IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

CASE NO. 12-cr-00033-JLK-1

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. JAMSHID MUHTOROV,

Defendant.

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED OR DERIVED FROM SURVEILLANCE UNDER THE FISA AMENDMENTS ACT AND MOTION FOR DISCOVERY

The defendant, Jamshid Muhtorov, through the undersigned, appointed counsel of record, and the American Civil Liberties Union Foundation, and the American Civil Liberties Union Foundation of Colorado, moves to suppress all evidence obtained or derived from surveillance conducted pursuant to the FISA Amendments Act of 2008 ("FAA").

Related to this, Mr. Muhtorov moves for discovery of evidence concerning the manner in which the FAA was used in the government's investigation of him.

INTRODUCTION

Jamshid Muhtorov is charged with his codefendant, Bakhtiyor Jumaev, in an indictment alleging the two men conspired and attempted to provide material support to a group identified as a terrorist organization. Doc. 50.[1] More than two years after his arrest, Mr. Muhtorov was notified that the government intends to "offer into evidence or otherwise use or disclose" in these proceedings "information obtained or derived" from surveillance conducted under the FAA. Doc. 457.[2] That statute purports to allow the government to collect the international communications of U.S. citizens and residents en masse, without probable cause. Publicly available documents make clear that the government has implemented the statute's authority broadly.

Mr. Muhtorov now moves to suppress the fruits of the FAA surveillance on the grounds that the government's monitoring of his communications under the statute violated the Fourth Amendment to the U.S. Constitution as well as Article III. *See* 50 U.S.C. § 1806(g) (providing for suppression of evidence where surveillance was "not lawfully authorized or conducted"); *United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297 (1972) (hereafter "*Keith*") (warrantless surveillance conducted for domestic security purposes violates Fourth Amendment); *Berger v. New York*, 388 U.S.

---

[1] "Doc." refers to the Clerk's Docket.

[2] The codefendant, Mr. Jumaev, was not provided similar notice. The issue of whether he should have been, and his standing to raise the same challenges Mr. Muhtorov does here are before the Court. *See* Docs. 458, 470, 499, 518. Should Mr. Jumaev choose to do so, Mr. Muhtorov welcomes his adoption of the arguments advanced in this brief. *See* D.C.Colo.LCr 12.1 (b).

41 (1967) (requiring suppression of evidence obtained in reliance on unconstitutional eavesdropping statute).

In addition, Mr. Muhtorov moves for discovery of material that would be helpful and material to his defense, that would permit him to better understand the role that the FAA played in the government's investigation of him, and that would enable him to challenge the specific manner in which the FAA was used in his case. As explained below, Mr. Muhtorov is entitled to such discovery under both the Foreign Intelligence Surveillance Act ("FISA") and the due process clause of the Fifth Amendment.

FACTUAL AND STATUTORY BACKGROUND

A. Jamshid Muhtorov

Jamshid Muhtorov was born in Jizzak, Uzbekistan, when the country was still under communist rule. He is the oldest of five children. His father, Asror Muhtorov, is a doctor, and his mother, Robiya Muhtorova, was a school teacher. Both still live in Uzbekistan.

A few years after graduating from a technical university, Mr. Muhtorov was offered a position with the Ezgulik Human Rights Society, a human rights organization in Uzbekistan. In 2003, he became the head of the Jizzak branch.

During his time with Ezgulik, Mr. Muhtorov worked closely with Human Rights Watch, foreign embassies, and NGOs, as a result of which he came under increasing scrutiny from the repressive regime of Islam Karimov, who has been in power since the breakup of the Soviet Union. This scrutiny intensified after the Andijon Massacre in May

2005, and, in 2006, according to Human Rights Watch reports, led to Mr. Muhtorov being threatened and beaten unconscious. With the help of other activists, Mr. Muhtorov escaped from Uzbekistan just ahead of agents of the Karimov regime who were pursuing him. His wife and children followed him shortly afterward, joining him in Kyrgystan.

In February 2007, Mr. Muhtorov and his family were admitted to the United States as political refugees. He, his wife, Nargiza Muhtorova, and the couple's two children settled in Colorado. (The couple's third child was born after they arrived here.) Mr. Muhtorov has no criminal record and, before his arrest on the instant charges two years ago, had never been arrested—except by the Uzbek security police. Today, he is a legal permanent resident of the United States.[3]

After arriving in Denver, Mr. Muhtorov worked mainly as a truck driver, supporting his family, and repaying the loan made to him by Lutheran Immigration and Refugee Services that enabled him and his family to resettle here. He became active with a local mosque, and continued to follow political developments in Uzbekistan. Until his arrest in January of 2012, he felt free: free to practice his faith; free to engage in political discourse; free to express his own views without fear of arrest, physical assault or repression.

---

[3] *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"); *id.*§ 1881(a). This brief will, on occasion, refer to "Americans." Where appropriate, this term is meant to include "United States persons."

B. The government's belated notice of FAA surveillance

This case involves numerous intrusive searches of Mr. Muhtorov's computer, email accounts, private residence, and personal effects. At the outset of the prosecution, the government represented that it had conducted these searches based on "court authorization[s]." Aff. of Donald E. Hale, Special Agent, FBI ¶ 12 (attached to Crim. Compl., Doc. 1). On February 7, 2012, the government notified Mr. Muhtorov that it intended to "offer into evidence or otherwise use or disclose" in these proceedings information "information obtained and derived" from surveillance conducted under FISA, 50 U.S.C. §§ 1801–1811, 1821–1829. Doc. 12. That notice, however, made no mention of surveillance under the FAA.

Mr. Muhtorov did not learn that the government had intercepted his communications under the FAA until October 25, 2013, twenty months after the government's initial FISA notice. *See* Doc. 457. This was because, until recently, the government had a policy of concealing from criminal defendants any connection between the FAA and their prosecutions. This policy violated both the FAA itself, 50 U.S.C. §§ 1881e(a), 1806(c), and the due process rights of criminal defendants like Mr. Muhtorov.

The government's policy of withholding notice of FAA surveillance came to light only after the Supreme Court decided *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), last winter. In that case, the government argued that human rights groups and other organizations lacked standing to challenge the FAA's constitutionality because they could not show a sufficient likelihood that their communications would be monitored

under it. In making that argument, the government assured the Court that dismissing the case would not forever insulate the statute from judicial review. In particular, the government stated that it would notify criminal defendants against whom it intended to introduce evidence obtained or derived from FAA surveillance, and that lower courts would have an opportunity to adjudicate the statute's constitutionality when defendants filed motions to suppress. *See* Br. of Petitioners 8, *Amnesty*, 133 S. Ct. 1138 (No. 11-1025) (citing 50 U.S.C. §§ 1881e(a), 1806(c)); *see also* Tr. of Oral Argument at 4:12–17, *Amnesty*, 133 S. Ct. 1138 (No. 11-1025). Relying on the government's representation, *Amnesty*, 133 S. Ct. at 1154, a divided Court dismissed the case, *id*. at 1155.

Though the Solicitor General did not know it at the time, his representation to the Court in *Amnesty* was untrue. In the five years between the FAA's enactment and the Court's consideration of *Amnesty*, no criminal defendant had received notice of FAA surveillance. In fact, the Justice Department had a practice of concealing from criminal defendants the role that the FAA had played in the government's investigation of them.[4] The Solicitor General apparently learned of the Justice Department's policy only because the Chair of the Senate Select Committee on Intelligence, Senator Dianne Feinstein, made public statements about the government's use of evidence acquired under the FAA in certain criminal prosecutions, including this one. Those statements led some criminal

[4] On November 21, 2013, three members of the Senate Select Committee on Intelligence wrote to the Solicitor General requesting a "formal notification to the Supreme Court of the government's misrepresentations" in *Amnesty*. *See* Letter from Sen. Mark Udall, Sen. Ron Wyden & Sen. Martin Heinrich to Donald Verrilli, Solicitor General (Nov. 20, 2013), http://1.usa.gov/1knrIRv.

defendants to seek clarification from the government. When he learned of the Justice Department's policy, the Solicitor General reportedly concluded that the policy "could not be justified legally." *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, http://nyti.ms/1bAe7QZ. After extended debate within the executive branch, the Justice Department ultimately changed its policy and publicly affirmed its notice obligation. *See, e.g.*, Devlin Barrett, *U.S. Spy Program Lifts Veil in Court*, Wall St. J., July 31, 2013, http://on.wsj.com/19nu8KC.

In October of last year, Mr. Muhtorov became the first person charged as a defendant in a criminal prosecution to receive notice of FAA surveillance. *See* Devlin Barrett, *U.S. Tells Suspect for First Time It Used NSA Surveillance Program in Criminal Case*, Wall St. J., Oct. 25, 2013, http://on.wsj.com/16Bv4av. The notice he received states, in relevant part, that the government:

> hereby provides notice to this Court and the defense, pursuant to 50 U.S.C. § 1806(c) and 1881e(a), that the government intends to offer into evidence or otherwise use or disclose in proceedings in the above-captioned matter information obtained or derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §1881a.

Doc. 457.

C. The Foreign Intelligence Surveillance Act

In 1975, Congress established a committee, chaired by Senator Frank Church, to investigate allegations of "substantial wrongdoing" by the intelligence agencies in their conduct of surveillance. *Final Report of the S. Select Comm. to Study Governmental*

Operations with Respect to Intelligence Activities (Book II), S. Rep. No. 94-755, at v (1976) ("Church Report"). The committee discovered that, over the course of four decades, the intelligence agencies had "violated specific statutory prohibitions," "infringed the constitutional rights of American citizens," and "intentionally disregarded" legal limitations on surveillance in the name of "national security." *Id*. at 137. Of particular concern to the committee was that the agencies had "pursued a 'vacuum cleaner' approach to intelligence collection," in some cases intercepting Americans' communications under the pretext of targeting foreigners. *Id*. at 165. To ensure proper judicial involvement in the protection of Americans' communications, the committee recommended that all surveillance of communications "to, from, or about an American without his consent" be subject to a judicial warrant procedure. *Id*. at 309.

In 1978, largely in response to the Church Report, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny government applications for surveillance orders in certain foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). In its current form, FISA regulates, among other things, "electronic surveillance," which is defined to include:

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.

50 U.S.C. § 1801(f)(2).

Before passage of the FAA in 2008, FISA generally foreclosed the government from engaging in "electronic surveillance" without first obtaining an individualized and particularized order from the FISC. To obtain a traditional FISA order, the government is required to submit an application that identifies or describes the target of the surveillance; explains the government's basis for believing that "the target of the electronic surveillance is a foreign power or an agent of a foreign power;" explains the government's basis for believing 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;" and describes the nature of the foreign intelligence information sought and the type of communications that will be subject to surveillance. *Id*. § 1804(a).

