IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. JAMSHID MUHTOROV,
2. BAKHTIYOR JUMAEV,

Defendants.

ORDER DENYING MOTION TO SUPPRESS EVIDENCE OBTAINED OR DERIVED UNDER FISA AMENDMENTS ACT OR FOR DISCOVERY (Doc. 520)

Kane, J.

Jamshid Muhtorov, together with his co-defendant Bakhtiyor Jumaev, is charged with providing material support to a designated terrorist organization, and attempt and conspiracy to do the same. His arrest on a one-way flight to Turkey was originally believed to be solely the result of warrantless surveillance and physical searches authorized under Title I and III of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801-1811, 1821-1829. Mr. Muhtorov moved to suppress that FISA-acquired evidence earlier in these proceedings, which motion I denied based on a determination, after an extensive *in camera* review of the classified materials submitted to the FISA Court, that there was probable cause to believe the target was an agent as described and

therefore lawfully subject to those searches.

The matter is before me on a renewed Motion to Suppress, precipitated by the government's supplemental disclosure, nearly two years after Mr. Muhtorov's arrest, that some of the FISA-acquired evidence it intends to use against him in this case was derived from surveillance conducted under § 702 of the FISA Amendments Act of 2008 ("FAA").[1] Section 702, codified at 50 U.S.C. § 1881a, establishes procedures for the warrantless surveillance of targeted persons overseas "to acquire foreign intelligence information." Because communications to and from a target under § 702 are swept up without reference to who is sending them and without any determination of probable cause, the FAA results in the "incidental" interception, collection, and retention of communications from unconsenting U.S. persons including, in this case, Mr. Muhtorov.

Judicial review of § 702 authorizations is narrow, and until the Snowden leaks in 2013, the American public was led to believe that the government did not query or use FAA-acquired surveillance against non-targeted U.S. persons. *See Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138 (2013). The belated notice in this case was part of the Snowden fallout and the revelation, post-*Clapper*, that the Executive Branch does, in fact, use FAA-acquired information to investigate U.S. persons for suspected criminal activity, and that it intends to use it against Mr. Muhtorov here.

[1] The FAA added Title VII to the FISA statute, which establishes "Additional [intelligence gathering] Procedures Regarding Certain Persons Outside the United States." It is intended to sunset on December 31, 2017. *See* P.L. 110-261, § 403(b)(1), 122 Stat. 2474, as amended, appearing in 50 U.S.C. § 1881 note.

In his renewed Motion, Mr. Muhtorov moves to suppress all of the FAA-acquired evidence in this case and the "fruits thereof" on grounds that § 702's authorization and implementation procedures permit the government to collect and retain the communications of U.S. persons without a warrant and without probable cause in violation of the Fourth Amendment. Alternatively, as an "aggrieved person" entitled to challenge the lawfulness of the acquisitions directly under § 702, he argues the statute was unlawfully applied to him and seeks discovery into the means and methods of the government's FAA surveillance in this case to substantiate that claim. With the entry of the ACLU as co-counsel for the defense, briefing has emphasized the former, with Mr. Muhtorov serving as the *Clapper*-qualified[2] successor to the plaintiffs in that case, who were deemed insufficiently "harmed" by § 702's surveillance procedures to have standing to pursue a Fourth Amendment challenge. I find the *Clapper* argument attenuated by Mr. Muhtorov's status as a criminal defendant – rather than an incidental interceptee generally – and that his privacy-related *Clapper* claim is transformed by that fact. As a U.S. person and a criminal defendant, Mr. Muhtorov is entitled to the full panoply of statutory and constitutional protections afforded under § 702 and the U.S. Constitution. As a criminal defendant whose communications were captured pursuant to FISA Title I and III

[2] In *Clapper v. Amnesty Int'l USA*, __ U.S. __, 133 S. Ct. 1138 (2013), Justice Alito writing for a majority of the Supreme Court held that attorneys, human rights, and media organizations lacked article III standing to challenge the constitutionality of § 702 because they could only speculate that their communications had been or would be incidently acquired during FAA surveillance of their clients or other targeted persons abroad. With the government's notice in this case, the acquisition of Mr. Muhtorov's communications is demonstrable and he is therefore "*Clapper*-qualified" to challenge the law.

surveillance targeting an agent of a foreign power, however, these protections are counteracted to a significant extent by FISA and prerogatives long recognized in U.S. law regarding the Executive's primacy in the arena of foreign affairs and national security.

My concern as a trial court judge is with the individual criminal defendants before me and their rights to due process and a fair trial. The constitutional question at issue is one the Executive and courts have wrestled with since the Supreme Court's acknowledgment in the 1972 *Keith*[3] case of the dilemma invited when warrantless national security intelligence surveillance uncovers evidence of crime. The question here is where – on the continuum between the largely unfettered authority the government enjoys in national security matters and foreign intelligence surveillance on the one hand, and its constitutionally limited authority to investigate its citizens for crimes – stands Mr. Muhtorov.[4] It is a particularized inquiry of the most solemn kind. While I am convinced the FAA is susceptible to unconstitutional application as an end-run around the Wiretap Act and the Fourth Amendment's prohibition against warrantless or unreasonable

---

[3] *United States v. United States Dist. Court for the Eastern Dist. of Mich.*, 407 U.S. 297 (1972)(known as the *Keith* case).

[4] I note Mr. Jumaev has filed his own renewed Motion to Suppress and/or for Discovery (Doc. 521), insisting that FAA must have informed the government's investigation and indictment of him notwithstanding the government's disclaimer and the fact that it filed no Notice of Intent to Use FAA-Acquired information against him in this case. Based on the government's representations that it does not intend to use FAA-acquired evidence against him and my *ex parte* review of all of the classified information in this case, I conclude Mr. Jumaev is not an "aggrieved person" authorized under 50 U.S.C. § 1806(e) to move to suppress such evidence or to bring an as-applied constitutional challenge to Section 702. The question of whether the disclaimer deprives Mr. Jumaev of standing to assert a facial challenge to the FAA under *Clapper* is an open one, in my view, but one, given my ruling in this case, that does not need to be answered. I limit my analysis in this opinion to the constitutional arguments raised by Mr. Muhtorov.

searches, I am equally convinced that it was not unconstitutionally applied to Mr. Muhtorov. Based on my *in camera* review of the classified and unclassified documents made available to me, the FAA surveillance at issue was narrowly tailored to the government's foreign intelligence-gathering prerogatives. Because I find Section 702 to have been constitutionally applied in this case, the facial challenge to the FAA must be denied. I will address Mr. Muhtorov's request for specific, additional discovery and declassification in a separate order, after conducting one or more prefatory CIPA § 4 hearings on the subject.[5]

I.

BACKGROUND AND PROCEDURAL HISTORY.

Jamshid Muhtorov was born in Jizzak, Uzbekistan, when that country was still under communist rule. He is the oldest of five children. After graduating from a technical university, Mr. Muhtorov was offered a position with the Ezgulik Human Rights Society in Uzbekistan, becoming the head of the Jizzak branch in 2003.

During the course of his work with Human Rights Watch, foreign embassies and NGOs, Muhtorov came under the increasing scrutiny of Islam Karimov, the last president

[5] Section 4 of the Classified Information Procedures Act (CIPA) provides that "[t]he court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove." I have, to date, accepted the government's averred classification assertions as offered. Through the upcoming § 4 process, I intend to put the government through its paces to justify them, and to urge the declassification that was promised for much of the Muhtorov and Jumaev-related discovery in this case.

of Soviet Uzbekistan who became and remains the first president of independent Uzbekistan. This scrutiny intensified in May 2005, and in 2006, according to Human Rights Watch, Mr. Muhtorov was himself threatened and beaten. With the help of other activists, Mr. Muhtorov fled to Kyrgystan, and then, with his wife and children to the United States.

Mr. Muhtorov and his family were admitted to the United States as political refugees in February 2007. They settled in Colorado. Mr. Muhtorov has no criminal record and, until his arrest in January of 2012, had never been arrested. He is a legal permanent resident of the United States.[6]

The operative Second Superseding Indictment (Doc. 59) charges Mr. Muhtorov with two counts of providing and attempting to provide material support and resources to the Islamic Jihad Union (IJU), and Muhtorov and Jumaev with one count of conspiring to commit that offense, in violation of 18 U.S.C. § 2339B. If convicted, each faces a maximum term of imprisonment of 15 years.

The allegations in the indictment were initially attributed to information gleaned in investigations of Mr. Muhtorov's computer, email accounts, private residence, and personal effects. *See* Criminal Compl. (Doc. 1)(and attached Affid. of FBI Special Agent Hale). When the government formally notified Mr. Muhtorov that it intended to use FISA-acquired information against him in the proceedings (Doc. 12), Mr. Muhtorov

[6] *See* 50 U.S.C. § 1801(i)(defining "United States person" as, among other things, "a citizen of the United States" or "an alien lawfully admitted for permanent residence").

exercised his right as an "aggrieved person" under the statute and moved to suppress. (Docs. 14, 125). I denied that Motion in a written Order issued September 24, 2012 (Doc. 196), applying the standards set forth at 50 U.S.C. § 1806(e) & (f) and finding the surveillance and physical searches at issue were lawfully authorized and conducted. I specifically concluded that the attested facts submitted to the FISA Court supported a finding of probable cause to believe the target was an "agent[] of a foreign power," and concluded that the FISA application and related materials should not, in the interest of national security, be disclosed. *Id.* p. 3. I denied Mr. Jumaev's related Motion on the same basis.

On October 25, 2013, the government filed a Second Notice of Intent to Use FISA-acquired Information (Doc. 457), formally notifying Mr. Muhtorov of its intent to use information obtained or derived from the acquisition of foreign intelligence information under the Foreign Intelligence Surveillance Act of 1978, "as amended," and citing 50 U.S.C. § 1881a. Given its timing in the Snowden-*Clapper* aftermath, the Notice was clearly intended to notify Mr. Muhtorov that he was a member of the previously undisclosed class of U.S. persons whose international communications had been monitored and acquired incidently to surveillance conducted under § 702 of the FAA. Viewing the affidavit informing the publicly available Complaint in this case in that light, it is clear that FAA surveillance overseas resulted in the acquisition of communications later traced to Muhtorov. *See* Affid. of FBI Agent Hale (attached as Ex. A to Complaint (Doc. 1)). What was acquired and over what period of time is classified information that

has not yet been shared with the defense.

Foreign Intelligence Gathering and FISA.

Presidents since FDR have claimed an inherent constitutional authority to conduct electronic surveillance in national security matters without prior judicial approval. The authority is grounded in Article II of the Constitution, which charges the Executive to "preserve, protect and defend the Constitution of the United States." This authority was accorded great deference for many years, until that began to change in the early 1970s.[7]

In 1972, the Supreme Court took up the question in *United States v. United States District Court* (*Keith)*, 407 U.S. 297 (1972), a case involving the bombing of a CIA building and the warrantless surveillance that led to the indictment of the U.S. persons involved. Justice Powell, writing for the majority, rejected the government's assertion of a blanket national security exception to the Fourth Amendment's warrant requirement as codified in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), concluding the government's concerns did not justify a departure from the customary Fourth Amendment requirement of judicial pre-approval under the circumstances presented.[8] *Id.* at 323-24. The Court expressly refused, however, to "judge[] the scope of the President's surveillance power with respect to the activities of

---

[7] *See* Fiss, O., "Even in a Time of Terror," 31 Yale Law & Policy Rev. 1 (2012).

[8] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act") governs domestic electronic surveillance activities and requires federal, state, and other officials to obtain judicial approval on a specific showing of probable cause before intercepting "wire, oral, and electronic" communications such as telephone conversations and e-mails.

foreign powers, within or without [the U.S.]," *id.* at 308, leaving that question open. The Court further recognized potential distinctions between national security surveillance and "surveillance of 'ordinary crime,'" and invited Congress to consider protective standards for the former different from those prescribed in Title III that took these distinctions into account. *Id.* at 322-23. "Different standards," the Court acknowledged, "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." *Id.* at 323.

The Watergate scandal in 1974 thrust the Executive's use of electronic surveillance into the public eye. Revelations during several Senate Committee hearings revealed a host of warrantless privacy infringements of U.S. citizens in the name of national security, including wiretapping of congressional staffers, anti-war protesters, and civil rights activists including Dr. Martin Luther King. After fourteen Senate Reports and significant debate, Congress enacted the Foreign Intelligence Surveillance Act "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes." *See* S. Rep. 95-604, p. 7 (1977). President Carter signed it shortly thereafter. 92 Stat. 1783, 50 U.S.C. § 1801 *et seq.*

In constructing a framework for foreign intelligence surveillance that balanced the Executive's foreign intelligence and security prerogatives with Americans' privacy interests, Congress defined "electronic surveillance" narrowly to include only foreign

intelligence collection activities that impacted U.S. persons or took place on U.S. soil,[9] and prohibited anyone from engaging in "electronic surveillance under color of law *except* as authorized by this Act." 50 U.S.C. § 1809(a)(emphasis mine). Congress then created two specialized foreign intelligence courts – the FISA Court (FISC) and the FISA Court of Review (FISR) – that would approve and review the approval of "electronic surveillance" under the Act. 50 U.S.C. § 1803(a) & (b), *discussed* in *Clapper*, 133 S. Ct. at 1143. Surveillance authorization would be given if there was "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and 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"; and if minimization procedures are in place that meet with FISC approval under the standards articulated in the statute. *See* 50 U.S.C. § 1805(a). As will be

---

[9] *See* 50 U.S.C. § 1801(f)(1)-(4)(§ 1801(f)(1)-(4)(defining "electronic surveillance" in terms of wire or radio communications targeting a person "in," acquired "in," or intended for or received by someone "in," the "United States"). Given that international communications in 1978 were carried through satellite signals or over transoceanic cables subject to interception offshore, Congress understood this language would exempt NSA's foreign-to-foreign as well as most of its international communications surveillance from regulation, because neither would fall within the definition of "electronic surveillance" under the Act:

> "The language of this amendment exempts . . . foreign intelligence gathering . . . . if the acquisition does not come within the definition of 'electronic surveillance'. . . . Specifically this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

See United States v. Mohamud, Crim., Case No. 10-cr-475-KI, *slip op.* at p. 12, 2014 WL 2866749 (D. Or. June 24, 2014)(quoting S. Rep. No. 95-701, at 71 (1978)).

discussed in more detail below, "minimization procedures" serve as the principle means of protecting the Fourth Amendment privacy interests of U.S. persons whose communications are caught up in foreign intelligence surveillance under FISA.[10]

Expansion of FISA Authority.

Almost as soon as it was enacted, pressure began to build to clarify and expand the Executive's foreign surveillance authority under the FISA statute. Increasing terrorist activity raised the stakes[11] and changes in communications technology brought intelligence surveillance intended to remain outside FISA's purview within its definition of domestic surveillance and thus subject to FISA Court review and regulation.[12]

In 1981, President Reagan issued Executive Order 12333, reaffirming the Executive's inherent authority to conduct covert operations and collect information on

---

[10] "Minimization procedures" under FISA are defined as "specific procedures . . . adopted by the Attorney General, that are 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).

[11] The 1979 seizure of the U.S. embassy in Tehran; a series of Libyan and Hezbollah bombings, attacks and hostage taking beginning in 1982 and continuing throughout the 80s and early 90s, including the 1988 bombing of a Pan-Am flight over Lockerbie, Scotland, in 1988; the 1993 World Trade Center bombing in New York; and the Oklahoma City bombing in 1995 are but a few examples.

[12] The advent of the internet, for example, meant that foreign communications previously transmitted via satellite or transoceanic cables in 1978 were now carried over fiber optic cables. Because these cables were arguably "wires," foreign surveillance that would have been excluded from FISA regulation in 1978 was rendered potentially unlawful due merely to a change in technology, rather than any intentional decision by Congress. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Sel. Comm. on Intel.*, 110th th Cong., 1st Sess. (2007) at pp. 9-19 (testimony of the Director of National Intelligence).

"foreign powers, organizations, persons, and their agents" without reference to FISA, and specifically authorizing "elements of the intelligence community . . . to collect retain, or disseminate information concerning United States persons." EO 12333, Parts 2.2, 2.3.[13] In 1995 and 1998, Congress amended FISA directly, first to include physical searches, 50 U.S.C. §§ 1821-29, and then the installation and use of pen register and trap and trace devices, §§ 1841-46, "for foreign intelligence purposes."

Then in 2001, foreign terrorists carried out the coordinated 9/11 attacks on New York City and the Pentagon, killing nearly 3,000 people on American soil. Within weeks, both President George W. Bush and Congress had acted to expand Executive surveillance authority and facilitate more effective coordination between the intelligence community and federal law enforcement agencies. In October 2001, Congress passed the USA PATRIOT ACT,[14] sweeping legislation that modified multiple existing laws and enhanced the government's law enforcement authority as it related to investigating and prosecuting terrorism.[15] Among other things, the PATRIOT ACT revised FISA § 104's

---

[13] EO 12333's complete text appears at 46 Fed. Reg. 59941, 3 C.F.R.

[14] United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the "USA PATRIOT ACT), Pub. L. 107-56 (October 26, 2001).

[15] The USA PATRIOT Act not only amended FISA, but also the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Pen Register and Trap and Trace Statute, Money Laundering Act, Immigration and Nationality Act, Money Laundering Control Act, Bank Secrecy Act, Right to Financial Privacy Act, and the Fair Credit Reporting Act all were impacted by USA PATRIOT Act amendments. *See generally,* Congressional Research Service (2002b), "The USA PATRIOT Act: A sketch." [On-line]. Available: http://www.fas.org/irp/crs/RS21203.pdf

"purpose" requirement. Responding to a series of court cases and intelligence agency policies that had erected a "Wall" between foreign intelligence and criminal investigations, the ACT authorizing FISA applications on a certification that foreign intelligence gathering was a "significant," rather than "primary" purpose of the surveillance sought. *Compare* 50 U.S.C. § 1804(a)(6)(B) (2008) *with* 50 U.S.C. § 1804(a)(7)(B) (2000)(change discussed at length in *United States v. Abu-Jihaad*, 630 F.3d 102, 122-23 (2d Cir. 2010)). President Bush, meanwhile, responded to the 9/11 attacks by authorizing the NSA to conduct warrantless wiretapping of telephone and e-mail communications in the United States outside the purview of FISC entirely, as long as one party to a communication was located outside the United States and a participant in "the call was reasonably believed to be a member or agent of Qaeda or an affiliated terrorist organization." *See Clapper*, 133 S. Ct. at 1143-44. Until 2005, neither the public nor most members of Congress were aware the President's Terrorist Surveillance Program (TSP) existed.

