C. §§ 1881a[b][1], 1881a[b][2]), and/or engaged in "reverse targeting" of him;

3. Whether the FAA surveillance relied upon against Hasbajrami intentionally targeted "a United States person reasonably believed to be located outside of the United States" (50 U.S.C. § 1881a[b][3]);

4. Whether the FAA surveillance relied upon against Hasbajrami "intentionally acquire[d] any communication as to which the sender and all intended recipients [were] known at the time of the acquisition to be located in the United States" (50 U.S.C. § 1881a[b][4]);

5. Whether the Government has any reason to believe that the FAA surveillance relied upon against Hasbajrami were not "conducted in a manner consistent with the fourth amendment to the Constitution of the United States" (50 U.S.C. § 1881a[b][5]);

6. Copies of all FISA warrants and FISA warrant applications not previously disclosed to the defense in this case;

7. Material documenting what minimization and targeting procedures and interpretive instructions were in effect at the time any foreign intelligence evidence or information was gathered, and how those procedures were implemented (i.e., who was being targeted, what was the basis for that targeting, and what minimization procedures were used during that targeting);

8. What information, if anything, was told to was the Foreign Intelligence Surveillance Court (FISC) about FAA surveillance relative to Hasbajrami (or other persons relevant to this case) in approving any FISA warrants in this case;

9. Notice of whether any other surveillance programs were utilized and/or relied upon during the investigation of this case and aggrieved Hasbajrami; and

10. Notice of whether any "programmatic analytics" were utilized, or whether cross-referencing or searching or analysis occurred with respect to the information derived from FAA and FISA surveillance and interception, and/or any other surveillance, interception, collection, and/or retention program.

Sixth Motion

MOTION FOR AN ORDER DIRECTING THE GOVERNMENT TO IDENTIFY ANY AND ALL WITNESSES THAT IT LEARNED OF DURING, OR AS A RESULT OF, THE INTERROGATION OF THE DEFENDANT

Pursuant to Rule 12(b)(4) and Rule 16 of the Federal Rules of Criminal Procedure, the defendant respectfully requests that this Court issue an order directing the Government to specify in detail any witness about whom they became aware of through, or as a result of, interrogation of Agron Hasbajrami described Defendant's Fourth Motion, supra. This information is necessary to enable the defense to move for exclusion of the testimony of such witness(es), should the Government elect to call such witness(es) at trial.

Seventh Motion

MOTION FOR AN ORDER DIRECTING THE GOVERNMENT TO SPECIFY ALL EVIDENCE THAT IS SUBJECT TO SUPPRESSION AND/OR PRECLUSION AS A RESULT OF THE INTERROGATION OF THE DEFENDANT

Pursuant to Rule 12(b)(4) and Rule 16 of the Federal Rules of Criminal Procedure, the defendant respectfully requests that the Court issue an order directing the Government to specify in detail any evidence that it intends to offer at trial, which the Government became aware of either directly or indirectly through the interrogation of Hasbajrami described in Defendant's Fourth Motion, supra. This information is necessary to enable the defense to move for exclusion of the testimony of such witness(es), should the Government elect to call those witness(es) at trial.

Eighth Motion

MOTION FOR AN ORDER DIRECTING THE GOVERNMENT TO PROVIDE IMMEDIATE NOTICE OF EXPERT WITNESSES IT INTENDS TO RELY UPON AT TRIAL

Pursuant to Rule 12(b)(4) and Rule 16 of the Federal Rules of Criminal Procedure, the defendant respectfully requests that this Court issue an order directing the Government to provide immediate notice of any expert witnesses it intends to rely upon at trial. This information is necessary to enable the defense to

move to limit or exclude the testimony of such witness(es), should the Government elect to call such witness(es) at trial.