The FISC may issue a traditional FISA order only if it finds that, among other things, there is "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," *id*. § 1805(a)(2)(A), 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," *id*. § 1805(a)(2)(B).

D. The warrantless wiretapping program

On October 4, 2001, President George W. Bush secretly authorized the NSA to engage in warrantless electronic surveillance inside the United States.[5] After *The New*

[5] *See* Public Declaration of James R. Clapper, Director of National Intelligence ("DNI") ¶ 6, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. Dec. 20, 2013), Doc. 168 ("Clapper *Jewel* Decl.").

York Times exposed the program and a federal district court ruled that the program was unconstitutional, *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), the government stated that the program would not be reauthorized in its then-existing form. The government ultimately sought legislative amendments to FISA that granted authorities beyond what FISA had allowed for three decades.[6]

E. The FISA Amendments Act

The legislative amendments sought by the Bush administration were embodied in the FAA, which was signed into law on July 10, 2008.[7] The FAA substantially revised the FISA regime and authorized the acquisition without individualized suspicion of a wide swath of communications, including U.S. persons' international communications, from internet and telecommunications providers inside the United States. Like surveillance under FISA, FAA surveillance takes place on U.S. soil. But the authority granted by the FAA is altogether different from, and far more sweeping than, the authority that the government has traditionally exercised under FISA. The FAA's implications for U.S. persons' constitutional rights are correspondingly far-reaching. Because Mr. Muhtorov contests the lawfulness of the government's surveillance of him under the FAA, it is necessary to describe the statute in some detail.

---

[6] *See id.*; *see also Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the H. Comm. on the Judiciary*, 110th Cong. (2007) (statement of J. Michael McConnell, DNI), http://1.usa.gov/1kb6c26.

[7] On August 5, 2007, Congress passed a predecessor statute, the Protect America Act, Pub. L. No. 110-55, 121 Stat. 552 (2007), whose authorities expired in February 2008.

The FAA allows the government to conduct dragnet surveillance of international communications entering or leaving the United States, including communications sent or received by U.S. persons. It does this by permitting the government to intercept communications when at least one party to a phone call or email is a foreigner located abroad. In particular, the FAA permits the Attorney General and DNI 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).

No court ever approves the target of this surveillance. Rather, the FISC approves only the general procedures the government proposes to use in carrying out its surveillance and, on the basis of those procedures alone, the FISC issues a so-called "mass-acquisition order." *See id.* § 1881a. Before obtaining such an order, the Attorney General and DNI must provide to the FISC a written certification attesting that the FISC has approved, or that the government has submitted to the FISC for approval, both "targeting procedures" and "minimization procedures." *Id.* § 1881a(d)–(g). The targeting procedures must be "reasonably designed" to ensure the acquisition is "limited to targeting 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). The minimization procedures must meet the requirements of section 1801(h), 1821(4). *Id.* § 1881a(g)(2)(A)(ii).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to prevent the targeting of U.S. persons in certain contexts, *id*. § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose" of the acquisition is "to obtain foreign intelligence information." *Id*. § 1881a(g)(2)(A)(iii)–(vii). The phrase "foreign intelligence information" is defined broadly to include, among other things, information concerning terrorism, national defense, and foreign affairs. *Id*. § 1801(e).

A crucial difference between the FAA and traditional FISA is that the FAA authorizes surveillance not predicated on probable cause or individualized suspicion. When the government makes an FAA application to the FISC, it simply asks the court to approve the overall targeting and minimization procedures that will guide the government's surveillance for the following year. The government need not demonstrate to the FISC that its surveillance targets are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, the FAA permits the government to target any foreigner located outside the United States. *See* David S. Kris & J. Douglas Wilson, 1 *National Security Investigations and Prosecutions* § 17.3, 602 (2d ed. 2012) ("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.").

As noted, the FAA does not require the government to identify its surveillance targets to the FISC at all, or even to identify the specific "facilities, places, premises, or

property at which" its surveillance will be directed. 50 U.S.C. § 1881a(g)(4). This means that the government can "direct surveillance . . . at various facilities without obtaining a separate authorization for each one." Kris & Wilson § 17.3, 602. The government may even direct its surveillance at "gateway" switches, through which flow the communications of millions of people, rather than at individual telephone lines or email addresses. *Id.* § 16.12, 577. The FISC reported that in 2011—the year in which much of the government's surveillance of Mr. Muhtorov apparently took place—the NSA relied on the FAA to collect more than 250 million internet communications. *See [Redacted]*, 2011 WL 10945618, at *10 (FISC Oct. 3, 2011).

By dispensing with FISA's principal limitations, the FAA exposes every international communication—that is, every communication between an individual in the United States and a non-American abroad—to potential surveillance. Indeed, this was the statute's purpose. In advocating changes to FISA, intelligence officials made clear that their aim was to enable broader surveillance of communications between individuals inside the United States and non-Americans abroad. *See FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 9 (2006), http://1.usa.gov/1kbgHm3 (statement of NSA Director Michael Hayden) ("Hayden SJC Statement") (stating, with respect to the FAA's predecessor statute, that certain communications "with one end . . . in the United States" are the ones "that are most important to us"). As a result, the government can once again conduct the kind of vacuum-cleaner–style surveillance that the Church Committee found so troubling. And,

as discussed further below, the NSA is using the statute to do precisely this.

To the extent the statute attempts to provide safeguards for U.S. residents' constitutional rights, the safeguards take the form of "minimization procedures," which must be "reasonably 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), 1821(4)(A). The statute's minimization requirement is supposed to protect against the collection, retention, and dissemination of communications that have been collected "incidentally" or "inadvertently." However, the statute does not prescribe specific minimization procedures and it does not give the FISC the authority to monitor compliance with minimization procedures. Most significantly, it includes an exception that specifically allows the government to retain and disseminate communications—including those of U.S. persons—if the government concludes that they contain "foreign intelligence information," a term that is (as noted above) defined very broadly. *Id*. § 1881a(e). In other words, the statute is designed to allow the government not just to collect but to retain U.S. persons' international communications.

The FISC's oversight role in authorizing and supervising FAA surveillance is "narrowly circumscribed." *In re Proceedings Required by § 702(I) of the FISA Amendments Act of 2008*, No. Misc. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008) (quotation marks omitted). Unlike the judiciary's traditional Fourth Amendment role—as a gatekeeper for particular acts of surveillance—the FISC simply approves vague parameters under which the government is free to conduct surveillance for up to

one year. The FISC does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not supervise the implementation of the government's targeting or minimization procedures. The role that the FISC plays under the FAA bears no resemblance to the role that it traditionally played under FISA.

F. The government's implementation of the FISA Amendments Act

Nothing in the government's implementation of the statute cures or even mitigates the statute's significant defects. To the contrary, publicly available versions of the government's targeting and minimization procedures only confirm that the rules that supposedly protect privacy are weak and riddled with exceptions.[8] Even when the government abides by the rules, the government collects thousands, possibly millions, of U.S. residents' communications without probable cause or individualized suspicion.[9] And

---

[8] While the government has officially disclosed a version of the minimization procedures it uses to implement the FAA, *see Minimization Procedures Used by National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (Oct. 31, 2011), http://1.usa.gov/1e2JsAv ("2011 Minimization Procedures"), it has not officially disclosed its targeting procedures. It has, however, made several disclosures that reveal its targeting procedures in broad outlines. *See generally [Redacted]*, 2011 WL 10945618. Moreover, in June 2013, *The Guardian* revealed a copy of the FAA targeting procedures approved by the FISC in 2009. *See Procedures Used by the National Security Agency for Targeting Non–United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended* (July 28, 2009), https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf ("2009 Targeting Procedures").

[9] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, June 7, 2013, http://wapo.st/1kdYqVb ("Even when the system works just as advertised, with no American

recently released FISC opinions make clear that the government has violated the rules repeatedly, including in the period during which Mr. Muhtorov's communications were obtained. *See [Redacted]*, 2011 WL 10945618, at *2–*9.

Publicly available versions of the government's targeting procedures underscore the scope of the surveillance carried out under the statute. As noted above, one of the statute's principal purposes was to permit the government to conduct dragnet surveillance of U.S. persons' international communications. The procedures give effect to that intent by permitting the government to collect U.S. persons' international communications in the course of warrantless surveillance directed at targets outside the United States. *See, e.g.*, 2009 Targeting Procedures 6 (discussing need to prevent acquisition only of communications "as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States"). Indeed, the procedures ensure that U.S. persons' international communications will be collected in bulk. For example, while the procedures require the government to identify "targets" outside the country, once the targets have been identified, the procedures permit the NSA to sweep up not just any communications *to* and *from* those targets but any international communication *about* those targets. *See* 2009 Targeting Procedures 1 (discussing "those cases where NSA seeks to acquire communications about the target that are not to or from the target"); *see also [Redacted]*, 2011 WL 10945618, at *5.

---

singled out for targeting, the NSA routinely collects a great deal of American content.").

News reports discuss this kind of surveillance—sometimes called "about" surveillance—in more detail. An August 2013 report from *The New York Times* states that the NSA is "searching the contents of vast amounts of Americans' e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance, according to intelligence officials." Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1cez5ZK. The report continues: "While it has long been known that the agency conducts extensive computer searches of data it vacuums up overseas, that it is systematically searching—without warrants—through the contents of Americans' communications that cross the border reveals more about the scale of its secret operations." *Id*.

Thus, even when the government abides by its rules, it collects huge volumes of U.S. residents' international communications without any of the safeguards the Constitution ordinarily requires. Moreover, the minimization procedures place no meaningful limit on the government's authority to retain, analyze, and disseminate these communications. *See, e.g.*, 2011 Minimization Procedures §§ 3(b), 6 (permitting the government to retain communications to, from, or about U.S. persons for five years, or indefinitely if they contain "foreign intelligence information" or evidence of a crime). Even purely domestic communications can be retained indefinitely if the government concludes that they contain foreign intelligence information. *Id.* § 5.

The minimization procedures also permit the government to conduct warrantless searches in its database of communications collected under the FAA, including by using search terms or identifiers (names, email addresses, phone numbers, etc.) associated with U.S. persons.[10] These kinds of searches—"backdoor searches"—are an end-run around the Fourth Amendment. *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, Guardian, Aug. 9, 2013, http://gu.com/p/3tva4 ("Senator Ron Wyden told the Guardian that the law provides the NSA with a loophole potentially allowing 'warrantless searches for the phone calls or emails of law-abiding Americans'"). A presidential review group recently recommended ending the practice of backdoor searches, concluding that the practice violates the "full protection of [Americans'] privacy." *See* President's Review Group on Intelligence & Communications Technologies, Liberty and Security in a Changing World 149, 145–50 (Dec. 12, 2013), http://1.usa.gov/1be3wsO.

[10] These kinds of searches were once prohibited by the government's minimization procedures, but the prohibition was lifted in 2011. *Compare* Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702, As Amended § 3(b)(5) (July 29, 2009), http://bit.ly/1hKjOzC ("Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, *will not include United States person names or identifiers* . . . ." (emphasis added)), *with* 2011 Minimization Procedures § 3(b)(6) (omitting same restriction and stating that "use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures").

G. The role that the FAA played in the government's investigation of Mr. Muhtorov

The FAA notice in this case was filed belatedly, and only after the government reversed its existing policy of depriving criminal defendants of notice under the statute. The notice supplies no information beyond the bare fact that the government intends to introduce or otherwise use information obtained or derived through use of the FAA. Thus, while it is plain that the FAA played a key role in the government's investigation of Mr. Muhtorov, the government has not provided Mr. Muhtorov with information that is crucial to his defense.[11]

For example, the government has not told Mr. Muhtorov which communications it obtained under the FAA, when they were obtained, and whether they were used as the basis for subsequent warrant applications. It has not provided Mr. Muhtorov with its surveillance applications, the affidavits submitted in connection with those applications, or the FISC orders that granted those applications. It has not told Mr. Muhtorov which targeting and minimization procedures applied at the time his communications were collected; nor has it provided him with documents, including FISC orders, relating to the government's compliance or non-compliance with those procedures. Nor, finally, has it told Mr. Muhtorov which selectors, search terms, or filters were applied to information

[11] Discovery provided by the government thus far suggests that the government began intercepting Mr. Muhtorov's email communications no later than January 2011. The earliest communication provided to the defense is a January 29, 2011 email exchange between an account associated with Mr. Muhtorov and an account that is allegedly linked to the Islamic Jihad Union. The earliest cell-phone interception of which the defense is aware was on March 8, 2011, purportedly a call between Mr. Muhtorov and the codefendant, Mr. Jumaev.

collected in bulk such that the government's attention became focused on him.

To be clear, and as explained at greater length below, Mr. Muhtorov believes that the government's surveillance of him was unlawful for the simple fact that it was carried out under a statute that is procedurally defective—that is, because it was carried out under a statute that fails to comply with the Fourth Amendment's most basic requirements. But both FISA and the due process clause of the Fifth Amendment entitle Mr. Muhtorov to more information about how, precisely, the FAA was used to collect his communications, how the communications collected under the statute were used in the government's investigation of him, and in which ways the evidence they propose to use in the instant prosecution is tainted by the government's violation of his constitutional rights.

ARGUMENT

I. The evidence obtained or derived from surveillance under the FAA must be suppressed because the FAA is unconstitutional.

The fruits of the government's surveillance of Mr. Muhtorov must be suppressed because the statute that authorized the surveillance is unconstitutional. The FAA violates the Fourth Amendment because it authorizes surveillance that violates the warrant clause and, independently, because it authorizes surveillance that is unreasonable. The statute also violates Article III by requiring judges to issue advisory opinions in the absence of a case or controversy. The procedural deficiencies of the FAA render the statute unconstitutional, and they render the surveillance of Mr. Muhtorov unconstitutional as well. *See Sibron v. New York*, 392 U.S. 40, 59 (1968) ("No search . . . is valid" if

authorized by a statute whose "procedural safeguards" are "inadequate to ensure the sort of neutral contemplation by a magistrate of the grounds for the search and its proposed scope." (citing *Berger v. New York*, 388 U.S. 41 (1967)); *Bond v. United States*, 131 S. Ct. 2355 (2011).[12] All evidence obtained or derived from the unlawful surveillance conducted under the statute —that is, all evidence obtained directly or indirectly from the statute's use—must be suppressed. *See* 50 U.S.C. § 1806(g).

A. The FAA violates the Fourth Amendment.

The FAA gives the government nearly unfettered access to U.S. persons' international communications. Whereas FISA authorizes the government to conduct relatively narrow surveillance of foreign agents and foreign powers, the FAA permits the government to monitor *any* international communication without a warrant so long as the target of its surveillance is a foreigner abroad and a significant purpose of its surveillance is to acquire foreign intelligence information. In effect, the statute allows the government to acquire essentially any communication that originates or terminates outside the United States.

The statute violates the warrant clause because it allows the government to monitor U.S. persons' international communications without obtaining prior judicial approval

---

[12] *See Berger*, 388 U.S. at 58 (invalidating an electronic surveillance statute that lacked "precise and discriminate" procedural requirements "carefully circumscribed so as to prevent unauthorized invasions" of privacy); *see also*, *e.g.*, *Chandler v. Miller*, 520 U.S. 305 (1997) (invalidating state statute requiring candidates for state office to undergo warrantless and suspicionless drug tests); *Payton v. New York*, 445 U.S. 573 (1980) (invalidating state statute authorizing warrantless entry into homes); *Torres v. Puerto Rico*, 442 U.S. 465 (1979) (invalidating state statute permitting warrantless and suspicionless searches of luggage).

based upon probable cause, and without describing the communications to be obtained with particularity. It also violates the reasonableness requirement. The Supreme Court has emphasized that a surveillance statute is reasonable only if it is precise and discriminate. The FAA is anything but.

1. Mr. Muhtorov had a reasonable expectation of privacy in his international communications.

American citizens and residents—including Mr. Muhtorov—have a constitutionally protected privacy interest in the content of their telephone calls and emails. *United States v. Katz*, 389 U.S. 347, 353 (1967); *see also Keith*, 407 U.S. at 313 ("[*Katz*] implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."); *Alderman v. United States*, 394 U.S. 165, 177 (1969); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *In re Applications for Search Warrants for Info. Associated with Target Email Address*, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (following *Warshak*). Indeed, as the Supreme Court noted in *Berger,* "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices," 388 U.S. at 63. In invalidating the New York surveillance statute before it, the Court wrote: "[I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded." *Id*. at 63.

The Fourth Amendment's protection extends not just to domestic communications but to international ones as well. *See, e.g.*, *United States v. Ramsey*, 431 U.S. 606, 616–20 (1977); *see also* Defs.' Mem. in Opp'n to Pls.' Mot. for Summ. J. 48, *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633 (S.D.N.Y. 2009) (No. 08 Civ. 6259) (not contesting that Fourth Amendment protects privacy of U.S. persons' international communications).

2. The FAA permits surveillance of U.S. persons' international communications in violation of the warrant requirement.

a. The FAA authorizes "general searches."

The Fourth Amendment requires that search warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Supreme Court has interpreted these words to require three things: (1) that any warrant be issued by a neutral, disinterested magistrate; (2) that those seeking the warrant demonstrate to the magistrate there is probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense; and (3) that any warrant particularly describe the things to be seized as well as the place to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979).

The FAA authorizes the executive branch to conduct electronic surveillance without complying with any of these three requirements; accordingly, the statute is presumptively unconstitutional. *See Katz*, 389 U.S. at 357 (Warrantless searches are "per se unreasonable under the Fourth Amendment—subject only to a few specifically

established and well-delineated exceptions."); *accord Payton*, 445 U.S. 573; *Chimel v. California*, 395 U.S. 752, 768 (1969).

First, the FAA fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Katz,* 389 U.S. at 357 (internal quotation marks omitted). While the government may not initiate an acquisition under the FAA without first applying for a mass-acquisition order from the FISC (or obtaining such an order within seven days of initiating the acquisition), the FISC's role is solely to review general procedures relating to targeting and minimization. Every decision relevant to the surveillance of *specific* targets is made by executive officers and never presented to the FISC. Indeed, nothing in the FAA requires the government even to *inform* the FISC who its surveillance targets are (beyond to say that the targets are outside the United States), what the purpose of its surveillance is (beyond to say that a "significant purpose" of its year-long program of surveillance is to gather foreign intelligence), or which, or how many, U.S. persons are likely to be implicated by the acquisition. *Compare with* 18 U.S.C. § 2518(1)(b) (requiring government's application for Title III warrant to include details of the particular offense that has been committed, a description of the nature and location of facilities to be monitored, a description of the type of communications to be intercepted, and the identity of the individual to be monitored); 50 U.S.C. § 1804(a) (setting out similar requirements for FISA orders).

The Fourth Amendment reflects a judgment that "[t]he right of privacy [is] too precious to entrust to the discretion of those whose job is the detection of crime and the

arrest of criminals," *McDonald v. United States*, 335 U.S. 451, 455–56 (1948), but this is precisely what the FAA does: It entrusts to the *unreviewed* discretion of the executive branch decisions that affect the privacy rights of countless U.S. persons.

Second, the FAA fails to condition government surveillance on the existence of probable cause. It permits the government to conduct acquisitions without proving to a court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. *Compare with* 18 U.S.C. § 2518(3) (Title III probable cause requirement); 50 U.S.C. § 1805(a)(2) (corresponding provision for FISA). It permits the government to conduct acquisitions without even making an *administrative* determination that its targets fall into any of these categories.

It is important to recognize that the absence of an individualized suspicion requirement has ramifications for U.S. persons like Mr. Muhtorov even though the government's ostensible targets are foreign citizens outside the United States. The absence of an individualized suspicion requirement means that the government can engage in the wholesale collection of U.S. persons' international communications—that it can, for example, intentionally collect all communications between the New York and London offices of Amnesty International, or all communications between Human Rights Watch in New York and human rights researchers in South and Central Asia. In fact, under the FAA the government could collect *all* communications between New York and London so long as the nominal targets for this mass acquisition were non-U.S. persons believed to be in the United Kingdom.

Third, the FAA fails to restrict the government's surveillance authority to matters described with particularity. The requirement of particularity "is especially great in the case of eavesdropping," as eavesdropping inevitably results in the interception of intimate conversations that are unrelated to the investigation. *Berger*, 388 U.S. at 56. Unlike Title III and FISA, however, the FAA does not require the government to identify the individuals to be monitored. *Compare with* 18 U.S.C. § 2518(1)(b)(iv) (Title III); 50 U.S.C. § 1804(a)(2) (FISA). It does not require the government to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. *Compare with* 18 U.S.C. § 2518(1)(b)(ii) (Title III); 50 U.S.C. § 1804(a)(3)(b) (FISA). It does not limit the kinds of communications the government can acquire, beyond requiring that a programmatic purpose of the government's surveillance be to gather foreign intelligence. *Compare with* 50 U.S.C. § 1804(a)(6) (allowing issuance of FISA order only upon certification that a significant purpose *of the specific intercept* is to obtain foreign intelligence information). It does not require the government to identify "the particular conversations to be seized," *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). *Compare with* 18 U.S.C. § 2518(1)(b)(iii) (Title III); 50 U.S.C. § 1804(a)(6) (FISA). Nor, finally, does it place any reasonable limit on the duration of mass-acquisition orders. *Compare* 50 U.S.C. § 1881a(a) (allowing surveillance programs to continue for up to one year), *with* 50 U.S.C. § 1805(d)(1) (providing that surveillance orders issued under FISA are generally limited to 90 or 120 days), and 18 U.S.C. § 2518(5) (providing that surveillance orders issued under Title III are limited to 30 days).

The FAA simply does not ensure that surveillance conducted under the Act "will be carefully tailored." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

b. There is no special needs exception to the warrant requirement for foreign intelligence gathering.

No "special needs" exception to the warrant requirement applies to the surveillance conducted under the FAA. Even if the foreign intelligence context may justify a *modification* to the probable cause requirement (as some courts have held with respect to traditional FISA), it does not justify abandoning altogether that requirement. Courts have recognized an exception to the warrant requirement "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring); *see Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (adopting Justice Blackmun's "special needs" formulation for the Court). The mere fact that the government's surveillance is conducted for foreign intelligence purposes, however, does not render the warrant and probable cause requirement unworkable.

Any discussion of the lawfulness of warrantless intelligence surveillance must begin with *Keith*, 407 U.S. 297, in which the Supreme Court addressed the lawfulness of warrantless surveillance conducted by the FBI against individuals eventually charged with having planned or carried out the bombing of a CIA office in Ann Arbor, Michigan. In that case, the government argued that the warrantless surveillance was lawful because

it had been conducted for intelligence purposes rather than law enforcement purposes. The Court emphatically disagreed. Addressing the government's effort to distinguish intelligence surveillance from law enforcement surveillance, the Court wrote that "[o]fficial surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech." *Id*. at 320. Addressing the government's claim that security matters would be "too subtle and complex for judicial evaluation," it observed that the judiciary "regularly deal[s] with the most difficult issues of our society" and that there was "no reason to believe that federal judges [would] be insensitive to or uncomprehending of the issues involved in domestic security cases." *Id*. Finally, addressing the government's contention that the warrant requirement would "fracture the secrecy essential to official intelligence gathering," the Court noted that the judiciary had experience dealing with sensitive and confidential matters and that in any event warrant-application proceedings were ordinarily *ex parte*. *Id*. at 320–21.

Keith involved surveillance directed at domestic security threats, but its logic applies with equal force to surveillance directed at threats with a foreign nexus—at least when that surveillance sweeps up U.S. persons' communications (as surveillance conducted under the FAA does), and is conducted inside the United States (as surveillance conducted under the FAA is). *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 278 (1990) (Kennedy, J., concurring) (concluding that a warrant was not required for the search of a non-resident alien's home in Mexico but stating that "[i]f the

search had occurred in a residence within the United States, I have little doubt that the full protections of the Fourth Amendment would apply"); *see* also H.R. Rep. No. 110-373(I), at 15 n.26 (2007) ("In judging the 'reasonableness' of [a] search, however, the location of the intercept can be as important as the location of the U.S. person under surveillance." (citing *Verdugo-Urqidez*, 494 U.S. at 278 (Kennedy, J., concurring)).

First, intelligence surveillance conducted inside the United States presents the same risks to "constitutionally protected privacy of speech" whether the asserted threats are foreign or domestic. Both forms of surveillance can produce the "indiscriminate wiretapping and bugging of law-abiding citizens" that the *Keith* Court feared. *See Keith*, 407 U.S. at 320–21; *see also* S. Rep. No. 95-701 at 15, *reprinted* at 1978 U.S.C.C.A.N. 3973, 3984 (stating Senate Intelligence Committee's judgment that the arguments in favor of prior judicial review "apply with even greater force to foreign counterintelligence surveillance"). The risks are still greater if, as under the FAA, there is no requirement that the government's surveillance activities be directed at specific foreign agents, or subject to individualized judicial review.

Second, the courts are just as capable of overseeing foreign intelligence surveillance of U.S. persons' communications as they are of overseeing domestic intelligence surveillance of their communications. Indeed, for the past thirty-five years, the courts *have* been overseeing intelligence surveillance relating to agents of foreign powers because, since its enactment in 1978, FISA has required the government to obtain individualized judicial authorization—based on probable cause that the target is an agent

of a foreign power—before conducting foreign intelligence surveillance inside the nation's borders. There is nothing unworkable about FISA's core requirement of judicial authorization. Since 1978, the FISC has granted more than 33,000 surveillance applications submitted by the executive branch, and the government has brought dozens of prosecutions based on evidence obtained through FISA. *See, e.g.*, Foreign Intelligence Surveillance Act Orders 1979–2012, Elec. Privacy Info Ctr., http://bit.ly/LoZqZG; FISA Annual Reports to Congress 1979–2007, Foreign Intelligence Surveillance Act, Fed'n of Am. Scis. http://bit.ly/1cvnUef; *United States v. Sattar*, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (collecting cases). The country's experience with FISA shows also that judicial oversight can operate without compromising the secrecy that is necessary in the intelligence context.

Thus, there is no basis to conclude that the warrant and probable cause requirement is unworkable here. Moreover, other factors weigh against recognizing a special needs exception to the warrant requirement in this context. Most significantly, special needs exceptions have generally been recognized only in contexts in which the search in question was minimally intrusive and the discretion of executive officers was strictly confined. *See, e.g.*, *Skinner v. Railway Labor Execs.' Ass'n*, 489 U.S. 602, 624 (1989). This is not such a context. Surveillance under the FAA is exceptionally intrusive, and it is conducted by executive officers who enjoy broad authority to decide whom to monitor, when, and for how long.

c. Even if a foreign intelligence exception to the warrant requirement exists, it is not broad enough to make the FAA constitutional.

Even if the government's need to gather intelligence about security threats with a foreign nexus constitutes a special need justifying an exception to the warrant requirement, any such exception is not broad enough to render FAA surveillance constitutional.

Following *Keith*, the circuit courts split on the question of whether warrantless surveillance for foreign intelligence purposes could ever be constitutional. While the Tenth Circuit has never addressed the question, the D.C. Circuit has suggested that a warrant should be required even for foreign intelligence surveillance directed at suspected foreign powers and agents. *Zweibon v. Mitchell*, 516 F.2d 594, 614 (D.C. Cir. 1975) (stating in *dicta* that "we believe that an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional"); *see Berlin Democratic Club v. Rumsfeld*, 410 F. Supp. 144, 159 (D.D.C. 1976). Several other circuit courts have held that warrantless surveillance for foreign intelligence purposes is constitutional in some circumstances. *See, e.g.*, *United States v. Truong Dinh Hung*, 629 F.2d 908, 912–15 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 604–05 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973). Crucially, however, all these cases involved surveillance conducted before the enactment of FISA in 1978, and FISA seriously

undermines their rationale. *See United States v. Bin Laden*, 126 F. Supp. 2d 264, 272, 274 nn.8–9 (S.D.N.Y. 2000). As discussed above, FISA demonstrates that the mere fact that the government's surveillance is conducted for foreign intelligence purposes does not render the warrant and probable cause requirements unworkable.

Perhaps more important here, the courts that recognized a foreign intelligence exception to the warrant requirement have defined that exception very narrowly. They excused the government from compliance with the warrant requirement only where the surveillance in question was directed at a specific foreign agent or foreign power. *See, e.g., Truong*, 629 F.2d at 915–16; *United States v. Ehrlichman*, 546 F.2d 910, 925 (D.C. Cir. 1976); *Bin Laden*, 126 F. Supp. 2d at 277. They required that the government's "primary purpose" be to gather foreign intelligence information. *See, e.g., Truong*, 629 F.2d at 916. And they required that the surveillance be personally approved by the President or Attorney General. *See, e.g.*, *Ehrlichman*, 546 F.2d at 926 ("Unless carefully circumscribed, such a power is easily subject to abuse."); *Bin Laden*, 126 F. Supp. 2d at 277.

The FAA contains none of these limitations—it permits warrantless surveillance in circumstances far removed from those that have previously been held to fall within the foreign intelligence exception. Surveillance under the FAA is not directed only at foreign powers and their agents; FAA surveillance operates at a wholesale level, allowing the government to collect and search the international communications of U.S. persons in bulk. Nor does the FAA require that warrantless surveillance be personally approved by

the President or the Attorney General. The Attorney General has a role in authorizing FAA surveillance, but this role involves approval of the overall procedures, not individual targets. *See* 50 U.S.C. § 1881a.

Nor, finally, does the FAA require that the government's "primary purpose" be to collect foreign intelligence information. To the contrary, it allows the government to engage in warrantless surveillance even when its primary purpose is to gather evidence of criminal activity rather than to collect foreign intelligence information. *See* 50 U.S.C. § 1881a(g)(2)(A)(v) (permitting warrantless surveillance where gathering foreign intelligence information is simply a "significant purpose" of the interception). The possibility that FAA surveillance will be coopted for ordinary law enforcement surveillance is particularly acute, because the statute's "significant purpose" requirement only attaches at the broad, *programmatic* level. *See* 50 U.S.C. § 1881a(g)(2)(A)(v). Unlike under FISA, 50 U.S.C. §§ 1804(a)(5), 1805(c)(1)(C), the government is not required to have a significant foreign intelligence purpose focused on the specific targets and facilities it ultimately chooses to monitor.

3. The FAA violates the Fourth Amendment's requirement of reasonableness.

The FAA would be unconstitutional even if the warrant clause were inapplicable because "the ultimate touchstone of the Fourth Amendment is reasonableness"—a test the FAA fails. *See Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (quotation marks omitted). The reasonableness requirement applies even where the warrant requirement

does not. *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985); *see In re Sealed Case*, 310 F.3d 717, 737 (FISCR 2002) (assessing reasonableness of FISA); *Figueroa*, 757 F.2d 466, 471–73 (2d Cir. 1985) (Title III); *United States v. Duggan*, 743 F.2d 59, 73–74 (2d Cir. 1984) (assessing reasonableness of FISA); *United States v. Tortorello*, 480 F.2d 764, 772–73 (2d Cir. 1973) (Title III). Reasonableness is determined by examining the "totality of circu[m]stances" to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169–70 (2008).

In the context of electronic surveillance, reasonableness requires that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions of privacy." *Berger*, 388 U.S. at 58 (quotation marks omitted); *see United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973) ("[W]e must look . . . to the totality of the circumstances and the overall impact of the statute to see if it authorizes indiscriminate and irresponsible use of electronic surveillance or if it authorizes a reasonable search under the Fourth Amendment."). Courts that have assessed the lawfulness of electronic surveillance have looked to FISA and Title III as measures of reasonableness. *See, e.g.*, *United States v. Mesa-Rincon*, 911 F.2d 1433, 1438 (10th Cir. 1990) (evaluating reasonableness of video surveillance); *United States v. Biasucci*, 786 .2d 504, 510 (2d Cir. 1986) (same); *United States v. Torres*, 751 F.2d 875, 884 (7th Cir.

1984) (same). While the constitutional limitations on foreign intelligence surveillance may differ in some respects from those applicable to law enforcement surveillance, *see Keith*, 407 U.S. at 323–24, "the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns," *In re Sealed Case*, 310 F.3d at 737.

a. The FAA exposes every U.S. person's international communications to the possibility of warrantless surveillance.

By abandoning the core requirements of the warrant clause—individualized suspicion, prior judicial review, and particularity—the FAA eliminates the primary protections against general surveillance. Whereas both FISA and Title III require the government to identify to a court its targets and the facilities it intends to monitor, the FAA does not. Whereas both FISA and Title III require the government to demonstrate individualized suspicion to a court, the FAA does not. (Indeed, the FAA does not require even an *administrative* finding of individualized suspicion.) And, whereas both FISA and Title III impose strict limitations on the nature of the communications that the government may monitor and the duration of its surveillance, the FAA does not. The FAA's failure to include these basic safeguards is fatal, because these are the very safeguards that the courts have cited in upholding the constitutionality of both FISA and Title III. *See, e.g.*, *Duggan*, 743 F.2d at 73 (FISA); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (FISA); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (FISA); *In re Sealed Case*, 310 F.3d at 739–40 (FISA); *In re Kevork*, 634 F.

Supp. 1002, 1013 (C.D. Cal. 1985) (FISA), *aff'd*, 788 F.2d 566 (9th Cir. 1986); *United States v. Falvey*, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (FISA); *Tortorello*, 480 F.2d at 773–74 (Title III); *Bobo*, 477 F.2d at 982 (Title III); *United States v. Cafero*, 473 F.2d 489, 498 (3d Cir. 1973) (Title III).

The consequence of the FAA's failure to include any of these limitations is that the government may target effectively any foreigner for surveillance—even where another party to the communication is a U.S. person. Unlike Title III (in which the government's surveillance targets must be criminal suspects, *see* 18 U.S.C. § 2518(1), (3)) and FISA (in which the surveillance targets must be agents of a foreign power, *see* 50 U.S.C. § 1804(3)), the FAA permits the surveillance of *any* foreigner abroad. 50 U.S.C. § 1881a(d). This sweeping authorization ensures that the communications of countless innocent U.S. persons will be monitored. Indeed, allowing the government to acquire U.S. persons' international communications was the very purpose of the FAA. *See* Hayden SJC Statement.

For U.S. persons whose international communications are swept up by FAA surveillance, such as Mr. Muhtorov, the sole protection is the FAA's requirement that the government "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); *see* 50 U.S.C. § 1881a(e). This requirement, however, does not apply to communications that contain "foreign intelligence information." *Id*. Moreover, the statute's definition of "foreign intelligence information" is extraordinarily broad,

encompassing not just information relating to terrorism, but information relating to "the conduct of the foreign affairs of the United States." *See* 50 U.S.C. § 1881(a); *id.* § 1801(e).

In short, the FAA's targeting and minimization requirements permit the government to target any foreigner abroad for surveillance and to acquire and retain any U.S. persons' international communications with (or about) those foreigners that relate to "the conduct of the foreign affairs of the United States." *See* U.S.C. § 1801(e). In this way, the FAA exposes virtually every international communication—including those with one end in the United States—to the possibility of warrantless surveillance.[13]

As touched on earlier, publicly available information about the targeting and minimization procedures that has been used by the government confirms the statute's defects. *See generally* 2009 Targeting Procedures; 2011 Minimization Procedures. These

---

[13] The FAA exposes even purely domestic communications to the possibility of surveillance as well. The FAA requires the government 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." 50 U.S.C. § 1881a(d)(1)(B) (emphasis added). In other words, the statute permits the government to collect any communication so long as it does not know for a fact that all parties to the communication are located inside the United States. This likely has had dramatic implications for the privacy of American residents' purely domestic communications, as even the executive itself has indicated that uncertainty about location is the rule rather than the exception. *See, e.g.*, *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II): Hearing Before the H. Judiciary Comm. on the Foreign Intelligence Surveillance Act and Protect America Act*, 110th Cong. 92 (2007) (statement of DNI McConnell) ("Sir, in the old days, Cold War days, location was much, much easier. Today, with mobile communications, it is more difficult. . . . There are some keys that can assist, but we can't know for certain[]."). On one occasion, the FISC held that the government's minimization procedures were unconstitutional because they resulted in the collection of "a very large number" of purely domestic communications. *[Redacted]*, 2011 WL 10945618, at *28 (FISC Oct. 3, 2011).

procedures give effect to the statute's design by allowing the government to collect U.S. persons' international communications in the course of surveillance directed at foreign targets. They allow the government to search literally every international communication going into or out of the United States for information "about" its targets, so long as it uses "an Internet Protocol filter to ensure that" one of the parties to the communication "is located overseas." 2009 Targeting Procedures 1–2; *see also* Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1cez5ZK. Those same procedures also reveal that among the factors that government analysts examine to determine whether a particular email address or phone number will be used to communicate foreign intelligence information is whether it has been used in the past to communicate with "an individual associated with a foreign power or foreign territory"—a definition broad enough to encompass essentially any foreign person. 2009 Targeting Procedures 4.

The procedures also explicitly permit the retention and dissemination of U.S. persons' international communications if "necessary to understand foreign intelligence information or assess its importance." 2011 Minimization Procedures § 6(a)(2), (b)(2). They permit the government to retain purely domestic communications acquired through the accidental targeting of U.S. persons if the government determines that they contain "significant foreign intelligence information" or "evidence of a crime." *Id.* § 5(1)–(2). U.S. persons' communications that do not contain foreign intelligence or evidence of a crime may be retained for up to five years. *Id.* § 3(b)(1). Even communications identified

as "attorney–client" communications may be retained to "preserv[e] foreign intelligence information contained therein." *Id*. § 4. Finally, the minimization procedures allow so-called "backdoor searches," in which the government later searches communications acquired under the FAA specifically for information about U.S. persons—like Mr. Muhtorov—for any reason whatsoever. *See id.* § 3(b)(6).

As codified and as implemented, the FAA's targeting and minimization requirements—in permitting nearly unfettered surveillance of U.S. persons' international communications—bear little resemblance to the procedures in place under Title III and FISA. *See, e.g.*, *In re Sealed Case*, 310 F.3d at 740–41 (stating that courts have found FISA's minimization requirements to be "constitutionally significant"); *Pelton*, 835 F.2d at 1075 (similar); *Duggan*, 743 F.2d at 74 (similar); *United States v. Turner*, 528 F.2d 143, 156 (9th Cir. 1975) (finding Title III constitutional because, among other things, "measures [must] be adopted to reduce the extent of . . . interception [of irrelevant or innocent communications] to a practical minimum"); *Figueroa*, 757 F.2d at 471 (similar).

Title III requires the government to conduct surveillance "in such a way as to minimize the interception of" innocent and irrelevant conversations, 18 U.S.C. § 2518(5); *see id.* (stating that "every order and extension thereof shall contain a provision" regarding the general minimization requirement), and strictly limits the use and dissemination of material obtained under the statute, *see* 18 U.S.C. § 2517. FISA similarly requires the government to minimize the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons. *See* 50

U.S.C. § 1801(h). It requires that each order authorizing surveillance of a particular target contain specific minimization procedures that will govern that particular surveillance. *See* 50 U.S.C. § 1804(a)(4); 50 U.S.C. § 1805(a)(3); 50 U.S.C. § 1805(c)(2)(A). FISA also specifically provides the FISC with authority to oversee the government's minimization on an individualized basis during the course of the actual surveillance. *See* 50 U.S.C. § 1805(d)(3); *see also* 18 U.S.C. § 2518(6). Thus, under FISA, minimization is required with respect to every individual surveillance target, and, equally important, minimization s judicially supervised during the course of the surveillance.[14]

The targeting and minimization procedures under the FAA are problematic for still other reasons. Unlike the privacy protections in Title III and FISA, the FAA's targeting and minimization procedures are neither individualized nor subject to ongoing judicial supervision. Under the FAA, minimization is not individualized but programmatic: Minimization procedures apply not to surveillance of specific targets but rather to surveillance *programs*, the specific targets of which may be known only to the executive branch. Moreover, the FISC is granted no authority to supervise the government's compliance with the minimization procedures during the course of an acquisition or even to inquire about the treatment of U.S. persons' communications. *Compare with* 50 U.S.C.

---

[14] *See* Kris & Wilson § 9:1–2 (explaining that "each FISA application must describe specific minimization procedures that the Attorney General believes are appropriate for the particular surveillance or search in question," that "the FISC may modify the proposed minimization procedures," that the order "must direct that the (modified) procedures be followed . . . in conducting the surveillance," and that the FISC "enjoys the authority to review the government's compliance with minimization procedures").

§ 1805(d)(3). Nor is there any requirement that the government seek judicial approval before it analyzes, retains, or disseminates U.S. communications. *Compare with* 50 U.S.C. § 1801(h)(4) (requiring court order in order to "disclose[], disseminate[], use[] . . . or retain[] for longer than 72 hours" U.S. communications obtained in the course of warrantless surveillance of facilities used exclusively by foreign powers).

The FAA's meager minimization provisions are especially problematic because the FAA does not provide for individualized judicial review at the acquisition stage. Under FISA and Title III, minimization operates as a second-level protection against the acquisition, retention, and dissemination of information relating to U.S. persons. The first level of protection comes from the requirement of individualized judicial authorization for each specific surveillance target. *Cf. Scott v. United States*, 436 U.S. 128, 130–31 (1978) ("'The scheme of the Fourth Amendment becomes meaningful only when it is assured that at some point the conduct of those charged with enforcing the laws can be subjected to the more detached, neutral scrutiny of a judge who must evaluate the reasonableness of a particular search or seizure in light of the particular circumstances.'" (quoting *Terry v. Ohio*, 392 U.S. 1 (1968))); *United States v. James*, 494 F.2d 1007, 1021 (D.C. Cir. 1971) ("The most striking feature of Title III is its reliance upon a judicial officer to supervise wiretap operations. Close scrutiny by a federal or state judge during all phases of the intercept, from the authorization through reporting and inventory, enhances the protection of individual rights." (quotation marks omitted)); *Cavanagh*, 807 F.2d at 790.

Under the FAA, by contrast, there is no first-level protection, because the statute does not call for individualized judicial authorization of specific surveillance targets (or, for that matter, of specific facilities to be monitored or specific communications to be acquired). Unlike FISA and Title III, the FAA permits dragnet surveillance - the mass acquisition of Americans' international telephone calls and emails. In this context, minimization requirements should be at least as stringent as they are in the context of FISA surveillance of facilities used exclusively by foreign powers. *See* 50 U.S.C. § 1801(h)(4).

b. The FAA lacks other basic protections.

The FAA is also unreasonable insofar as it permits the government to conduct dragnet surveillance of international communications so long as "a significant purpose of the acquisition is to obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v). This relaxed purpose standard allows the government to engage in FAA surveillance even if its *primary* purpose is to discover evidence of criminal activity.

As explained above, the Supreme Court and circuit courts have generally permitted departures from the Fourth Amendment's ordinary requirements only where the government's *primary* purpose is to collect foreign intelligence information. *See Truong*, 629 F.2d at 915–16; *Butenko*, 494 F.2d at 606; *Brown*, 484 F.2d at 427 (Goldberg, J., concurring); *see also United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (stating that "the investigation of criminal activity cannot be the primary purpose of the surveillance" and that FISA may "not . . . be used as an end-run around the Fourth

Amendment's prohibition of warrantless searches"); *Pelton*, 835 F.2d at 1067 interpreting purpose" to mean "primary purpose"); *United States v. Megahey*, 553 F. Supp. 1180 (E.D.N.Y. 1982), *aff'd sub nom.*, *Duggan*, 743 F.2d at 59. While some courts have upheld FISA despite Congress's amendment of it to permit surveillance so long as a "significant purpose" of that surveillance is to gather foreign intelligence, *see, e.g.*, *In re Sealed Case*, 310 F.3d at 742–44; *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 306–09 (D. Conn. 2008), at least one court has found that the amendment renders FISA unconstitutional, *Mayfield v. United States*, 504 F. Supp. 2d 1037 (D. Or. 2007), *vacated*, 599 F.3d 964 (9th Cir. 2010) (*en banc*).

Whether or not the "significant purpose" standard is constitutional in the context of FISA, the standard is unreasonable in the context of FAA surveillance. The FAA's purpose requirement—unlike FISA's purpose requirement—applies not to individualized particularized surveillance orders but to entire programs of surveillance. Under the FAA, the government must certify that a significant purpose of a mass-acquisition order is to gather foreign intelligence information, but once the FISC has endorsed that acquisition, the government may target particular individuals primarily, or entirely, for the purpose of collecting evidence of criminal activity. Because the FISC may not review on an individualized basis the government's purpose in targeting particular individuals or groups under the FAA, no court has ever reviewed the purpose of the FAA surveillance of the sort that resulted in the interception of Mr. Muhtorov's communications.

B. The FAA violates Article III of the Constitution.

The FAA violates Article III because it authorizes the FISC to issue mass-acquisition orders in the absence of any case or controversy and requires the court to review the legality and constitutionality of the government's programmatic procedures in the abstract.

The Constitution "extend[s]" the judicial power of the United States to only "cases" and "controversies." U.S. Const. art. III, § 2. That requirement is a condition precedent to the exercise of judicial authority, "restrict[ing]" federal courts to the "resolution of concrete disputes between the parties before them." *Sec'y of State of Md. v. Joseph H. Munson Co., Inc*., 467 U.S. 947, 976 (1984); *accord Massachusetts v. EPA*, 549 U.S. 497, 516 (2007); *see also Chi. & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 113 (1948) (Article III forbids federal courts from issuing "advisory opinions[,] even when asked by the Chief Executive."). In other words, courts may pass only upon particularized issues capable of judicial resolution—"flesh-and-blood legal problems with data relevant and adequate to an informed judgment." *New York v. Ferber*, 458 U.S. 747, 768 (1982) (quotation marks omitted). Conversely, courts are without the power to issue "abstract declaration[s] of the law," *In re Summers*, 325 U.S. 561, 566–67 (1945) (quotation marks omitted), or adjudicate legal questions based "upon a hypothetical state of facts," *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 241 (1937). *See* Felix Frankfurter*, A Note on Advisory Opinions*, 37 Harv. L. Rev. 1002, 1005 (1937) ("Facts and facts again are decisive."); *see also Flast v. Cohen*, 392 U.S. 83, 97 (1968); *Citizens*

Concerned for Separation of Church & State v. City & Cnty. of Denver, 628 F.2d 1289, 1295 (10th Cir. 1980); *United States v. Smith*, 686 F. Supp. 847, 855 (D. Colo. 1988) (Kane, J.) ("Discharging tasks other than the deciding of cases and controversies would 'involve the judges too intimately in the process of policy and thereby weaken confidence in the disinterestedness of their judicatory functions'").

The FAA assigns to an Article III court a role that is fundamentally incompatible with the case-or-controversy requirement. Under the FAA scheme, the government asks the FISC to approve programmatic surveillance orders that will result in the mass acquisition of Americans' communications without any individualized review or approval of the government's monitoring activity. The FISC's role is limited to evaluating in a vacuum whether the government's proposed targeting and minimization procedures comply with the statute and the Constitution, without any concrete factual context relating to particular targets. Article III "admonishes federal courts . . . to abstain from entangling themselves in abstract disagreements," *Keyes v. Sch. Dist. No. 1*, 119 F.3d 1437, 1443 (10th Cir. 1997) (quotation marks omitted), but engagement with abstraction is exactly what the FAA demands. And while Article III only "embraces application of principles of law or equity to facts," *Vermont v. New York*, 417 U.S. 270, 277 (1974), the FAA calls for n abstract assessment of the general rules that will govern a surveillance program to be implemented entirely by the executive branch.

It is instructive that, in rejecting Article III challenges to the *traditional* FISA process, courts have pointed to the fact that the traditional FISA process is a

particularized one—that it involves the court's consideration of concrete facts about the specific person to be monitored, the facilities to be targeted, and the purpose of the surveillance. For example, in *Megahey*, the court rejected an Article III challenge to a traditional FISA order because "[a]pplications 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." 553 F. Supp. at 1197; *see id.* ("The FISC judge who is faced with a [traditional FISA] 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." (emphasis added)); *see also United States v. Falvey*, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982); *see In re Kevork*, 634 F. Supp. 1002.

The Office of the Legal Counsel ("OLC") relied on the same reasoning in defending the constitutionality of FISA in the debate preceding that statute's enactment in 1978. Key to the OLC's analysis was the fact that the FISC would be able to "apply standards of law to the facts of a particular case" in the form of probable cause determinations akin to those "made in other warrant proceedings." Memorandum from John M. Harmon, Assistant Att'y Gen., OLC, to Hon. Edward P. Boland, Chairman, House Permanent Select Comm. on Intelligence (Apr. 18, 1978), *reprinted in Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and*

H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence, 95th Cong. 26, 28 (1978).

Thus, as both the judicial and executive branches have recognized, a traditional FISA order presents the court with a concrete question about a particular proposed interception. By contrast, a mass-acquisition order under the FAA demands only a broad assessment of whether the government's minimization and targeting procedures are reasonable—a question asked and answered at the highest level of generality without reference to particular persons or facilities. That question is simply not a case or controversy appropriate for judicial resolution under Article III.

II. Mr. Muhtorov is entitled to discovery concerning the government's interception of his communications under the FAA.

Although Mr. Muhtorov challenges the constitutionality of FAA surveillance in this motion, the government has not provided him with material that would enable him to raft a challenge to the specific manner in which the FAA was used in his case. In order for this Court to "make an accurate determination of the legality of the surveillance," 50 U.S.C. § 1806(f), and as required by due process, *id*. § 1806(g); *Brady v. Maryland*, 373 U.S. 83 (1963), it should order disclosure of information including but not limited to: the government's applications to the FISC seeking authorization for, and the FISC's orders authorizing, the FAA surveillance that intercepted communications to or from Mr. Muhtorov; notice of all communications to or from Mr. Muhtorov intercepted under the FAA; all evidence obtained under the FAA that the government intends to use at trial or

that is material to Mr. Muhtorov's defense; all evidence derived from communications intercepted under the FAA that the government intends to use at trial; and records indicating how Mr. Muhtorov's communications were intercepted and identified under the FAA or were derived from communications collected under the FAA. *See* Part II.B, *infra*.

A. Disclosure of additional information is required by FISA and the due process clause.

The government's notice of its intent to use information obtained or derived from FAA surveillance contains only a bare recitation of the statutory language requiring the notice, 50 U.S.C. § 1806(c). *See* Doc. 457. The notice is insufficient to allow Mr. Muhtorov to craft a suppression motion addressed to the specific FAA surveillance to which he was subjected. FISA provides two vehicles for correcting this deficiency.

First, even where the Attorney General has certified that disclosure of materials relevant to a motion to suppress would harm the national security, FISA provides that "the court may disclose to the aggrieved person, 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). Second, even where section 1806(f) does not mandate disclosure, the statute requires disclosure "to the extent that due process requires" it, 50 U.S.C. § 1806(g), thus expressly incorporating the protections of the Fifth Amendment's due process clause. Here, disclosure is required for both reasons.

1. Disclosure is necessary to make an accurate determination of the legality of the surveillance in light of the complexity of the issues and the lack of prior judicial interpretation of the FAA.

Mr. Muhtorov's challenge presents legal issues of first impression and factual issues of significant complexity. Resolution of unique and "complex" questions justifies disclosure of information to defense counsel to facilitate an informed adversarial process. *See United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982). No federal court has yet addressed the constitutionality of FAA surveillance.[15] Indeed, as discussed above, Mr. Muhtorov's case is the first in which a defendant has received the statutorily required notice that evidence obtained or derived from FAA surveillance will be used against him. In light of the complexity of the issues and the dearth of judicial interpretation of section 1881a, disclosure is warranted.

The issues before the Court are many and complicated. It must evaluate whether the order or orders authorizing the FAA surveillance of Mr. Muhtorov comply with the Fourth Amendment and section 1881a, and whether the government's applications to the FISC seeking those orders contained material omissions or misrepresentations or were otherwise deficient. *Cf. Franks v. Delaware*, 438 U.S. 154 (1978).

---

[15] The FISC itself believes it lacks the power to address the facial validity of the FAA. *See In re Proceedings Required by § 702(I) of FISA Amendments Act of 2008*, No. Misc. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008) (stating that its role in reviewing the FAA is "narrowly circumscribed," with its mandate limited to accepting or rejecting "the certification, the targeting procedures and the minimization procedures" provided by the government (quotation marks omitted)).

This Court must further determine whether the targeting and minimization procedures in use at the time the government obtained Mr. Muhtorov's communications complied with the Fourth Amendment and section 1881a, whether the government complied with those procedures, and whether the methods used to collect, identify, and search Mr. Muhtorov's communications were lawful. It must determine whether Mr. Muhtorov's communications were obtained via "to/from" or "about" searches of targeted communications, whether the selectors for which the government searched were consistent with the FAA's requirements (e.g., whether they were identified with a non–United States person), whether Mr. Muhtorov's communications obtained pursuant to section 1881a were with a lawfully targetable non-U.S. person, and whether, if the communications were not properly obtained, they were inappropriately retained by the government and identified via later queries seeking selectors linked to Mr. Muhtorov or other individuals. Finally, it must assess whether other evidence derived, directly or indirectly, from the FAA surveillance must be suppressed as the fruit of an unconstitutional search. *See Wong Sung v. United States*, 371 U.S. 471, 487–88 (1963); *United States v. Carson*, 793 F.2d 1141, 1147–48 (10th Cir. 1986). Answering the latter question will involve determining whether the applications for traditional FISA warrants were tainted by information unconstitutionally obtained pursuant to the FAA.

Not only are these questions factually and legally complex, but this Court must answer them without the aid of precedent. No court has substantively ruled on a motion to suppress FAA-obtained or -derived surveillance (nor on an affirmative civil challenge to

such surveillance), setting this case apart from those that involved traditional FISA surveillance in which courts have denied disclosure under section 1806(f). In traditional FISA cases, courts can look to a significant body of case law assessing the constitutionality of the FISA scheme and providing factors with which to evaluate FISA applications and orders. *See, e.g., United States v. Duka*, 671 F.3d 329, 336–47 (3d Cir. 2011); *United States v. Abu-Jihaad*, 630 F.3d 102, 117–31 (2d Cir. 2010); *United States v. Hammoud*, 381 F.3d 316, 332–34 (4th Cir. 2004), *vacated on other grounds*, 543 U.S. 1097 (2005).

In such cases, courts have found that "review of the FISA materials . . . [was] relatively straightforward and not complex," and therefore *ex parte*, *in camera* consideration was appropriate. *Abu-Jihaad*, 630 F.3d at 129 (brackets in original) (quotation marks omitted). *But see* Mem. Op. and Order at 3-5, *United States v. Daoud*, No. 12 cr 723 (N.D. Ill. Jan. 29, 2014) (granting criminal defendant's motion for disclosure of classified FISA materials). Here, however, the legal issues are complex and there is little guidance from other courts about how to evaluate the constitutionality of orders granting applications for FAA surveillance or actual execution of the surveillance. Disclosure of the requested information is therefore "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f).

Without disclosure, Mr. Muhtorov can challenge the FAA statutory scheme, as he does here, but he cannot assess the government's actual surveillance of him. Nor can he participate in the adversarial process to inform this Court's evaluation of these issues.

The Supreme Court in *Amnesty* envisioned that a criminal case such as this one would provide the opportunity to test the constitutionality of particular FAA acquisitions. *See* 133 S. Ct. at 1154. But in order for this Court to provide the review, disclosure is required. It is entirely reasonable to assume Mr. Muhtorov would advance additional arguments regarding the legality of the government's surveillance of him if he understood what that surveillance entailed. Without disclosure, the Court, and Mr. Muhtorov, will lose the benefit of informed arguments from the defense on these issues.

2. Disclosure and an adversarial hearing is required in light of the government's repeated misrepresentations to the FISC.

In cases involving traditional FISA surveillance, courts of appeals have identified factors that would warrant disclosure of applications, warrants, and other materials under section 1806(f). Consistent with FISA's legislative history,

> disclosure is "necessary" only where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as "indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order."

Belfield, 692 F.2d at 147 (quoting S. Rep. No. 95–701, 95th Cong., 2d Sess. 64 (1978)); *accord United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987); *Duggan*, 743 F.3d at 78. Recent disclosures demonstrate that all of these infirmities have plagued FAA surveillance, including during the period when Mr. Muhtorov was surveilled.

Recently declassified FISC opinions show that the government has made a series of incomplete or inaccurate representations in its applications for approval of surveillance under the FAA and other FISA authorities, and that the government has repeatedly failed to comply with restrictions imposed by the FISC.

Most notably, one of those opinions held that FAA collection during the same period as the investigation of Mr. Muhtorov violated the Fourth Amendment. *See [Redacted]*, 2011 WL 10945618 (FISC Oct. 3, 2011). That opinion details the government's May 2011 disclosure to the FISC that, contrary to previous statements, the NSA was relying on the FAA to collect internet communications that are "wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection," and that the "government might lack confidence in the effectiveness" of its procedures for ensuring that FAA surveillance of internet transactions was being limited to targets actually located overseas. *Id.* at *2. In other words, "the government . . . advised the Court that the volume and nature of the information it [had] been collecting [was] fundamentally different from what the Court had been led to believe." *Id*. at *9. These disclosures "fundamentally alter[ed] the Court's understanding of the scope of collection conducted pursuant to Section 702." *Id*. at *5. The government's applications for authorization to conduct FAA surveillance thus contained all the problems that justify disclosure: "misrepresentation of fact, vague identification of the persons to be surveilled, [and collection of] surveillance records which include a significant amount of nonforeign intelligence information, calling into

question compliance with the minimization standards contained in [past] orders." *Belfield*, 692 F.2d at 147.

Again, these problems coincide temporally with the likely period of FAA surveillance in this case. The government notified the FISC of its FAA compliance problems in a May 2, 2011, letter. As discussed above, the government intercepted email and phone communications involving Mr. Muhtorov as early as January 29 of the same year. The criminal complaint in this case refers to communications between Mr. Muhtorov and a person located overseas on February 5, March 8, March 22–23, April 2, April 4, August 19, August 26, September 1, and September 4, 2011. Crim. Compl. ¶¶ 12–17, 26–27, Doc. 1.

The criminal complaint does not indicate under what authority the surveillance was carried out, nor whether any of Mr. Muhtorov's communications were intercepted or obtained prior to January 29, 2011, under section 1881a or another FISA authority. It appears from these facts, however, that Mr. Muhtorov's communications were collected pursuant to section 1881a in early 2011, in the months immediately preceding (and possibly continuing after) the government's disclosure to the FISC that it was operating its FAA collection in a manner other than what the FISC had approved.

The government submitted incorrect and misleading information to the FISC on other occasions, as well. As Judge Bates explained, "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial

misrepresentation regarding the scope of a major collection program." *[Redacted]*, 2011 WL 10945618, at *30 n.14; *see also In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted]*, No. BR 09-13, 2009 WL 9150896, at *2 (FISC Sept. 25, 2009) (Walton, J.) ("The Court is deeply troubled by the incidents described above, which have occurred only a few weeks following the completion of an 'end to end review' by the government of NSA's procedures and processes for handling the BR metadata, and its submission of a report intended to assure the Court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems in this matter and had taken the necessary steps to ensure compliance with the Court's orders going forward."); *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9150913 (FISC Mar. 2, 2009) (Walton, J.) (detailing "misrepresentations to the Court" and "violations of its Orders"); *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9157881, at *2 (FISC Jan. 28, 2009) (Walton, J.) ("The Court is exceptionally concerned about what appears to be a flagrant violation of its Order in this matter . . . ."); *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620–21 (FISC 2002) (Lamberth, J.) (explaining government's "errors related to misstatements and omissions of material facts" in FISA applications), *abrogated on other grounds, In re Sealed Case*, 310 F.3d 717.

The errors in the government's applications to the FISC, including its applications for FAA surveillance authorization, were not merely "typographical or clerical in nature."

United States v. El-Mezain, 664 F.3d 467, 566 (5th Cir. 2011) (quotation marks omitted). Rather, "the errors were . . . pervasive enough to confuse the court as to the quantity or quality of the evidence described in the applications," such that "disclosing the applications and related materials to defense counsel would assist the court in making an accurate determination of the legality of the surveillance." *Id*. at 567 (quotation marks omitted). Moreover, because numerous FISC opinions—including opinions authorizing FAA surveillance—remain classified, counsel for Mr. Muhtorov have no way to know the full extent of any government misrepresentations or omissions in its applications to the FISC or of its noncompliance with FISC orders. Disclosure under section 1806(f) is necessary to enable the robust adversarial testing that accurate review of these issues requires.

Any misrepresentations in the applications that led to the orders under which Mr. Muhtorov's communications were seized also provide a basis for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154. "Under *Franks*, a hearing on the veracity of the affidavit supporting a warrant is required if the defendant makes a substantial showing that the affidavit contains intentional or reckless false statements and if the affidavit, purged of its falsities, would not be sufficient to support a finding of probable cause." *United States v. Kennedy*, 131 F.3d 1371, 1376 (10th Cir. 1997). *Franks* permits challenges to "material omissions[] as well as affirmative falsehoods," *id*. (quotation marks omitted), and applies to applications for electronic surveillance orders as well as those seeking Rule 41 warrants, *United States v. Green*, 175 F.3d 822, 828 (10th Cir.

1999); *see Duggan*, 743 F.3d at 77 n.6. Given the record of affirmative misrepresentations and omissions made by the government in its applications for section 1881a authorizations (as well as its misrepresentations and omissions in applications for orders authorizing other forms of FISA surveillance), an adversarial hearing is required to assess whether the fruits of those authorizations must be suppressed.

3. Disclosure is required because information about applications, orders, and fruits of FAA surveillance are helpful to Mr. Muhtorov's suppression motion and defense.

The information sought by Mr. Muhtorov is relevant both to his motion to suppress the fruits of unconstitutional FAA surveillance, and to the adjudication of his guilt and punishment. Evidence must be turned over under *Brady* if it is favorable to the defense—in other words, if it is "exculpatory or impeaching." *Browning v. Trammell*, 717 F.3d 1092, 1094 (10th Cir. 2013). The due process rights embodied in *Brady* apply both to trials and to motions to suppress. *United States v. Barton*, 995 F.2d 931, 935 (9th Cir. 1993); *Smith v. Black*, 904 F.2d 950, 965 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992); *see also United States v. Johnson*, No. 96-2008, 117 F.3d 1429, at *2 (10th Cir. 1997) (unpublished table opinion) (assuming that *Brady* applies at motions to suppress).

The information and records requested in this motion will likely contain information favorable to Mr. Muhtorov's motion to suppress. For example, the government's applications to the FISC and the FISC's orders that led to the surveillance of Mr. Muhtorov will provide evidence that the FAA surveillance scheme approved by

the FISC and used to surveil Mr. Muhtorov violated the warrant clause and the requirements of section 1881a.[16] Information about what communications were surveilled and how and why they were obtained will indicate whether the government violated the targeting and minimization restrictions approved by the FISC, whether the search was unreasonable under the Fourth Amendment, and whether Mr. Muhtorov's communications were intercepted for a law enforcement purpose rather than a foreign intelligence one. The identification of Mr. Muhtorov's communications obtained through FAA surveillance, and any evidence derived from that surveillance, will allow the defense o identify the evidence that should be suppressed as the fruits of an unconstitutional search. All of the requested materials will provide grounds for impeaching declarations or testimony of government officials in opposition to this motion to suppress.

The information and records requested in this motion would likely be helpful to Mr. Muhtorov in mounting a defense at trial. The contents of any communications obtained under the FAA but not yet provided to the defense (or even described in the criminal complaint) may be exculpatory, and may provide innocent explanations for seemingly incriminating evidence. They may also provide grounds for impeaching the testimony of prosecution witnesses. Due process requires that all records favorable to Mr. Muhtorov, including records that are exculpatory or impeaching, must be disclosed.

---

[16] FISA provides for suppression of evidence on the grounds that "(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval." 50 U.S.C. § 1806(e); *see id.* § 1806(f)–(g).

4. If information helpful or material to the defense is classified, it must be disclosed or excluded.

The government violates due process when it withholds information or evidence from the defense as classified, but still seeks the benefit of the information in its prosecution:

> [T]he Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.

United States v. Reynolds, 345 U.S. 1, 12 (1953) (footnote omitted).

Some or all of the information sought by this motion as material to Mr. Muhtorov's defense, including the relevant applications to and orders of the FISC, is marked classified. Consistent with the principle set out in *Reynolds*, the Classified Information Procedures Act ("CIPA"), 18 U.S.C. app. III, provides a mechanism for accommodating both the government's interest in protecting classified information and the defendant's right to due process.

When the government makes a claim of privilege over classified information, a court must "decide whether the information is helpful or material to the defense." *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008). This is a low standard: "To be helpful or material to the defense, evidence need not rise to the level that would trigger the Government's obligation under *Brady v. Maryland* . . . to disclose exculpatory information. [I]nformation can be helpful without being 'favorable' in the *Brady* sense."

Id. (citations and quotation marks omitted). If information meets this standard, the government has four options: (1) disclose the material to defense counsel; (2) declassify the material and disclose it; (3) in some circumstances, provide an unclassified summary; or, (4) if it rejects the first three options, face exclusion of the material or dismissal of the prosecution. *See* 18 U.S.C. app. III at § 6(c), (e). These provisions function to "protect[ ] and restrict[ ] the discovery of classified information in a way that does not impair the defendant's right to a fair trial." *United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) (alterations in original) (quotation marks omitted).

CIPA thus provides this Court with the mechanism to honor Mr. Muhtorov's due process rights, as required by section 1806(g), without compromising the government's interest in protecting classified information. If the government declines to declassify the requested materials or produce an adequate unclassified summary, it must provide security clearances to Mr. Muhtorov's eligible counsel and disclose the materials under an appropriate protective order, as it has done in other prosecutions involving classified information.[17] *See, e.g.*, *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93, 116–18 (2d Cir. 2008); *see also United States v. Libby*, 467 F. Supp. 2d 20, 22 n.1, 24–25 (D.D.C. 2006). If the government fails to do so, it may not rely on evidence obtained or derived from FAA surveillance. Otherwise, a violation of Mr. Muhtorov's due process rights will result.

---

[17] If necessary to gain access to the materials requested in this motion, defense counsel are willing to receive security clearances and to abide by the requirements of those clearances and any additional restrictions imposed by protective orders of this Court.

5. *Ex parte* proceedings are inconsistent with the requirements of due process.

A failure to disclose to the defense the requested materials, resulting in *ex parte* proceedings on the legality of the FAA surveillance, would, under the circumstances of this case, be inconsistent with due process and the adversary process upon which this nation's justice system is premised.

The Supreme Court has recognized the necessity of adversarial proceedings to protect the rights of defendants and reach the correct outcome: "'[F]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.'" *United States v. James Daniel Good Real Prop.*, 510 U.S. 43, 55 (1993) (alterations in original) (quoting *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 170–72 (1951) (Frankfurter, J., concurring)). Indeed, "[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations" than an *ex parte* proceeding. *Am.-Arab Anti-Discrimination Comm. v. Reno*, 70 F.3d 1045, 1069 (9th Cir. 1995) (quotation marks omitted).

The guarantee of adversarial proceedings finds a source not only in the due process clause, but also in the Sixth Amendment's confrontation and assistance of counsel clauses. "'The central concern of the confrontation clause is to ensure the reliability of the evidence against a criminal defendant by subjecting it to rigorous testing in the context of

an adversary proceeding before the trier of fact.'" *United States v. Gomez*, 191 F.3d 1214, 1220 (10th Cir. 1999) (quoting *Lilly v. Virginia*, 527 U.S. 116 (1999)). Likewise, the Sixth Amendment "right to counsel is so fundamental to a fair trial, the Constitution cannot tolerate trials in which counsel, though present in name, is unable to assist the defendant to obtain a fair decision on the merits." *Evitts v. Lucey*, 469 U.S. 387, 395 (1985). When a defendant's counsel is denied access to material evidence and information, the defendant is denied a constitutionally adequate defense.

The Supreme Court has cautioned that "[i]n both the volume of the material to be examined and the complexity and difficulty of the judgments involved, cases involving electronic surveillance will probably differ markedly from those situations in the criminal law where in camera procedures have been found acceptable to some extent." *Alderman*, 394 U.S. at 182 n.14. Here, only by their direct, informed participation can defense counsel be confident that the court is made aware of material omissions or misrepresentations in the government's FISC submissions, evaluate the content of intercepted communications for exculpatory or otherwise material information, and enable adequate and accurate consideration by this Court.

The need for adversarial proceedings is highlighted by the failures of the FISC's initial *in camera*, *ex parte* authorization of the FAA surveillance that swept up Mr. Muhtorov's records. *See Franks*, 438 U.S. at 169 (explaining inadequacies of *ex parte* proceedings for issuing search warrants and explaining why defendants must be provided an opportunity to later challenge the adequacy and veracity of the government's arrant

applications in adversary proceedings). Many of the defects of the FISC's non-adversarial process are now on display. Recently declassified FISC opinions demonstrate not only a repeating pattern of government misrepresentations, but also repeated reprieves granted by the FISC as the government failed to meet successive deadlines to report to the FISC or to conform its surveillance to the law. *E.g.*, *[Redacted]*, 2011 WL 10945618, at *2–*3; *see also* Part II.A.2, *supra*. During these delays, the FISC failed to provide relief to persons subject to illegal surveillance by halting that surveillance for the duration of the government's noncompliance. Most importantly, relying on only the representations of the government, without adversarial testing, the FISC approved surveillance programs that turned out to be overly broad, in violation of statutory authority. *See* Part II.A.2, *supra*. The failure of *ex parte* proceedings to achieve fair and correct outcomes has resulted in calls—from members of Congress,[18] the President's blue ribbon panel on intelligence reform,[19] the Privacy and Civil Liberties Oversight Board,[20] and others—for appointment of an advocate to argue against the government in FISC proceedings. The

---

[18] *See, e.g.*, USA FREEDOM Act, H.R. 3361, 113th Cong. § 401 (2013), http://1.usa.gov/1mPQmsh (proposing creation of Office of the Special Advocate to "vigorously advocate before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, as appropriate, in support of legal interpretations that protect individual privacy and civil liberties").

[19] *See* President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World 200–05 (Dec. 12, 2013), http://1.usa.gov/1be3wsO.

[20] Privacy & Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 183–87 (Jan. 23, 2014), http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

President has agreed with the need for the FISC to "hear[] a broader range of privacy perspectives," and has proposed "the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court."[21]

Mr. Muhtorov understands the Court would, in any *in camera*, *ex parte* proceedings, make every effort to anticipate the arguments his attorneys might raise were they privy to the information sought in this motion and allowed to advocate for suppression on that basis. However, given the complex constitutional issues of first impression raised here, it would be particularly difficult—and inappropriate—for the Court to function as both advocate and judge. The Court would need to anticipate the defense arguments that seek a particular result, evaluate how secret evidence may or may not support that result, and then decide—without particularized briefing or pointed advocacy—whether the arguments it assumes would have been made are persuasive. In this case, as in any where an accused faces the loss of liberty, Mr. Muhtorov is entitled to have the lawyer defending him be his advocate, and to do everything possible to persuade the Court to grant the relief he seeks. *See* Mem. Op. and Order at 5, *United States v. Daoud*, No. 12 cr 723 (N.D. Ill. Jan. 29, 2014) (ordering disclosure of classified FISA materials because "an accurate determination of the legality of the surveillance is best made in this case as part of an adversarial proceeding").

---

[21] President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://1.usa.gov/1l2zOBS.

B. Mr. Muhtorov is entitled, at a minimum, to disclosure and discovery of the following materials and facts.

For the preceding reasons, Mr. Muhtorov respectfully seeks disclosure to the defense of the following information and records, with full opportunity for defense participation in any hearings pertaining to them:

1. Materials relating to the government's failure to provide Mr. Muhtorov with timely notice that it intended to introduce or otherwise use information obtained or derived from FAA surveillance in this proceeding, including copies of any documents setting out, or purporting to justify, the Justice Department's now-withdrawn policy of concealing the role of FAA surveillance from criminal defendants.
2. Materials indicating how Mr. Muhtorov's communications were intercepted and identified under the FAA, including the nature of the targeting and queries that led to their detection (e.g., whether the government conducted "to/from" searches or "about" searches, whether the government collected metadata or contents of communications, and what surveillance programs the government used to effect the collection).
3. Documents indicating which of Mr. Muhtorov's communications were intercepted under the FAA, and the contents those communications.
4. Documents indicating whether the fruits of FAA surveillance were used to justify further investigation of Mr. