UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

FOR ONLINE PUBLICATION

UNITED STATES OF AMERICA

- against -

AGRON HASBAJRAMI,

Defendant.

MEMORANDUM
11-CR-623 (JG)

JOHN GLEESON, United States District Judge:

Defendant Agron Hasbajrami was arrested on September 6, 2011 and charged with three counts of attempting to provide material support to terrorists. He sought to suppress evidence obtained or derived from surveillance conducted pursuant to Section 702 of the FISA Amendments Act ("FAA"), codified at 50 U.S.C. § 1881a (alternatively, "702 surveillance" or "702 collection"). *See* Def.'s Mot. to Supp., ECF No. 92 ("Def. Br."). This memorandum explains my February 20, 2015 ruling denying the motion to suppress.

PRELIMINARY STATEMENT

Few things are more unsettling than the idea that a government is spying on its own citizens.[1] Our country has a long history of holding our government accountable when it abuses its authority in ways that offend our Constitution's protections.

In the 1960s and 1970s, the public was outraged over the revelation that the government conducted domestic surveillance—in the name of national security—of Dr. Martin Luther King, Jr., Vietnam War protesters, and domestic groups the government labeled "subversive." *See* David S. Kris & J. Douglas Wilson, 1 *National Security Investigations and*

[1] "Citizen" in this opinion refers to both United States citizens and lawful permanent residents.

Prosecutions § 3.1 (2d ed. 2012) (hereafter "Kris & Wilson"). In 1967, the Supreme Court held that electronic surveillance is subject to the Fourth Amendment's prohibition on unreasonable searches. *Katz v. United States*, 389 U.S. 347 (1967) (the government's electronic surveillance of a phone conversation in a telephone booth constitutes a search under the Fourth Amendment); *Berger v. New York*, 388 U.S. 41 (1967) (the Fourth Amendment protects conversations, and the use of electronic devices to capture a conversation is a search). In 1976, a select committee of the United States Senate, chaired by Senator Frank Church of Idaho, issued an exhaustive report (the "Church Report") documenting the intelligence community's systematic violations of the law in gathering information about United States citizens. Kris & Wilson § 2.2 (citing Final Rep. of the S. Select Comm. to Study Governmental Operations with respect to Intelligence Activities (Book II), S. Rep. No. 94-755, (1976)). Congress responded to the Church Report in 1978 by enacting the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, which governs foreign intelligence surveillance and searches. *See* S. Rep. No. 95-604, at 7-8 (1977).

History repeats itself. The post-9/11 era has once again highlighted the tension between privacy and national security interests. The public continues to scrutinize the government's intelligence gathering techniques.[2] But there is also no denying that in this era there are individuals and groups dedicated to inflicting grave harm on our nation, and that the intelligence gathering techniques at issue here are a critical component of our government's efforts to protect us from harm. The government has a duty to respect and protect our

---

[2] *See, e.g.*, Charlie Savage, *F.B.I. is Broadening Surveillance Role, Report Shows*, N.Y. Times, Jan. 11, 2015, at A10; Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014, *available at* https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story html; Claire Cain Miller, *Tech Companies Concede to Surveillance Program*, N.Y. Times, June 8, 2013, at A12.

constitutional rights while simultaneously ensuring the nation's security. This is a difficult task. And while there has been legitimate criticism of electronic surveillance practices under the FAA—in large part because it has been shrouded in secrecy—in this case, the government conducted its national security investigation within the confines of the Fourth Amendment.

FACTUAL BACKGROUND

A. *The Criminal Investigation*

An investigation by the Federal Bureau of Investigation's Joint Terrorism Task Force ("JTTF") revealed that from April 2, 2011 to August 28, 2011, Hasbajrami exchanged numerous emails with an individual he believed was associated with a terrorist organization. Gov't Unclassified Br. at 5 ("Gov't Br."). Hasbajrami sent money to the individual to support Islamic fundamentalist terrorism operations. *Id.* He also arranged to travel to the Federally Administered Tribal Areas ("FATA") of Pakistan to join a jihadist fighting group. *Id.*

On September 6, 2011, JTTF agents arrested Hasbajrami at John F. Kennedy International Airport as he was about to board a flight to Turkey en route to Pakistan. *Id.* A subsequent search of Hasbajrami's luggage "revealed a tent, boots, and cold-weather gear." Def. Br. at 4 (citing PSR at ¶¶ 2-3). Hasbajrami gave detailed statements regarding his offense. *Id.*

B. *The Government's Disclosure of its FISA Surveillance*

Title I and Title III of FISA, as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829, allow electronic surveillance and physical searches after obtaining a FISA warrant from the Foreign Intelligence Surveillance Court ("FISC").

On September 13, 2011, after Hasbajrami was arraigned, the government notified him that he had been subject to FISA surveillance and that it intended at trial to use information obtained or derived from that surveillance ("Title I collection") and certain physical searches

("Title III collection"). Notice, ECF No. 9. On April 12, 2012, after the government disclosed inculpatory evidence—including email communications obtained pursuant to FISA—Hasbajrami pled guilty to a single count of providing material support to terrorists. ECF No. 32. On January 8, 2013, I sentenced him principally to a 180-month term of imprisonment. ECF No. 44.

In July 2013, Hasbajrami filed a motion pursuant to 28 U.S.C. § 2255, seeking relief from his conviction and sentence on the ground that the statute under which he was convicted is unconstitutionally vague. Letter, ECF No. 61-1. Before that claim could be fully briefed and argued, the government revealed new information that eventually became the basis of the instant motion. Specifically, on February 24, 2014, the government notified Hasbajrami "that certain evidence or 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." Supplemental Notice, ECF No. 65.

The FAA permits, subject to certain statutory requirements, the interception of electronic communications of non-U.S. persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. 50 U.S.C. §1881a. It differs significantly from traditional FISA surveillance. To get a court order, FISA requires the government to demonstrate probable cause to believe that the "target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(2). By contrast, FAA surveillance does not require the government to specify the persons or places that it plans to target for surveillance. 50 U.S.C. §1881a. Instead, the FISC may authorize surveillance under

the FAA for up to one year after approving targeting and minimization procedures and receiving a government certification regarding the proposed surveillance. *See* 50 U.S.C. §1881a(a), (c), and (i)(3)(A). Because the FAA does not require an individual court authorization (that is, a warrant) for each data collection, FAA-derived intelligence has been described as "warrantless wiretap" information. *See, e.g.*, Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct. 27, 2013, at A21.

C. *The Withdrawal of the Guilty Plea*

On October 2, 2014, I allowed Hasbajrami to withdraw his guilty plea so he could challenge the constitutionality of the FAA-derived evidence and seek its suppression.[3] Order, ECF No. 85. Hasbajrami filed this motion to suppress on November 26, 2014, and I heard oral argument on the motion on January 23, 2015. On February 20, 2015, I denied the motion for the reasons discussed below. On June 26, 2015, Hasbajrami pled guilty to one count of attempting and one count of conspiring to provide material support to terrorists. ECF No. 142. I sentenced him on August 13, 2015, principally to a 192-month term of imprisonment. ECF No. 151.

DISCUSSION

Hasbajrami contends that the FAA surveillance violated the Fourth Amendment because it was not "confined to the collection of foreign communications by foreign actors" outside the United States. Def. Br. at 15-16. Because the government knew that the

---

[3] Specifically, I allowed Hasbajrami to:

> [W]ithdraw his plea of guilty because I conclude that he was not sufficiently informed about the facts. Under the precise circumstances presented here, and because of a DOJ policy that transcended this case, Hasbajrami could not have made an intelligent decision about whether to plead guilty: When the government provided FISA notice without FAA notice, Hasbajrami was misled about an important aspect of his case.

Order, ECF No. 85, at 6.

communications of U.S. persons—like Hasbajrami—inevitably would be collected, the argument goes, it was required to get a warrant. *See id.* Hasbajrami thus sought to suppress the FISA evidence on which the government's case was based because it was the fruit of the warrantless FAA surveillance.

For its part, the government argues that the FAA collection was constitutional because: (1) the warrant requirement is inapplicable to foreign intelligence collection targeted at foreign persons abroad, and the incidental collection of U.S. persons' communications did not trigger the warrant requirement; (2) the foreign intelligence exception to the warrant requirement applies; and (3) the FAA surveillance was reasonable under the Fourth Amendment. Accordingly, the government's argument continues, the FISC properly used the FAA-derived information in finding probable cause to support the FISA warrants, and the FISA collection was thus constitutionally sound.[4]

A. *The History of the Foreign Intelligence Surveillance Act*

As mentioned above, the government's surveillance activities came under scrutiny in the 1970s when it was discovered that the National Security Agency ("NSA") had been spying on United States citizens within the United States. *ACLU v. Clapper*, 785 F.3d 787, 792-93 (2d Cir. 2015). In 1972, the Supreme Court held that warrantless domestic surveillance violated the Fourth Amendment. *United States v. U.S. Dist. Court for the E. Dist. of Mich. ("Keith")*, 407 U.S. 297, 320-21 (1972). Three years later, Congress established the Select Committee to Study Governmental Operations with respect to Intelligence Activities (the "Church Committee") to investigate whether the government's "intelligence activities were governed and controlled consistently with the fundamental principles of American constitutional government[.]" Church

[4] Specifically, the FISC found that probable cause existed to believe that the target was an agent of a foreign power and that the target was using or about to use the facilities and places targeted for the FISA surveillance and search. Gov't Classified Br. at 23 ("Gov't Cl. Br.").

Report at v. The Church Committee found that the intelligence community had "violated specific statutory prohibitions and infringed the constitutional rights of American citizens [and had] intentionally disregarded [these prohibitions] in the belief that because the programs served the 'national security' the law did not apply."[5] *Id.* at 137. The Church Committee's findings, coupled with the Supreme Court's *Keith* decision and evidence of abuse by intelligence agencies, led to Congress's 1978 enactment of FISA, which was "aimed at curtailing abuses and delineating the procedures to be employed in conducting surveillance in foreign intelligence investigations." *Clapper*, 785 F.3d at 793.

1. *The Foreign Intelligence Surveillance Act*

FISA seeks to "provide effective, reasonable safeguards to ensure accountability and prevent improper surveillance." S. Rep. No. 95-604, at 7 (1977). The statute created the FISC and empowered it to grant or deny applications for surveillance orders in foreign-intelligence investigations. *See* 50 U.S.C. § 1803(a). "As originally enacted, FISA required a high-ranking member of the executive branch to certify that the purpose [of the FISA application] was to obtain foreign intelligence information." *United States v. Abu-Jihaad*, 630 F.3d 102, 119 (2d Cir. 2010) (internal quotation marks omitted). But in 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act") amended the statute to require a high-ranking official to certify that "a significant purpose" of the FISA application was to obtain foreign intelligence information. Pub. L. No. 107-56, 115 Stat. 272, 291 (2001) (codified as amended at 50 U.S.C. § 1804(a)(6)(B)). Thus, the amendments signaled that Congress no longer required foreign

[5] Intelligence agencies' illegal activities included covert mail-opening programs, warrantless "surreptitious entries," *i.e.*, break-ins, and the interception of domestic telegram and radio communications. Church Report at 139.

intelligence gathering to be the primary purpose of the FISA surveillance. *See Abu-Jihaad*, 630 F.3d at 119.

To obtain a FISA order, the government must make detailed factual showings about the target of the surveillance, the information sought, and the facilities at which the surveillance is directed. 50 U.S.C. § 1804(a). The FISC may issue an order authorizing electronic surveillance only if it finds probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power and that the facilities or places at which the surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power. *Id.* § 1805(a)(2)(A)-(B). A FISA order targeting a U.S. person may be approved for up to 90 days, and an order targeting a non-U.S. person may be approved for up to 120 days. *Id.* § 1805(d)(1).

FISA requires the government to implement minimization procedures reasonably designed to minimize the acquisition and retention, and prohibit the dissemination of, communications by United States citizens.[6] *Id.* §§ 1801(h)(1), 1821(4)(A). The Attorney General must approve all FISA applications to the FISC. *Id.* § 1805(a)(1).

2. *The Protect America Act and the FISA Amendments Act*

Under FISA, the definition of "electronic surveillance" was limited to four types of domestically-focused foreign intelligence collection activities.[7] *See* 50 U.S.C. § 1801(f).

---

[6] The Attorney General has adopted standard minimization procedures ("SMPs") for FISA-authorized surveillance and physical searches. Gov't Cl. Br. at 30. They are on file with the FISC and are incorporated by reference into every FISA application and every FISA order. *Id.* The FISC orders at issue here directed the government to follow the approved minimization procedures in conducting the electronic surveillance and physical searches. *Id.*

[7] Specifically, "electronic surveillance" was defined to mean: (1) the acquisition of the contents of a wire or radio communication obtained by "intentionally targeting" a "particular, known United States person who is *in the United States*" in certain circumstances; (2) the acquisition of the contents of a wire communication to or from a "person *in the United States*" when the "acquisition occurs in the United States"; (3) the intentional acquisition of the contents of certain radio communications when the "sender and all intended recipients are located *within the United States*"; and (4) the installation or use of a surveillance device "*in the United States*" for monitoring or to

Because that definition did not apply to surveillance conducted outside the United States, Congress enacted the Protect America Act ("PAA") in 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007), to modernize FISA in light of the "changes in communications technology" since 1978. S. Rep. No. 110-209 (Oct. 26, 2007) ("For example, in 1978, most foreign communications went through the air rather than over a wire . . . . Today, most international communications travel over a wire."). The PAA empowered the Director of National Intelligence ("DNI") and the Attorney General to authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States." *Id.* § 105B(a). The PAA required the DNI and the Attorney General to certify that there were reasonable targeting procedures in place to ensure that the surveillance targeted persons reasonably believed to be outside the United States; that the minimization procedures in place satisfied FISA's requirements for such procedures; and that a significant purpose of the acquisition was to obtain foreign intelligence information. *Id.* § 105B(a)(1)-(5).

The PAA, however, expired in February 2008 due to a sunset provision. In response, in July 2008, Congress enacted the FAA. The provision of the FAA at issue here, Section 702, "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad."[8] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013). Specifically, Section 702 (like the PAA before it) provides that upon the issuance of an order from the FISC, the Attorney General and the DNI may jointly authorize the "targeting of persons reasonably believed to be located outside the United States" for a

---

acquire information other than from a wire or radio communication in certain circumstances. 50 U.S.C. § 1801(f) (emphasis added).

[8] The definition of a U.S. person under Section 702 is incorporated from Title I of FISA and means a citizen of the United States or a lawful permanent resident. 50 U.S.C. §§ 1801(i), 1881(a). Hasbajrami is a lawful permanent resident.

period of up to one year to acquire "foreign intelligence information." 50 U.S.C. § 1881a(a). This includes any information "necessary to protect against the full range of foreign threats to national security, and information with respect to a foreign power that is necessary to the national defense or foreign affairs." Kris & Wilson § 17.3 (citing 50 U.S.C. §§ 1881a(a), 1801(e)). Consistent with its purpose, the statute prohibits intentionally targeting anyone located inside the United States and any United States citizens outside of the United States.[9] 50 U.S.C. § 1881a(b)(1)-(3).

Surveillance conducted pursuant to Section 702 does not require an individualized court order for each non-U.S. person to be targeted. Rather, the FISC approves annual certifications by the Attorney General and the DNI, thereby authorizing the acquisition of foreign intelligence information by targeting non-U.S. persons reasonably believed to be located outside the United States.[10] *Id.* § 1881a(a), (i)(3). The statute does not require the certifications to

---

[9] Under § 1881a(b), the government: "(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 . . . is to target a particular, known person reasonably believed to be in the United States; (3) may not intentionally target a United States person reasonably believed to be located outside 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) [an acquisition] shall be conducted in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. § 1881a(b)(1)-(5). *Amici* argue that one of the purposes of Section 702 was to enable "reverse targeting," *i.e.*, the legal targeting of a non-U.S. person abroad to capture the communications of U.S. persons that are otherwise subject to the warrant requirement, *Amici* Br. at 13, but the statute explicitly prohibits such targeting. *See id.* § 1881a(b)(2).

The NSA's determination of the target's location and non-U.S. person status is based on the totality of the circumstances. Privacy and Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* at 43 (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report.pdf ("PCLOB Report"). If conflicting information draws the target's location or status into question, the NSA must resolve the question before the person can be targeted. *Id.* at 44. In making the determination that the surveillance will lead to the acquisition of foreign intelligence information, the NSA must identify the specific foreign power or foreign territory from which the intelligence is being sought. *Id.* at 45.

[10] The Attorney General and the DNI must make the certifications, 50 U.S.C. § 1881a(g)(1), and they must attest that: (1) there are targeting procedures in place, which have been or will be submitted for approval by the FISC, that are reasonably designed to ensure that the acquisition is limited to targeting persons reasonably believed to be located outside the United States and to prevent the intentional acquisition of purely domestic communications; (2) the minimization procedures meet the definition of minimization procedures set forth in Titles I and III of FISA (50 U.S.C. §§ 1801(h), 1821(4)) and have been or will be submitted for approval by the FISC; (3) guidelines have been adopted by the Attorney General to ensure compliance with the aforementioned limitations set forth in § 188la(b) prohibiting, among other things, the targeting of U.S. persons; (4) the targeting and minimization

identify the facilities to be targeted for surveillance. *Id.* § 1881a(g)(4). Instead, the FISC approves the proposed targeting and minimization procedures, and if it finds that the certification contains the required elements and that those procedures are consistent with the Fourth Amendment, it issues an order authorizing the certification. *See id.* § 1881a(i)(3)(A).

The targeting procedures must be "reasonably designed" to ensure that the surveillance is limited to persons reasonably believed to be located outside the United States, and 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.* § 1881a(g)(2)(A)(i). Minimization procedures must also be "reasonably designed . . . 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." 50 U.S.C. §§ 1801(h)(l), 1821(4)(A). Thus, the targeting and minimization procedures aim to safeguard U.S. citizens against the acquisition of their communications under Section 702.

3. *Types of FAA Surveillance*

There are two types of Section 702 collection: PRISM and Upstream. *See* PCLOB Report at 7, 33. In PRISM collection, the government identifies the user accounts it wants to monitor and sends a "selector"—a specific communications facility, such as a target's email address or telephone number—to the relevant communications service provider. *Id.* at 32-33. A government directive then compels the communications service provider to give it

---

procedures and guidelines are consistent with the Fourth Amendment; (5) a significant purpose of the acquisition is to obtain foreign intelligence information; (6) the acquisition involves obtaining "foreign intelligence information from or with the assistance of an electronic communication service provider;" and (7) the acquisition complies with the limitations in 50 U.S.C. §1881 a(b) (*i.e.*, the targeting procedures). 50 U.S.C. § 1881a(g)(2)(A).

communications sent to or from that selector (*i.e.*, the government "tasks" the selector).[11] *Id.* at 33; 50 U.S.C. § 1881a(h). This type of surveillance, which intercepts "to/from" communications, can result in the interception of communications with U.S. persons if the target happens to communicate with such a person. *See* PCLOB Report at 33.

Upstream collection, on the other hand, involves the acquisition of communications through the compelled assistance of the providers that control the telecommunications backbone within the United States over which communications travel. *Id.* at 35. Like PRISM, upstream collection intercepts "to/from" communications. *Id.* at 37. But upstream collection is less tailored than PRISM collection; it allows the government to additionally intercept "about" communications, that is, communications that refer to, or are "about," a particular selector. *Id.* For example, an email in the body of which a targeted email address appears is an "about" communication, even though the targeted person is not necessarily a participant in the intercepted communication.[12] *Id.* If a communication is to, from, or about a

---

[11] Before a selector can be "tasked," that is, before service providers are compelled to forward communications associated with a selector, the NSA analyst must document his or her reasons for tasking it, and two senior NSA analysts must approve the tasking. NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, at 4-5 (Apr. 16, 2014), *available at* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf ("NSA Report"). In PRISM collection, "the Government provides selectors to service providers through the FBI. The service providers are compelled to provide NSA with communications to or from these selectors." NSA Report at 5.

[12] The PCLOB Report provides a detailed description of the mechanics of Upstream collection:

> Finally, the upstream collection of Internet communications includes two features that are not present in PRISM collection: the acquisition of so-called 'about' communications and the acquisition of so-called 'multiple communications transactions' ('MCTs'). An 'about' communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being 'to' or 'from' the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be 'about' the selector. An MCT is an Internet 'transaction' that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or 'about' a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.

tasked selector, the NSA can acquire an entire MCT, which may contain more than one discrete communication. *Id.* at 39-41. Simply put, the government can collect other discrete communications that do not have anything to do with the tasked selector, which can result in the collection and querying of wholly domestic communications of non-targeted persons.[13] *Id.* at 7; NSA Report at 5-6. Some have argued that the FISC erred in its approval in 2011 of "about" communications collection, instead of limiting Section 702 surveillance to communications intercepted by "to/from" collection. *See, e.g.*, Donohue at 159; First Amended Complaint, *Wikimedia Found. v. NSA*, 15-CV-00662, ¶ 50 (D. Md. June 19, 2015) (equating upstream collection with allowing "a government agent [to] open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase").

The government conducted the disputed surveillance in this case under the PRISM program. Gov't Cl. Br. at 54. None of the Section 702 communications used in the Title I and Title II FISA applications targeting the agent of a foreign power were "about" communications. *Id.* Thus, the constitutionality of upstream collection is not at issue here.

B. *The Constitutionality of Section 702 is Limited to an As Applied Challenge*

As a preliminary matter, Hasbajrami asserts a facial challenge and an "as applied" challenge to the constitutionality of Section 702 collection. Def. Br. at 13-31. A facial challenge would require Hasbajrami to establish that there is no set of circumstances under which Section 702 is valid. *United States v. Salerno*, 481 U.S. 739, 745 (1987). Given that the government "implemented [the statute] in a defined context" in this case, I need not "speculate about the

---

PCLOB Report at 7.

[13] "FISC estimated in 2011 that somewhere between 300,000 and 400,000 MCTs were being collected annually on the basis of 'about' communication—where the 'active user' was not the target. So hundreds of thousands of communications were being collected that did not include the target as either the sender or the recipient of the communication." Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol'y 117 (2015), *available at* http://scholarship.law.georgetown.edu /cgi/viewcontent.cgi?article=2364&context=facpub.

validity of the law as it might be applied in different ways or on different facts." *In re Directives*, 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008); *see also Ayotte v. Planned Parenthood of N. New England*, 546 U.S. 320, 328-30 (2006) (discussing the Court's preference for as-applied challenges in an attempt to "limit the solution to the problem"); *United States v. Mohamud*, 2014 WL 2866749, at *13-14 (D. Oreg. June 24, 2014) (declining to consider a facial challenge under the Fourth Amendment to Section 702 collection). I therefore limit Hasbajrami's challenge to an as-applied challenge.

C. *Warrantless Surveillance Pursuant to Section 702 is Lawful Under the Fourth Amendment When It Targets Non-U.S. Persons Abroad*

The Fourth Amendment protects an individual's "persons, houses, papers, and effects, against unreasonable searches and seizures." For a search or seizure to be consistent with the Fourth Amendment, it must be carried out with a valid warrant, based on probable cause, and be issued by a neutral and detached judicial officer (or fall under one of the exceptions to the warrant requirement). The central inquiry in my Fourth Amendment analysis is "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security." *Terry v. Ohio*, 392 U.S. 1, 19 (1968). Because Section 702 does not require a warrant before the government can seize the communications of non-U.S. persons abroad, the dispute before me centers on whether the search of communications between a U.S. person and individuals who are legitimate targets of Section 702 surveillance is constitutional. For the reasons that follow, I conclude that it is.

1. *The Fourth Amendment Does Not Apply to Foreign Persons Abroad*

The Fourth Amendment's protections do not "apply to activities of the United States directed against aliens in foreign territory." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990) (non-U.S. persons outside the United States who lack a "substantial connection"

with the country do not benefit from the Fourth Amendment's protections). Accordingly, under *Verdugo-Urquidez*, the Fourth Amendment does not constrain the government from collecting the communications of non-U.S. individuals targeted by Section 702 surveillance. The collection at issue was directed at non-U.S. persons the government reasonably (and correctly) believed were located in foreign countries. Although Hasbajrami was a legal resident of the United States who was in the country when he communicated with one or more non-U.S. persons abroad, it was those non-U.S. persons who were the targets of Section 702 surveillance.

Defendant and *amici* challenge the fact that the FAA allows the government to collect these communications without establishing probable cause or finding individualized suspicion. Def. Br. at 6, 10-11; *Amici* Br. at 14. However, because the warrant requirement is inapplicable here, so too is the need to establish probable cause or individualized suspicion.

2. *The Incidental Collection of U.S. Persons' Communications with Lawfully Targeted Non-U.S. Persons Abroad Does Not Trigger the Warrant Requirement*

The real question is whether the incidental interception of U.S. persons' communications during the otherwise lawful collection of non-U.S. persons' communications is constitutional. While Section 702 does not allow intentional targeting of U.S. persons or non-U.S. persons located in the United States, 50 U.S.C. §1881a(b)(1)-(4), it is inevitable that the government will incidentally intercept communications of persons who are not the intended targets—including, as here, U.S. persons in the United States—during the ordinary course of lawful surveillance.

Minimization and targeting procedures help protect the privacy interests of U.S. persons whose communications are incidentally intercepted. Minimization procedures mask the identities of U.S. persons whose communications the government incidentally collects. *See In re Directives*, 551 F.3d at 1015 (effective minimization procedures "serve . . . as a means of

reducing the impact of incidental intrusions into the privacy of non-targeted United States persons"). The minimization procedures in this case required the NSA to conduct post-targeting analyses to effectuate a stop of the acquisition of communications without delay if it learned at any point that the target had either entered the United States or was in fact a U.S. person. Gov't Cl. Br. at 108.

Hasbajrami contends that the collection of U.S. persons' communications during 702 surveillance targeting non-U.S. persons abroad cannot be properly considered "incidental" because the government knows that the foreign targets will inevitably communicate with U.S. persons, Def. Br. at 11-12, and the minimization procedures permit the government to retain the communications under certain circumstances. Gov't Br. at 31 ("Such circumstances may include where the U.S. person has consented to the dissemination, the specific information about the U.S. person is already publicly available, the U.S. person's identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities." (citing PCLOB Rep. at 64-65)). However, the government notes that the same is true of Title I FISA surveillance and Title III electronic surveillance, "in which, inevitably, the government collects communications of third parties and the minimization procedures permit retention of those communications in certain circumstances." Gov't Cl. Br. at 80. As with the FISA and Title III collection, acquisitions from Section 702 surveillance are not made unlawful by "incidental collections occurring as a result of constitutionally permissible acquisitions." *In re Directives*, 551 F.3d at 1015 (warrantless surveillance of individuals reasonably believed to be outside the United States under the PAA was reasonable). The collection of U.S. persons' communications—incidentally obtained through lawful targeting—does not require a separate warrant.

Courts have long dealt with the issue of incidental interception of non-targeted persons' communications.[14] *Amici* correctly point out that some of those cases involve surveillance predicated on warrants, *Amici* Br. at 14 (citing *Kahn*, 415 U.S. at 143 and *Figueroa*, 757 F.2d at 466), but that is because the targets at issue were U.S. citizens and the surveillance took place on United States soil. *See Kahn*, 415 U.S. at 144-49 and *Figueroa,* 757 F.2d at 468-69. A warrant was necessary for the initial surveillances to be lawful. While those cases are thus distinguishable, the guiding principle behind them applies with equal force here: when surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad[15]—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful. *Mohamud*, 2014 WL 2866749, at *15 ("The § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's communications with the extraterritorial target would be lawful.").[16]

---

[14] *See, e.g.*, *United States v. Kahn*, 415 U.S. 143, 157-58 (1974) (interception of wife's conversations on her home telephone was incidental, and not in violation of the Fourth Amendment, because her criminal activities were not foreseen when Title III wiretap order targeting her husband was obtained); *United States v. Figueroa,* 757 F.2d 466, 472-73 (2d Cir. 1985) (Title III allows interception of conversations of "others as yet unknown," *i.e.*, unknown third parties, and that "does not render a statute [] unconstitutional on its face as authorizing a general warrant"); *United States v. Butenko,* 494 F.2d 593, 608 (3d Cir. 1974) (upholding the constitutionality of warrantless surveillance for foreign intelligence purposes even though "conversations . . . of American citizens[] will be overheard"); *United States v. Bin Laden,* 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.").

[15] The government concedes that information-gathering under Section 702 takes place within the United States. Gov't Br. at 43. But what matters here is the location of the *target*. *See* Kris & Wilson, § 17.3 ("For non-U.S. person targets, there is no probable-cause requirement; the only thing that matters is []the government's reasonable belief about[] the target's location."). The mere fact that Section 702 surveillance originated from within the United States, or that the communications obtained through such surveillance originated from or terminated within the United States, is not enough to trigger the warrant requirement. The government intercepted the emails in this case because Hasbajrami communicated with foreign persons outside the United States, at email addresses believed to belong to them. Section 702 requires that the government reasonably believe that the non-U.S. person is located outside the United States in order to target them. 50 U.S.C. § 1881a(a). The facts here indicate that the government reasonably (and correctly) believed that the persons Hasbajrami communicated with were non-U.S. persons abroad, and thus the government was well within its boundaries. That the seizure took place from within the United States does not alter these facts, and therefore does not implicate the warrant requirement.

[16] Hasbajrami also contends that the FAA is unconstitutional because it permits surveillance and interception without probable cause, particularity, or the involvement of a neutral and detached judicial officer. Def.

3. *PRISM Collection is Reasonable Under the Fourth Amendment*

"The ultimate touchstone of the Fourth Amendment is reasonableness[,]" and the requirement that the PRISM collection at issue here be reasonable applies even when the warrant requirement does not. *Brigham City, Utah v. Stuart*, 547 US 398, 403 (2006). Thus, I must determine whether Section 702 meets the general reasonableness standard. *Id.* The statute aims to collect foreign intelligence information to protect national security. As discussed above, I must balance that interest with U.S. persons' privacy interests in their international communications. *See Samson v. California*, 547 U.S. 843, 848 (2006) (applying the totality of the circumstances test to the Fourth Amendment reasonableness inquiry). I have balanced these interests and find the intelligence gathering here is reasonable under the Fourth Amendment.

a. *The Government Has a Compelling Interest in Obtaining Foreign Intelligence Information to Protect National Security*

The 702 surveillance at issue here furthered an indisputably compelling government interest. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) ("Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order."); *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (internal quotation marks omitted)); *see also In re Directives*, 551 F.3d at 1012 (the government's national security interest in acquiring foreign intelligence information pursuant to the PAA "is of the highest order of magnitude"). The fruits of the surveillance led to the prosecution and conviction

---

Br. at 22-30. But because the warrant requirement is inapplicable here, so too is the necessity for "the three principal warrant requirements: prior judicial review, probable cause, and particularity." *In re Directives*, 551 F.3d at 1013 ("We therefore decline the petitioner's invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable."). Additionally, because I find that the surveillance at issue did not require the government to get a warrant, I consider it unnecessary to determine whether the good-faith exception to the exclusionary rule or the foreign intelligence exception to the warrant requirement apply, and I thus decline to do so.

of a U.S. person who was attempting to lend support to a terrorist organization whose purpose is to inflict serious harm upon the United States.

b. *Individuals Have a Diminished Expectation of Privacy in Email Communications with Non-U.S. Persons Outside the United States*

In evaluating the reasonableness of the incidental acquisition of non-targets' communications, I consider the degree to which U.S. citizens have a reasonable expectation of privacy in their email communications with non-U.S. persons abroad.

A person's expectation of privacy in email communications diminishes after sending the email because he or she assumes the risk that the recipient will share the communication with others. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("[An individual] may not . . . enjoy [] an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient."); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (email sender loses his or her legitimate expectation of privacy in an email that has already reached the recipient). Email communications are easily forwarded to or read by other parties. But this diminished expectation of privacy in email communications does not mean the government can search every email with impunity just because the email sender communicated with a foreign person abroad.[17]

Analogizing to traditional post-mail, the government contends that an email sender "loses any cognizable Fourth Amendment rights" in the communication once it reaches the recipient. Gov't Br. at 62; *see also United States v. Gordon*, 168 F.3d 1222, 1228 (10th Cir. 1999) ("[O]nce a letter is sent to someone, the sender's expectation of privacy ordinarily

[17] I reject the government's contention that "any expectation of privacy of the defendant in his electronic communications with a non-U.S. person overseas is . . . diminished by the prospect that his foreign correspondent could be a target for surveillance by foreign governments or private entities, whose activities are not governed by the United States Constitution or federal law, *or by the U.S. Government*, pursuant to various authorities applicable to foreign intelligence surveillance conducted abroad." Gov't Br. at 62 n.48 (emphasis added). The government's logic is circular, and it risks allowing the fact of the government's lawful surveillance of non-U.S. persons abroad to seep into and erode the rights of United States citizens.

terminates upon delivery." (internal quotation marks omitted)). But the loss of the privacy interest in that setting typically flows from the recipient's provision of the communication to the government.[18] This case, of course, concerns government *interception* of emails. Nonetheless, given that the emails here had in fact been sent to a third party, I conclude that Hasbajrami had a diminished—if not nonexistent—expectation of privacy in those communications.

c. *Section 702's Safeguards and Procedures Sufficiently Protect Non-Targeted U.S. Persons' Privacy Interests*

As part of my inquiry into the reasonableness of searches conducted pursuant to Section 702, I also consider the safeguards the government has employed to help protect Hasbajrami's privacy interest and to ensure that 702 surveillance is appropriately targeted at non-U.S. persons located outside the United States. Section 702 itself requires these safeguards. The government's Section 702 applications in this case included the required certifications by Executive Branch officials—the DNI and the Attorney General—that detailed the targeting and minimization procedures used to protect the privacy of U.S. and non-U.S. persons located in the United States. Gov't Cl. Br. at 49-52; 50 U.S.C. §§ 1881a(a), (g), and (i). Upon review, the FISC approved the certifications, finding that they contained the elements required by Section 702, and that the targeting and minimization procedures were consistent with the Fourth Amendment. 50 U.S.C. §§ 1881a(i)(3)(A). The Attorney General and the DNI must also periodically review the government's compliance with the minimization and targeting

[18] *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 443 (1976) ("The [bank] depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."); *Hoffa v. United States*, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) ("[T]he maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others.").

procedures and submit assessments to the FISC and congressional oversight committees. *See* 50 U.S.C. 1881a(l).[19]

The oversight provisions of the FAA require the government to regularly report instances of non-compliance to the FISC, which can withhold approval of proposed minimization procedures or require the government to amend them to ensure that they are reasonably designed to limit the acquisition, retention, and dissemination of information concerning U.S. persons. *See* PCLOB Report at 76 (citing FISC Rule of Proc. 13(b)). The oversight provided by the FISC, the executive branch, and Congress work to safeguard Fourth Amendment protections, lending further support to the reasonableness of Section 702 surveillance. *Cf. Mohamud*, 2014 WL 2866749, at *24 (finding that Section 702's requirements for minimization procedures contribute to the statute's reasonableness); *In re Directives*, 551 F.3d at 1013 (relying on a "matrix of safeguards"—including targeting and minimization procedures and a procedure to ensure that a significant purpose of the surveillance is to obtain foreign intelligence information—in determining that the PAA was reasonable under the Fourth Amendment).

The most significant of these safeguards are the government's targeting and minimization procedures. *See, e.g.*, *In re Directives*, 551 F.3d at 1015 (minimization procedures "serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons"). The government did not target "entire geographical areas," as the defendant contends, *see* Def. Br. at 23, but instead used FISC-approved targeting procedures to target specific non-U.S. persons

[redacted]

[19] In four years of oversight, the Senate Select Committee on Intelligence did not find "a single case in which a government official engaged in a willful effort to circumvent or violate the law." S. Rep. No. 112-174, at 7 (2012).

[redacted] Gov't Cl. Br. at 107-111. "Strong" selectors, such as email addresses, weed out innocent or inadvertent communications "[b]ecause of the small set of people with knowledge of the email address or phone number of a subject of foreign intelligence interest." Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection after Snowden*, 66 Hastings L. J. 1, 47 (Dec. 2014) (citing PCLOB Report at 32-33). Such was the case here: the government collected emails to or from unique email addresses because it reasonably believed the owners of those email addresses were non-U.S. persons outside the United States, and that the collection would lead to the acquisition of foreign intelligence information. This cannot be characterized as an unreasonably broad form of interception. To the contrary, these FISC-approved targeting procedures were employed—and worked—exactly as they were intended to.

The government's use of the minimization procedures described above also helped limit the acquisition, retention, and dissemination of information concerning U.S. persons under Section 702, further supporting the reasonableness of the acquisition here.[20] *See Mohamud*, 2014 WL 2866749, at *24 (Section 702's minimization procedures ameliorate Fourth Amendment concerns because they limit "the retention and dissemination of foreign communications of or concerning United States persons" and they require "the identity of the United States Person" to be deleted "in any dissemination of the information unless certain requirements are met"); *see also In re Directives*, 551 F.3d at 1015 (it is "significant" that the

[20] That the government is able to query information obtained under the PRISM program, *i.e.*, lawfully-obtained communications that were to or from legitimate targets, does not render the minimization procedures inadequate, as *amici* contend. *See Amici* Br. at 21-22. Here, once the government learned that the target was potentially an agent of a foreign power, the government sought orders from the FISC for electronic surveillance and physical searches pursuant to Title I and Title III of FISA targeting an agent of a foreign power. Gov't Cl. Br. at 119-20 n.149. I agree with the government that "[i]t would be perverse to authorize the unrestricted review of lawfully collected information but then [] restrict the targeted review of the same information in response to tailored inquiries." Gov't Br. at 71-72.

minimization procedures help prevent identification errors and reduce the impact of incidental interceptions of non-targeted U.S. persons under the PAA).

Moreover, before approving the surveillance, the FISC found that the targeting and minimization procedures in the government's Section 702 applications were consistent with and reasonable under the Fourth Amendment. Specifically, when balancing the government's national security interests against Fourth Amendment interests, the FISC concluded that the surveillance was reasonable in light of the government's important national security interests and the safeguards contained within the targeting and minimization procedures. All of these procedures help limit the scope of Section 702 surveillance, and thus support the reasonableness of that surveillance under the Fourth Amendment.

In evaluating the totality of the circumstances and weighing the government's interest in national security with Hasbajrami's diminished privacy interest, the government's interest outweighs the intrusion. The stringent safeguards embodied in the FAA, *i.e.*, its targeting and minimization procedures, ensured that only the communications of non-U.S. persons abroad were collected. And the targeting that took place in this case was as particular as it gets—the FISC approved the targeting of specific non-U.S. persons outside the United States for specific counterterrorism purposes. The incidental interception of Hasbajrami's emails as a consequence of that lawful surveillance does not alter the reasonableness of the interception.

D. *The Traditional FISA Information Was Lawfully Acquired Because It Was Obtained Pursuant to a Warrant Based on Probable Cause*

"FISA warrant applications are subject to minimal scrutiny by the courts, both upon initial presentation and subsequent challenge." *Abu-Jihaad*, 630 F.3d at 130 (internal quotation marks omitted). In the FISC's initial review, the FISA Judge must "(1) [] find probable cause to believe that the target of the requested surveillance is an agent of a foreign

power; (2) [] find that the application is complete and in proper form; and (3) when the target is a United States person, [] find that the certifications are not 'clearly erroneous.'" *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984).

As in *Abu-Jihaad*, I find that "the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review" than the deferential one that I must apply. 630 F.3d at 130. I have conducted a careful *ex parte* examination and agree that the certifications here were made in accordance with FISA's requirements and the targeting of an agent of a foreign power was not "clearly erroneous." *See id.* The certifications explained that a significant purpose of the FISA surveillance was to obtain foreign intelligence information[21] that could not be reasonably obtained through regular investigative techniques.

I have also examined the application materials and find that they meet the showing of probable cause required by FISA. *See* 50 U.S.C. § 1805(a)(2). The government's submissions here were "quite detailed and complete; they described at length the facts supporting the Government's assertion that there was probable cause to believe that the target of the FISA surveillance was an agent of a foreign power and . . . that a significant purpose of the surveillance was to gather foreign intelligence information." *Abu-Jihaad*, 531 F. Supp. 2d at 313.

Specifically, the government obtained—pursuant to Section 702 surveillance—many email communications between Hasbajrami and non-U.S. persons reasonably believed to be located outside the United States who were [redacted] Gov't Cl.

---

[21] Indeed, the certifications stated that the primary purpose of the surveillance of physical search was "'**not** to obtain information for the prosecution of crimes other than those [international terrorism and foreign intelligence crimes] referred to in [FISA] . . . or related to such foreign intelligence crimes.'" Gov't Cl. Br. at 193 (quoting the certifications at issue) (emphasis in original).

Br. at 3. The government described these emails in its Title I and Title III FISA applications targeting an agent of a foreign power, and they supported the FISC's finding of probable cause that the target was an agent of a foreign power. *See* 18 U.S.C. § 1805(a)(2)(A). In addition, I find that the "[t]he target is described with particularity, as is the basis for believing that the facilities at which electronic surveillance would occur was being used, or about to be used, by the target and that the premises or property to be searched contained foreign intelligence information that was owned, used, possessed by, or in transit to or from the target." *Abu-Jihaad*, 531 F. Supp. 2d at 313. The exhaustive submissions I have received in connection with the application provided ample support for my finding that the government met its probable cause requirement.

Lastly, the FISA collection of Hasbajrami's communications adhered to the approved minimization procedures. The test of compliance in the context of FISA surveillance is "whether [the government attempted] a good faith effort to minimize" the interception of innocent conversations. *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135 (D. Mass. 2007) (quoting *United States v. Armocida*, 515 F.2d 29, 44 (3d Cir. 1975)). The government made that effort here. In addition to numerous other steps, only authorized personnel were able to review the information acquired, and the identities of U.S. persons were minimized before the communications were disseminated by the FBI to other agencies. Gov't. Cl. Br. at 202-04.

Based on this information, the government lawfully conducted the FISA surveillance at issue. The government properly made the required certifications and followed the minimization procedures, and the applications established probable cause. As such, the FISA evidence need not be suppressed.

E. *The Motion for Discovery of FISA and 702 Materials*

Hasbajrami moved for discovery of the classified materials relating to the Section 702 and FISA authorizations and collection. Def. Br. at 66-99. A court may disclose to a defendant "under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). But where a 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.* § 1806(f). With these statutory guidelines in mind, the Second Circuit concluded that disclosure of FISA materials "is the exception and *ex parte*, *in camera* determination is the rule." *United States v. Stewart*, 590 F.3d 102, 129 (2d Cir. 2010). The same *ex parte*, *in camera* procedure applies to discovery motions related to Section 702. *See* 50 U.S.C. § 1881e(a).

After careful review of the FISA and Section 702 materials here it is clear to me that disclosure was unnecessary here. "It is of course true that the legality of the surveillance and search would be better tested through the adversarial process," *Mubayyid*, 521 F. Supp. 2d at 130, but the statute asks me to determine what is *necessary* to accurately determine whether the government complied with the law. 50 U.S.C. § 1806(f). My review of the materials was "relatively straightforward and not complex[,]" and I was able to evaluate the legality of the challenged surveillance without concluding that due process first warranted disclosure. *Abu-Jihaad*, 630 F.3d at 129 (quoting *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310-11 (D. Conn. 2008)). Specifically, the foreign intelligence information obtained pursuant to the FISA and FAA surveillance and searches was lawfully acquired because the collection of foreign

intelligence pursuant to Section 702's PRISM program complies with the Fourth Amendment, and because the government complied with the relevant statutory directives. Given this determination, disclosure of the materials to the defendant is unnecessary.

CONCLUSION

The incidental collection of Hasbajrami's communications with non-U.S. persons abroad—lawfully targeted under Section 702—did not require a warrant and was reasonable in light of the Fourth Amendment's protections. For that reason, Hasbajrami's motion to suppress the evidence obtained from the Section 702 surveillance, along with its fruits, was denied. Further, I find that the government lawfully acquired the traditional FISA information, because it was obtained based upon probable cause and in compliance with the statute's requirements. Finally, because the government legally obtained the surveillance at issue, I deny Hasbajrami's motion for discovery of classified materials.

Dated: February 18, 2016
Brooklyn, New York