President Bush's confirmation in December 2005 that the NSA had been conducting warrantless electronic surveillance of U.S. persons without even FISA Court approval prompted Congress, once again, to conduct a "vigorous inquiry" into the Executive's secret surveillance activities. *See* S. Rep. No. 110-209, 1st Sess. 1 (2007). With all parties in agreement that FISA required updating, Congress set to work. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the H.*

Permanent Select Comm. on Intel., 109th Cong., 2d Sess. (2006).[16]

The PAA and Elimination of the "Foreign Agent" Probable Cause Requirment

As a result of these efforts, Congress enacted the Protect America Act ("PAA") in August 2007, a temporary measure that brought the Executive's TSP authority into the FISA fold. Codified at 50 U.S.C. § 1805a, b & c, the PAA permitted the Director of National Intelligence and the Attorney General to authorize the acquisition of foreign intelligence information "concerning persons reasonably believed to be located outside the United State" without reference to their status as foreign agents, limited solely by the establishment of targeting and minimization procedures to "preserve the privacy interests

---

[16] During hearings, Congress heard testimony on the ways the advancement of communications technology since 1978 had created unforeseen consequences under FISA. Transmission over an integrated global communications grid blurred the distinction between domestic and offshore acquisition. Domestic communications between neighbors in Peoria could travel around the world and be intercepted abroad. Foreign-to-foreign communications that were previously beyond FISA's reach could be intercepted in the United States.

> [As a communication travels the global network,] NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science . . . . Intercept of a particular communication . . . is always probabilistic, not deterministic [and] [n] o coverage is guaranteed.

FISA for the 21st Century: Hg. before the S. Comm. on the Judiciary, 109th Cong., 2d Sess. (2006)(statement of NSA Director General Michael V. Hayden). The necessary fix, Congress was told, was a "technology-neutral" framework for surveillance of foreign targets – focused not on "how a communication travels or where it is intercepted," but on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes." *FISA Modernization Hg.* at 46 (statement of Asst. Atty Gen. Kenneth L. Wainstein). With these changes, it was implied, the original balance between strictly "foreign" foreign intelligence gathering and foreign intelligence gathering that impacted Americans struck by FISA in 1978 could be reconstituted, and secret programs like TSP could be brought to light and integrated into the FISA framework.

of persons in the United States." S. Rep. No. 209, 110th Cong. 1st Sess. at 5-6. The PAA was revised and incorporated into FISA by the FISA Amendments Act of 2008, becoming § 702 of a new FISATitle VII.

Section 702, like the PAA before it, authorizes the Attorney General and the Director of National Intelligence to authorize jointly, "for a period of up to 1 year," the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Like the PAA, § 702 permits the government to intercept all communications to and from the target, including those of U.S. persons, without demonstrating probable cause that either is a foreign power or the agent of a foreign power, and without identifying the facilities or places where the electronic surveillance will occur. FAA procedure simply requires the Attorney General, in consultation with the Director of National Intelligence, to select a target and adopt guidelines the Attorney General certifies will "ensure" compliance with appropriate targeting and minimization procedures, as well as the limitations on § 702 surveillance authority set forth in § 1881a(b). *See* § 1881a(f)&(g). If the FISC finds the AG's certifications, targeting, and minimization procedures are "consistent with [the FAA's requirements] and with the fourth amendment to the Constitution of the United States," it "shall" enter an order approving the certification and use of the procedures for the acquisition. 50 U.S.C. § 1881a(i).

Section 702's limitations are significant, but largely conclusory and "riddled with loopholes." An acquisition under § 702(a) may not "intentionally" target a person

"known" at the time of acquisition to be located in the United States (§ 1881a(b)(1)), or "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." § 1881a(b)(2). Also, acquisitions must be "conducted in a manner consistent with the fourth amendment to the Constitution." § 1881a(b)(5). But the government is the sole arbiter of its "knowledge," "intent," "purposes," and "conduct."[17] The government can continue "incidently" acquiring a person's communications under § 702 even after such reveals evidence of a crime, as long as the government avoids learning that the person is a U.S. person or located in the United States. It can avoid seeking Title I or Title III authority to target the person directly by simply declining to call that person a "target." It can say it is "conducting" this surveillance consistently with the fourth amendment, but § 702 provides no mechanism for FISC to assess whether that is the case. For an excellent discussion of the FAA's weaknesses and prescriptions for remedying them, *see* T. Anderson, "Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act," 8 Harv. Law & Policy Rev. 413 (Summer 2014).

[17] Compliance with § 702(b) limitations and with the Attorney General's proffered targeting and minimization procedures is self-monitored and self-executing under the FAA, as judicial review is limited to the initial authorization and any reauthorizations sought by amendment. *See* § 1881a(i). The FAA requires that the Attorney General and Director of National Intelligence conduct a "semi-annual assessment" of compliance with the targeting and minimization procedures of a particular surveillance authorization, § 1881a(l), but other than submitting that assessment to FISC and to congressional intelligence and judiciary committees, the FAA requires no action on the assessment and no judicial review on the part of FISC.

FISA and Law Enforcement.

Our concern in this case, of course, is the confluence of FISA and law enforcement, i.e., what happens when FISA surveillance results in the acquisition of evidence of a crime. It is clear that FISA surveillance is more than simply foreign intelligence gathering, and that its purpose since its inception has been the discovery and investigation of foreign intelligence crimes. *See In re Sealed Case*, 310 F.3d 717, 725 (Foreign Int. Surv. Ct. Rev. 2002). U.S. persons may be authorized targets, and surveillance may be part of an investigative process designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of foreign powers. *Id.* (quoting S. Rep. No. 95-701, at 10-11 (1978)). The question has always been where these two functions merge, i.e., where FISA-acquired electronic surveillance information, which is acquired *without* a warrant under the Wiretap Act, is used against an U.S. person who would otherwise enjoy the protections of that Act.

Before the enactment of the FAA, case law developed permitting the use of FISA-acquired evidence against U.S. persons in criminal prosecutions as long as there was probable cause to believe those persons were "foreign powers" or "agents of a foreign power" (50 U.S.C. § 1805(a)(2)) and the surveillance was properly conducted "to acquire foreign intelligence information." 50 U.S.C. § 1802(a)(1). *E.g. United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1988)(as long as the purpose of FISA surveillance is foreign intelligence gathering, that purpose is not

changed merely because government anticipates using fruits of FISA surveillance in criminal prosecution). The purpose of the surveillance cannot be a ruse. *See United States v. Johnson*, 952 F.2d 656, 572 (1st Cir. 1991), *cert. denied*, 506 U.S. 816 (1992)(government cannot use FISA as an "end-run around the Fourth Amendment's prohibition of warrantless searches" by drumming up a foreign intelligence purpose for ordinary criminal investigation); *United States v. Troung Dinh Hung*, 629 F.2d 908, 916 (4th Cir. 1980)(targets must "receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution.") But unless surveillance is conducted "solely" for law enforcement purposes, the Fourth Amendment under *Keith* is flexible enough to justify the use of FISA-acquired evidence in criminal prosecutions even without a Title III warrant. *See U.S. v. Duka*, 671 F.3d 329, 345 (3d Cir. 2011)(evidence derived from a reasonable search is admissible in a criminal trial); *Abu-Jihaad*, 630 F.3d at 12 (Fourth Amendment does not require the government to identify a primary purpose or limit its ability to secure a warrant to satisfaction of the standards for that purpose; rather, the government may secure a warrant under the probable cause standards applicable to any purpose that it pursues in good faith).

Under the FAA, § 702 does away with the § 105's probable cause requirement, permitting the government to target persons based solely on their physical presence outside the United States, and to intercept communications to and from those persons, as long as the surveillance was conducted "to acquire foreign intelligence information." § 1881a(a). Mr. Muhtorov contends this change distinguishes the case law allowing the

use of FISA-acquired evidence in criminal prosecutions, and renders the use of FAA-acquisitions against U.S. persons in criminal prosecutions unconstitutional.

II.

DISCUSSION.

Mr. Muhtorov contends the fruits of the government's § 702 surveillance must be suppressed because the statute that authorized the surveillance is unconstitutional. He argues the FAA violates the Fourth Amendment by authorizing surveillance that contravenes the warrant clause and, independently, surveillance that is unreasonable. He also argues the FAA violates Article III by requiring judges to issue advisory opinions in the absence of a case or controversy, citing my opinion in *United States v. Smith*[18] in support.

The FAA and Article III's Case or Controversy Requirement

I pause briefly to address Mr. Muhtorov's assertion that the FAA is unconstitutional because it violates Article III's "case or controversy" requirement. His argument is novel and elegant, but I will not be the first to adopt it. Plainly stated, Muhtorov argues the FAA assigns to the FISA Court a role "fundamentally incompatible with the case-or-controversy requirement" because it compels FISC to "evaluate in a vacuum whether proposed targeting and minimization procedures comply with the statute

[18] *United States v. Smith*, 686 F. Supp. 847 (D. Colo. 1988)(declaring Sentencing Reform Act of 1986 unconstitutional, in part, because role played by Article III judges on Sentencing Commission violated principles of separation of powers).

and the Constitution" without any particularized facts or context. Mot. (Doc. 520) at 45. The authority he cites for his proposition, however, is either inapposite,[19] or distinguishable,[20] and none applies the concept in the context of the "neutral magistrate" or other arbiter of search authorizations or warrants under the Fourth Amendment.

Mr. Muhtorov's strongest argument is that courts that have rejected Article III challenges to the *traditional* FISA process have done so because the FISC's job is a particularized one – i.e. that under 50 U.S.C. § 1805(a) and (b), FISC considers concrete facts about a specific person to be monitored and the facilities to be targeted. *Citing U.S.*

---

[19] *Flast v. Cohen*, 392 U.S. 83, 97 (1968)(addressing case in controversy requirement in context of standing analysis for taxpayer suit challenging validity of federal spending on textbooks); *Citizens Concerned for Separation of Church & State v. City & Cnty. of Denver*, 628 F.2d 1289, 1295 (10th Cir. 1980)(using case or controversy requirement as source for standing analysis, finding citizens lacked standing to bring First Amendment challenge to City's creche display because there was no showing of causal connection between the creche display and any injury in fact to plaintiff); *In re Summers*, 325 U.S. 227, 241 (1937)(holding that a claim of a present right to admission to state bar association and denial of that right is a case or controversy that may be reviewed under Article III when federal questions are raised). The citation to my opinion in *Smith* is more interesting, because although my ruling there passed on a completely different aspect of the separation of powers doctrine, I observed that article III judges "'[d]ischarging tasks other than the deciding of cases and controversies'" would involve them in the process of policy and thereby "'weaken confidence in the disinterestedness of their judicatory functions.'" 686 F. Supp. at 855 (quoting *In re Sealed Cases*, 838 F.2d 476, 512 (D.C. Cir. 1988). The point is correct, in my view, but not particularly germane. If the concern is that FISC's participation in § 702 authorizations undermines the perceived impartiality or detachment of the judiciary from law enforcement, it is of a kind with concerns over judges participation in secret or *ex parte* proceedings of all types, and wiretap authorizations generally.

[20] *See New York v. Ferber*, 458 U.S. 747, 768 (1982)(addressing the need to focus on "flesh-and-blood" applications of fact to law in context of First Amendment overbreadth challenge to child pornography statute); *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 239 (1937)(construing Declaratory Judgment Act's "actual controversy" requirement in context of Article III's limitation of judicial power to "'cases' and 'controversies,'" holding the term "'controversies,' if distinguishable at all from 'cases,' is so in that it is less comprehensive than the latter, and includes only suits of a civil nature").

v. Megahey, 553 F. Supp. 1180, 1186 (E.D.N.Y. 1982), *aff'd* 729 F.2d 1444 (2d Cir. 1983), *and aff'd on other grounds sub nom. United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984). In *Megahey*, defendants argued that FISC was not constitutionally authorized under Article III because FISA required it to issue orders on an *ex parte* basis without any adversarial proceedings. The district court rejected the argument, stating

> Applications for electronic surveillance submitted to FISC pursuant to FISA involve concrete questions respecting the application of the Act and are in a form such that a judge is capable of acting on them, much as he might otherwise act on an ex parte application for a warrant. In the case of each application, the FISC judge is statutorily obliged to ensure that each statutory prerequisite is met by the application before he may enter a surveillance order. The FISC judge who is faced with a surveillance application is not faced with an abstract issue of law or called upon to issue an advisory opinion, but is, instead, called upon to ensure that the individuals who are targeted do not have their privacy interests invaded, except in compliance with the detailed requirements of the statute.

553 F. Supp. 1180 at 1197.

That the FAA altered this analysis is undeniable. The "concrete questions" and "individual targets" contemplated by traditional FISA authorization requests have been excused in authorization requests under the FAA. Moreover, the "incidental interceptees" with whom we are concerned are nameless, faceless, and transient in the context of § 702 surveillance, and their privacy interests are evaluated solely in the context of the certified targeting and minimization procedures FISC is asked to approve.

The government dismisses this distinction, arguing FAA authorization approval is more similar to traditional FISA approval than different, and constitutionally not unlike other statutory schemes in which courts assess the reasonableness of standards and

procedures for conducting searches or surveillance consistently with Article III. Govt's Unclassified Resp. to Mot. Suppress (Doc. 559) at 79-80 (citing *United States v. Tortorello*, 480 F.2d 764, 772-73 (2d Cir. 1973)(analyzing adequacy of New York statutory procedures for reauthorizing surveillance after original authorization accidently uncovered evidence of crime) and *Camara v. Municipal Court*, 387 U.S. 523, 537-38 (1967)(approving warrantless inspection provision of municipal housing code – standard may be based on passage of time or nature of the building, and not necessarily specific knowledge of particular dwelling)). Accordingly to the government, FISC's job of analyzing the reasonableness of electronic surveillance by weighing national security interests against the privacy interests of potential subjects is a "traditional judicial function," citing *Halperin v. Kissinger*, 606 F.2d 1192, 1201 n.59 (D.C. Cir. 1979), and is not rendered otherwise by the fact that the potential subjects are not identified with particularity.

I do not dismiss the distinction so easily. FISC's job under the FAA is substantively different than it is under traditional FISA and under any of the other examples of "traditional judicial function" the government cites. Under the FAA, incidental interceptees are part of the surveillance contemplated, but no particularized information about them or their communications practices is presented to FISC for consideration. Each of the scenarios cited by the government is different: There would have been no "case or controversy" in *Tortorello* without Arthur Tortorello, and no "case or controversy" in *Camara* without Roland Camara.

FISC's role in approving the surveillance of individual foreign powers or agents under traditional FISA is qualitatively different from its role in approving the surveillance and incidental acquisition of strangers' communications under the FAA. Whether that role offends Article III sufficiently to invalidate § 702 as a tool for gathering foreign intelligence information is one I leave to a higher court.[21] For purposes of the case before me, my judgment is that it does not.

The FAA's Validity Under the Fourth Amendment.

While FISA authorizes the government to conduct relatively narrow surveillance of individuals reasonably believed to be "foreign agents" or "foreign powers," the FAA permits the government to monitor any person, and that person's contacts, without reference to his foreign status or agency. By permitting the government to acquire "essentially any communication that originates or terminates outside the United States,"

[21] I note that during the course of briefing in this case, Judge King in the District of Oregon issued his opinion in *United States v. Mohamud*, 2014 WL 2866749 (2014), upholding the FAA and the government's disclosure that it had used FAA-acquired evidence to secure the conviction of a U.S. person. Defendant's arguments in *Mohamud*, discussed further *infra*, included an Article III challenge similar to Mr. Muhtorov's here. While I agree with several of Judge King's legal conclusions in *Mohamud*, I find his analysis of defendant's "case or controversy" arguments unpersuasive. Judge King spent most of his discussion couching defendant's arguments in terms of a separation of powers challenge, which he contends has been put to rest by *Mistretta v. United States*, 488 U.S. 361 (1989). *Id.* at *10-11. As set forth in n. 19, *supra*, I find the separation of powers analysis inapposite to the "case or controversy" argument raised. Judge King's further discussion equates FISC's role in FAA surveillance authorizations to the "neutral and detached" review conducted by magistrates under the Wiretap Act, citing *Keith*. *Id.* at *11. In so doing, Judge King did not address the fundamental differences between wiretap authorization reviews conducted in criminal cases and traditional FISA on the one hand, and the FAA on the other. As a result, I do not believe *Mohamud* moves the ball forward on this issue.

Mr. Muhtorov contends the FAA violates both the Fourth Amendment's warrant clause and its ban on unreasonable searches and seizures. Mot. Suppress (Doc. 520) at 21.

The Fourth Amendment's Warrant Requirement

The Fourth Amendment 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 places to be searched, and the persons or things to be seized.

The modern Supreme Court has done away with an interpretation of the Fourth Amendment that requires a warrant, a probable cause determination, "'[]or, indeed, any measure of individualized suspicion," in every circumstance, before a search may be lawful. *Mohamud*, 2014 WL 2866749 at *12 (quoting *Nat'l Treasury Emp. Union v. Von Raab*, 489 U.S. 656, 665 (1989)(holding suspicionless drug-testing of certain United States Custom Service employees not unreasonable under the Fourth Amendment)). The warrant requirement does not apply to activities of the United States directed against aliens in a foreign territory, *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990)(search of the Mexican residences of a Mexican citizen), and does not apply to even U.S. persons if the government establishes a defensible "special need" to dispense with it. *See e.g. Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)(exception to Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, makes the warrant and probable-cause requirement impracticable.")).

Courts have combined these concepts to carve out a "foreign intelligence

exception" to the warrant requirement,[22] which Mr. Muhtorov urges me to reject.[23] I find the special need/foreign intelligence exception argument somewhat academic and limiting, because the standard ultimately is one of reasonableness, and it is on that standard that the constitutionality of § 702's warrantless surveillance authorization must be decided. *See Samson v. California*, 547 U.S. 843, 852 n.3 (2006)(declining to address whether California's parole search condition was justified "special need" under *Griffin* because determination that condition was reasonable rendered examination unnecessary).

On its face, § 702 surveillance targets individuals *outside* the United States "to acquire foreign intelligence information." The reasonabless of that targeting, without a warrant, is not the essence of our inquiry. *See In re Directives* [redacted text] *Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (For. Intel. Surv. Ct. Rev. 2008)(Even if a foreign intelligence exception applies in a given case, "governmental action intruding on the individual privacy interest [of U.S. persons] must comport with the Fourth Amendment's reasonableness requirement."). Our concern is with the axiomatic corollary of that targeting, *i.e.*, that U.S. persons' communications with the target are *perforce* acquired as part of that targeted surveillance, and may be used

---

[22] *See Duka*, 671 F.3d at 341 (stating "courts have concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of 'foreign intelligence exception' to the Fourth Amendment's warrant requirement," and collecting cases).

[23] Mot. Suppress (Doc. 520, at 27, 30)(there is no "special needs" exception to the warrant requirement for foreign intelligence and "not basis to conclude" the requirement is unworkable here).

against them in criminal investigations on American soil without any reasonable suspicion or probable cause determination having been made as to *them*.

Reasonableness.

The touchstone of constitutionality under the Fourth Amendment is reasonableness. It is a fluctuating rather than fixed standard. It depends not only on an analysis of the discrete facts incident to a finding of probable cause (and, for that matter, the search and/or seizure itself), but also the intent and purpose of the established laws of the United States. Because the test is one of reasonableness, the panoply of relevant factors must be considered. In the instant case, the charges against Mr. Muhtorov are premised in the constitutional requirement that the Executive has broad powers to protect the United States against foreign threats. What may be unreasonable in a purely domestic matter may, on balance, be considered reasonable in the context of the security of the nation in dealing with foreign powers and organizations that pose a threat. "It must be remembered that what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures." *Elkins v. Unites States*, 364 U.S. 206, 222 (1960).

To analyze whether a government search is reasonable under the Fourth Amendment, the court examines the totality of the circumstances. *Samson v. California*, 547 U.S. 843, 848 (2006). The court weighs "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Maryland v. King*, __ U.S. __, 133 S. Ct. 1958, 1970 (2013)(internal citations and quotations omitted). Under this standard, the modern Supreme Court has approved

statutory schemes requiring arrestees to submit to buccal swab DNA testing solely as a police booking procedure, *see id.*, and parolees to agree in writing to be subject to suspicionless searches at any time, day or night. *Samson*, 547 U.S. at 846 (Thomas, J.)

Mr. Muhtorov argues that in the context of electronic surveillance, reasonableness requires that eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions of privacy." Mot. (Doc. 520) at 34 (citing *Berger v. State of New York*, 388 U.S. 41 (1967) and *United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973)). He urges me to look to traditional FISA and Title III as measures of the reasonableness for electronic surveillance, arguing FAA's approval scheme permitting the generalized acquisition of U.S. persons' communications without any particularized showing or demonstration of cause is a bridge too far. *Id.* I do not disagree, but find there is more to the balance than that. The fact traditional FISA surveillance requires a particularized demonstration of probable cause and is constitutional does not mean that FAA surveillance is unconstitutional because it does not. The question is the degree of the intrusion, weighed against the government's legitimate interest in acquiring foreign intelligence information to protect against the commission of serious crimes such as espionage and terrorist acts committed by or on behalf of foreign powers. In my view, the FAA passes the Fourth Amendment test.

Privacy Interest.

As an initial matter, I consider Mr. Muhtorov's privacy interests. Under § 702, the intrusion on an individual's privacy is as an incidental third party who is a participant in

intercepted communications with a target overseas. The government contends defendants have little or "severely diminished" expectations of privacy in their communications with non-U.S. persons overseas, *see* Unclassified Br. (Doc. 559) at 59-61, & n. 37, based simply on the fact that those persons could be targets for surveillance both by the U.S. government and by other foreign governments or private interest. While I could never adopt the government's cynical view of the First and Fourth Amendment, it is true that expectations of privacy are diminished the more information one puts out into the ether, especially the ether of the global telecommunications network.

Fourth Amendment jurisprudence has long recognized a third-party doctrine, i.e., a diminishment or loss of a person's privacy interests where he reveals information to a third party, even in confidence. *See United States v. Miller*, 425 U.S. 435, 444 (1976)(bank records); *Smith v. Maryland*, 442 U.S. 735 (1979)(use of a pen register by telephone company does not constitute a search within meaning of Fourth Amendment because person has no legitimate expectation of privacy in numbers dialed on his phone). The concept has been held to apply to electronic communications, where "a person's reasonable expectation of privacy may be diminished in transmissions over the Internet or e-mail that have already arrived at the recipient ." *United Sates v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). While Mr. Muhtorov and others have a reasonable expectation of privacy in the content of their communications generally, those interests are at least somewhat diminished when transmitted to a third party over the internet.

Weighing Privacy and National Security Interests to Assess Reasonableness.

The intrusion into U.S. persons' legitimate privacy interests under § 702 is less than the generalized "vacuum-cleaner-style mass collection of virtually every person's international communications" of which Mr. Muhtorov, in his role as *Clapper*-qualified antagoniste, complains. Collection must be demonstrably intertwined with the government's efforts to "acquire foreign intelligence information,"[24] § 1881a(a), and may not "intentionally target any person known at the time of the acquisition to be located in the United States." § 1881a(b)(1). Approval hinges on findings that "foreign intelligence information" gathering is a "significant purpose" of the surveillance, and limitations against abusing the § 702 surveillance process to effectively target Americans will be observed.

More importantly, as was posited at the beginning of this opinion, *Mr. Muhtorov's* concern is less with the incidental acquisition of his communications by national intelligence agencies during the course of otherwise lawful foreign intelligence gathering, but in the retention and *use* of those communications by federal law enforcement in criminal proceedings against him in a court of law. FISA clearly contemplates that intelligence gathering and law enforcement "tend to merge" in the area of terrorism detection and prevention. *See In re Sealed Case*, 310 F.3d at 725 (citing S. Rep. 95-701

[24] "Foreign intelligence information" is defined under FISA as information that "relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . an actual or potential attack . . . sabotage, international terrorism, or the international proliferation of weapons of mass destruction . . . , or clandestine intelligence activities." § 1801(e)(1). It is also information with respect to a foreign power . . . that relates to, and if concerning a United States person is necessary to . . . the national defense or the security of the United States." § 1801(e)(2).

(1978)). The government's interest in using intelligence information to detect and prevent criminal acts of terrorism, and ultimately to punish their perpetrators, is a legitimate governmental interest against which individual FAA privacy intrusions must be weighed.

Relevant to balancing of FAA interceptees' privacy interests against the government's interest in detecting and preventing acts of terrorism, is the fact that the government's *use* of FAA-acquired communications is carefully controlled under FISA. *See id.*, 310 F.3d at 740-41. Minimization procedures must be adopted by the Attorney General for every application under the FAA, *see* § 1881a(e), and must be designed to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1). Procedures must provide for the weeding out of information that is not foreign intelligence information, and the protection of it from dissemination in any manner that identifies a United States person without his consent. § 1801(h)(2). Additional minimization procedures must be established for the retention and dissemination to law enforcement of information that is evidence of a crime, § 1801(h)(3), and provide for how communications to which a United States person is a party may be disclosed, disseminated, or used, and provide time limits for retention. § 1801(h)(4).

Mr. Muhtorov argues that § 702's minimization procedures are inadequate (and the approval scheme therefore constitutionally unreasonable) because they allow the

government to maintain a database of incidently collected information and query it for law enforcement purposes later. These "backdoor searches," Muhtorov concludes, require a warrant and render the FAA approval scheme unconstitutional. I disagree. Accessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information. Evidence obtained legally by one police agency may be shared with similar agencies without the need for obtaining a warrant, even if sought to be used for an entirely different purpose. This principle applies to fingerprint databases and has also been applied in the foreign intelligence context in *Jabara v. Webster*, 691 F.2d 272, 277-79 (6th Cir. 1982).

Applying these standards to the suspicionless incidental acquisition of U.S. persons' communications contemplated under the FAA, I cannot conclude that the FAA's approval procedures are per se constitutionally infirm. These acquisitions must be tailored to the very serious purpose of foreign intelligence gathering, as defined in the Act, and may not be used to target U.S. persons as an end-run around Title III. Minimization procedures must weed out acquisitions that are unrelated to foreign intelligence gathering, and inform the retention, querying, and dissemination of those acquisitions for law enforcement purposes in a manner that is consistent with the limitations in § 1881a(b). I note this conclusion is consistent with Judge King's in *Mohamud* (2014 WL 2866749 at *27), the only other decision to date to have addressed the specific Fourth Amendment challenge to the FAA presented here.

That I do not find the FAA unconstitutional on its face does not *per force* mean that it was constitutionally applied to Mr. Muhtorov. As I have already observed, § 702's authorization procedures are "riddled" with loopholes and there is no judicial oversight of their execution over time. Any acquisition, retention, dissemination, or use of his electronic communications that abused one of these loopholes or exceeded FISC's authorizations in this case would be unlawful. Accordingly, I proceed to consider the constitutionality of the specific § 702 acquisitions of Mr. Muhtorov's electronic communications in this case.

Acquisition of § 702 Materials in this Case.

Other than the specific timeline of the § 702 acquisitions involving Mr. Muhtorov, the relevant facts in this case are straightforward and minimally classified. Nearly all are recited in the Affidavit of Special Agent Hale of the Federal Bureau of Investigation, a public document filed with the court in support of the criminal complaint (Doc.1, filed 01/19/12). The problem with Agent Hale's factual recitation is that it elides any express distinction between the facts gathered as a result of Title I (electronic) and Title III (physical) searches on the one hand, and Title VII (FAA-acquired) information on the other.

The Islamic Jihad Union (IJU) is an extremist organization that splintered from the Islamic Movement of Uzbekistan (IMU) in the early 2000s. The IJU adheres to an anti-Western ideology, opposes secular rule in Uzbekistan, and seeks to replace the current regime with a government based on Islamic law. The IJU first conducted attacks

in April, 2004, targeting a popular bazaar and police at several roadway checkpoints. These attacks killed approximately 47 people, including 33 terrorists, some of whom were suicide bombers. The IJU claimed responsibility for these attacks on multiple militant Islamic websites and denounced the leadership of Uzbekistan. In July, 2004, the IJU conducted simultaneous suicide bombings of the United States and Israeli Embassies in Uzbekistan as well as the Uzbekistani Prosecutor General's Office in Tashkent, Uzbekistan. Claiming responsibility for these attacks, the IJU stated that its martyrdom operations would continue. The IJU also claimed the attacks were committed in support of its Palestinian, Iraqi and Afghan brothers in a global insurgency.

In September, 2007, German authorities arrested three IJU operatives, thus disrupting a plot against unidentified U.S. or Western facilities in Germany. The IJU operatives had available 700 kilograms of hydrogen peroxide and an explosives precursor sufficient in raw material to make the equivalent of about 1200 pounds of TNT. The IJU claimed responsibility for the foiled plot. The IJU has also claimed responsibility for attacks targeting coalition forces in Afghanistan in 2008 including a March suicide attack against a U.S. military post that was allegedly carried out by a German-born Turk.

In April, 2009, Turkish authorities seized weapons and detained extremists with ties to the IJU. The IJU also claimed responsibility for a May 2009 attack in Uzbekistan and numerous attacks in Afghanistan against coalition forces. At all times relevant to the charges against Mr. Muhtorov, the IJU was designated a terrorist organization by the Secretary of State, and has been so designated since June 12, 2005, under the name

Islamic Jihad Group.[25]

As has already been disclosed, the FISA application at issue in this case was based in part on FAA surveillance and collection. Mr. Muhtorov contends the "incidental" acquisition of his communications and their subsequent retention, querying, and use in criminal proceedings brought against him, was unreasonable under the Fourth Amendment. I have already reviewed the FISA Court's Title I and Title III approvals and concluded the searches and surveillance conducted under those approvals was lawfully authorized and conducted. I have since performed an exhaustive *in camera* and *ex parte* review of all relevant additional classified materials provided to me by the government, including supplemental classified materials prepared at my request. I conclude on the record before me that a proper and supported application was filed, and that the targeting and minimization procedures forwarded were tailored to the government's legitimate foreign intelligence purposes and took into account the privacy interests of individuals whose communications would be incidently acquired. Mr. Muhtorov's Motion to Suppress Evidence Obtained or Derived under § 702 (Doc. 520) is DENIED. Because I find all legal criteria were met by the government to establish that the searches and surveillance at issue were lawfully authorized and conducted, there is no need to consider the "good faith" alternative basis for denying the Motion to Suppress.

---

[25] Notification of its designation appears at 70 Fed. Reg. 35332-01 (June 17, 2005) and was amended to include the name "Islamic Jihad Union" on April 29, 2008, published in the 73 F. Reg 30443-01 (May 27, 2008).

As stated at the June 17, 2015 status conference, I will address Mr. Muhtorov's request for specific, additional discovery and declassification in a separate order, after conducting one or more prefatory CIPA § 4 hearings on the subject. Accordingly, this matter will be set for a discovery conference, to be attended by the government and the defense, at which time the government should be prepared to address the CIPA § 4 hearing and process for moving toward the declassification of any *Brady* and related information material to the defense in this case. The conference will be conducted before a court reporter and under conditions that will allow it to be conducted as a closed hearing, should the need arise.

Dated November 19, 2015

s/John L. Kane
SENIOR U.S. DISTRICT JUDGE