Ninth Motion

MOTION FOR IMMEDIATE PRODUCTION OF BRADY/GIGLIO MATERIAL

As a result of our review of information disclosed in this case, as well as our knowledge of relevant and related information disclosed in other cases to which the undersigned has been involved, defense counsel have a good faith basis to believe that information favorable to the defense exists in this case that will require extensive litigation in order to determine what aspects of such evidence may be presented to the jury. As such, due to this Court's stated desire to avoid unnecessary delay, we respectfully submit that all information that is discoverable to the defense under either Brady v. Maryland, 373 U.S. 83, 104 (1963), or United States v. Giglio, 405 U.S. 150 (1972), should be immediately disclosed to the defense. See also Kyles v. Whitley, 514 U.S. 419 (1995); United States v. Mahaffy, 693 F.3d 113, 130 (2d Cir. 2012).

As such, beyond evidence favorable to the defense under Brady, we also specifically request that the Government produce, for immediate review, all Giglio material, which would include any information that would substantially impeach the credibility of an important Government witness, including but not limited to, expert

witnesses that the Government intends to rely upon at trial. This request, more fully addressed in the legal discussion below, includes, with regard to such witnesses:

1. Prior inconsistent statements, including, but not limited to, inconsistent attorney proffers (see United States v. Triumph Capital Group, 544 F.3d 149 [2d Cir. 2008]);

2. Statements or reports reflecting witness statement variations;

3. Benefits provided to witnesses including:

   a. Dropped or reduced charges
   b. Immunity
   c. Expectations of downward departures or motions for reduction of sentence
   d. Assistance in a state or local criminal proceeding
   e. Considerations regarding forfeiture of assets
   f. Stays of deportation or other immigration status considerations
   g. S-Visas
   h. Monetary benefits
   i. Non-prosecution agreements
   j. Letters to other law enforcement officials (e.g., state prosecutors, parole boards) setting forth the extent of a witness's assistance or making substantive recommendations on the witness's behalf
   k. Relocation assistance
   l. Consideration or benefits to culpable or at risk third-parties

4. Other known conditions that could affect the witness's bias such as:

   a. Animosity toward defendant
   b. Animosity toward a group of which the defendant is a member or with which the defendant is affiliated
   c. Relationship with victim
   d. Known but uncharged criminal conduct (that may provide an incentive to curry favor with a prosecutor)

5. Prior acts under Fed.R.Evid. 608;

6. Prior convictions under Fed.R.Evid. 609;

7. Known substance abuse or mental health issues or other issues that could affect the witness's ability to perceive and recall events; and

8. With particular respect to expert witnesses, any other information that could bare upon their bias, including, but not limited to, any information that bares upon the independence of their testimony and whether they had ever, to the Government's knowledge, testified in a manner that was intended to intentionally mislead the Court, the jury, and/or defense counsel.

The law has long been clear that Brady v. Maryland, supra, 373 U.S. 83, 104 (1963), requires the Government to disclose evidence "favorable" to the defense as to guilt or punishment. To be favorable, evidence need not be determinative of guilt or innocence, but must "tend to exculpate" the defendant. See Brady, 373 U.S. at 88.

A defendant is also entitled to disclosure of "evidence affecting [the] credibility" of a witness whose reliability may be dispositive of guilt or innocence. United States v. Giglio, supra, 405 U.S. 150, 154 (1972), quoting, Napue v. Illinois, 360 U.S. 264, 269 (1959). As stated by the Supreme Court in United States v. Bagley, 473 U.S. 667 (1985), "[i]mpeachment evidence ... as well as exculpatory evidence, falls within the Brady rule." Id. at 674, citing Giglio, 405 U.S. at 150. This is self-evident, since "[t]he jury's estimate of the truthfulness and reliability of a given witness may well be determinative of guilt or innocence." United States v. Seijo, 514 F.2d 1357, 1364 (2d Cir. 1975), quoting, Napue, 360 U.S. at 269.

It has long been the rule that Brady material, including material to be used to impeach critical Government witnesses, must be turned over sufficiently in advance of trial to allow "for full exploration and exploitation by the defense." Grant v. Alldredge, 498 F.2d 376, 382 (2d Cir. 1974); see also United States v. Baum, 482 F.2d 1325, 1331 (2d Cir. 1973) ("Ordinarily it is disclosure rather than suppression, that promotes the proper administration of criminal justice."). Indeed, "There is no doubt that the timing of disclosure under Brady and Giglio may be of critical importance in many criminal cases." United States v. Coppa, 267 F.3d 132, 138 (2d Cir. 2001). As such, disclosure is required "in time for its effective use at trial or at a plea proceeding" and "the time required for the effective use of a particular item of evidence … depend[s] on the materiality of that evidence," which, of course, only the prosecutor can determine prior to disclosure. Coppa, 267 F.3d at 146.

The United States Attorney Manual recommends broader discovery than even that specifically prescribed by Brady, Giglio, or Kyles:

> Department policy recognizes that a fair trial will often include examination of relevant exculpatory or impeachment information that is significantly probative of the issues before the court but that may not, on its own, result in an acquittal or, as is often colloquially expressed, make the difference between guilt and innocence. As a result, this policy requires disclosure by prosecutors of information beyond that which is "material" to guilt as articulated in Kyles v. Whitley, 514 U.S. 419 (1995), and Strickler v. Greene, 527 U.S. 263, 280-81 (1999).

United States Attorney's Manual ("USAM") § 9-5.001(C).

Similarly, in reviewing what material should be provided in this case, we suggest that the following excerpts of Sections 9-5.001 and 9-5.100 of the United States Attorney Manual should also be considered:

> 1. **Additional exculpatory information that must be disclosed.** A prosecutor must disclose information that is inconsistent with any element of any crime charged against the defendant or that established a recognized affirmative defense, regardless of whether the prosecutor believes such information will make the difference between conviction and acquittal of the defendant for a charged crime.
>
> 2. **Additional impeachment information that must be disclosed.** A prosecutor must disclose information that either casts a substantial doubt upon the accuracy of any evidence – including but not limited to witness testimony – the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information must be disclosed regardless of whether it is likely to make the difference between conviction and acquittal of the defendant for a charged crime.
>
> 3. **Information.** Unlike the requirements of Brady and its progeny, which focus on evidence, the disclosure requirement of this section applies to information regardless of whether the information subject to disclosure would itself constitute admissible evidence.
>
> 4. **Cumulative impact of items of information.** While items of information viewed in isolation may not reasonably be seen as meeting the standards outlined in paragraphs 1 and 2 above, several items

> together can have such an effect. If this is the case, all such items must be disclosed.

USAM § 9-5.001(C).

> **Preface:** The following policy is established for … "investigative agencies"…. It addresses their disclosure of potential impeachment information to the United States Attorneys' Offices and Department of Justice litigating sections with authority to prosecute criminal cases…. The purposes of this policy are to ensure that prosecutors receive sufficient information to meet their obligations under Giglio v. United States, 405 U.S. 150 (1972), and to ensure that trials are fair….
>
> The exact parameters of potential impeachment information are not easily determined. Potential impeachment information, however, has been generally defined as impeaching information which is material to the defense. It also includes information that either casts a substantial doubt upon the accuracy of any evidence – including witness testimony – the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information may include but is not strictly limited to: (a) specific instances of conduct of a witness for the purpose of attacking the witness' credibility or character for truthfulness; (b) evidence in the form of opinion or reputation as to a witness' character for truthfulness; (c) prior inconsistent statements; and (d) information that may be used to suggest that a witness is biased.

USAM § 9-5.100.

In United States v. Crozzoli, 698 F.Supp. 430, 436-37 (EDNY 1988) (Glasser, J.), the court reasoned:

> [W]e reject the blanket assertion that Brady imposes no pretrial obligation on ... the Government .... We perceive the due process implications of Brady as obligating the Government to disclose exculpatory information as soon as the character of such information is recognized.

Crozzoli, 698 F.Supp. at 436, quoting, United States v. Mitchell, 372 F.Supp. 1239, 1257 (SDNY 1973) (emphasis in original).

As another District Court judge recognized, "[I]f exculpatory evidence is produced for the first time at trial, the defendant may not have an adequate opportunity to effectively utilize the material, particularly if it points to the existence of other evidence helpful to the defendant." United States v. Goldman, 439 F.Supp. 337, 349 (SDNY 1977) (Duffy, J.); see also United States v. Pollack, 534 F.2d 964, 973 (D.C. Cir. 1976) (disclosure "must be made at such time as to allow the defense to use the favorable material effectively in the preparation and presentation of its case"); United States v. Deutsch, 373 F.Supp. 289, 290 (SDNY 1983) ("[i]t should be obvious to anyone involved with criminal trials that exculpatory information may come too late if it is given only at trial").

We acknowledge that in Coppa, 267 F.3d at 146, the Second Circuit limited early Giglio discovery to impeachment evidence that is material to the offense. However, we note that more recently the Second Circuit expanded its definition of "materiality" when it reversed a conviction, holding, "Where suppressed evidence is inculpatory as well as exculpatory, and 'its exculpatory character harmonize[s] with

the theory of the defense case,' a Brady violation has occurred." United States v. Mahaffy, supra, 693 F.3d 113, 130 (2d Cir. 2012) (emphasis added).[20]

The foregoing analysis forecloses the argument that evidence, which is similarly discoverable under both Brady and the Jencks Act, may be withheld until trial; the timing of discovery under the Jencks Act certainly does not trump the obligations imposed as a matter of due process under Brady/Giglio. See Coppa, 267 F.3d at 146 (holding that notwithstanding the Jenks Act the pertinent question is whether the "impeachment evidence … r[o]se to the level of materiality prescribed by Agurs and Bagley"); see also United States v. McVeigh, 923 F.Supp. 1310, 1315 (D.Colo. 1996) (duty to turn over exculpatory and impeachment information under Brady neither altered nor modified by fact that information is contained in witness statements or grand jury testimony, "Therefore, such statements should now be provided."). Similarly, in United States v. Persico 164 F.3d 796 (2d Cir. 1999), the Second Circuit held that all Brady material – including that required to be disclosed by Giglio – must be disclosed before entry of a pretrial guilty plea:

> Rule 32(e) allows a defendant to withdraw a guilty plea before sentencing for "any fair and just reason." The Government's obligation to disclose Brady materials is pertinent to the accused's decision to plead guilty; the defendant is entitled to make that decision with full

[20] This principle also militates in favor or disclosure under 50 U.S.C. §§ 1806(f), 1806(g), as it is extraordinarily difficult, if not impossible, for a court to recognize how evidence possesses an exculpatory character because it "harmonizes with the defense theory of the case." That is the function of defense counsel.

> awareness of favorable (exculpatory and impeachment) evidence known to the Government.

164 F.3d at 804 (emphasis added) (citation omitted). If Brady/Giglio disclosure is required prior to a plea, at least absent a waiver, then certainly it is required before a trial when no waiver has, or likely ever would, occur.

Finally, we note that this Court has the inherent authority to order discovery beyond the bounds of the discovery rules, and as such this Court need not confine itself to Jenks Act or other discovery rules when it comes to scheduling the Government's disclosure requirements. See United States v. Beckford, 962 F.Supp. 748, 755 (E.D.Va. 1997) (collecting cases); see also United States v. Perez, 222 F.Supp.2d 164, 171 (D.Conn. 2002) (recognizing the court's authority to order early discovery through its "inherent power to manage its docket and provide for the orderly and timely disposition of cases"); cf. United States v. Feliciano, 998 F.Supp. 166, 170 (D.Conn. 1998) ("Rule 16 is 'intended to prescribe the minimum amount of discovery to which the parties are entitled. It is not intended to limit the judge's discretion to order broader discovery in appropriate cases."), citing, Fed.R.Crim.P. 16, Advisory Committee Note.

Here, Hasbajrami is charged in a four-count indictment, involving extremely serious offenses. Hasbajrami's prosecution has also taken on considerable national – and international – attention due to the unique legal issues involved in this case. See, e.g., Charlie Savage, *Justice Dept. Informs Inmate of Pre-Arrest Surveillance,*

N.Y. Times, Feb. 25, 2014; Andrew Keshner, *Terrorism Suspect Allowed to Withdraw Guilty Plea*, N.Y. Law Journal, Oct. 6, 2014; *Albanian man can withdraw terror plea over warrantless surveillance*, The Guardian, Oct. 6. 2014.

Accordingly, we respectfully submit that all Brady material, including Giglio material, should be disclosed immediately to the defense, particularly if it "harmonize[s] with" the Government's understanding of "the theory of the defense case." Mahaffy, 693 F.3d at 130.

Tenth Motion

MOTION FOR EARLY DISCLOSURE OF 3500 MATERIAL

For similar reasons as those outlined in Defendant's Ninth Motion, supra, the defense requests a court order directing the Government to provide early disclosure of 3500 material. To that end the defense requests that 3500 material be produced at least 30 days prior to trial. There exists a unique pubic importance to this case and the discovery thus far disclosed is both voluminous and complex. As such, we respectfully submit that early production of 3500 material will help ensure that no unnecessarily delays occur that might derail a timely and efficient trial.

Eleventh Motion

MOTION FOR NOTICE OF EVIDENCE THE GOVERNMENT INTENDS TO OFFER UNDER FED.R.EVID. 404(b)

Fed.R.Evid. 404(b) requires the Government, upon request of the defense, to provide pretrial notice of evidence it intends to offer under Fed.R.Evid. 404(b). We call upon the Government to provide such notice, and to do so at least 30 days prior to trial.

V. Other Motions

Twelfth Motion

MOTION FOR LEAVE TO SUBMIT FURTHER MOTIONS

Defense counsel have endeavored to bring all unclassified motions applicable at this time but request leave to bring any additional motions – classified and/or unclassified – which may become necessary based upon the Government's response to the present motions or new facts uncovered by the defendant's ongoing investigation into this case.

Similarly, and as merely one example, the Government has been ordered to complete its Section 4, 18 U.S.C. App. 3, applications by January 9, 2015. Defense counsel reserves the right to file motions, pursuant to Section 5 of the Classified Information Procedures Act, 18 U.S.C. App. 3, at the appropriate time after this Court rules on the Government's Section 4 applications.

Additionally, Hasbjarami's FAA and FISA-related suppression motions are based upon the assumptions that: (1) all of the FISA-related evidence that the Government intends to rely upon at trial was derived either directly or indirectly from FAA surveillance; and (2) that no argument will be raised by the Government that certain of its evidence was sufficiently attenuated or derived from an independent source.

Defense counsel base these assumptions on the Government's Supplemental Notice, dated, February 24, 2014, as well as arguments made during oral argument on September 12, 2014, which were had in relationship to Hasbajrami's Section 2255 and Rule 33-related discovery motions (see *ecf* #76). See, e.g., Gov't Sup. Notice, dated, February 24, 2014 (*ecf* #65), at 1 (the Government providing notice to Hasbajrami that "evidence and information, obtained or derived from Title I or III FISA collection, that the government intended to offer into evidence or otherwise use or disclose in proceedings in this case was derived from acquisition of foreign intelligence information conducted pursuant to the FAA").

To the extent, however, that the Government's response to the present suppression motions raises – now for the first time – the attenuation and/or independent source doctrines, then we respectfully submit leave to file additional FISA motions, including, suppression motions based upon, for example,.50 U.S.C. § 1805(a).

Conclusion

WHEREFORE, Defendant Agron Hasbajrami, by and through his attorneys, respectfully moves for the relief set forth herein, and for such other and further relief as this Court may deem just and proper.

Dated: New York, New York
November 26, 2014

Respectfully submitted,

Michael K. Bachrach
Steve Zissou
Attorneys for Defendant
Agron Hasbajrami

Also on the brief: Joshua L. Dratel, Esq.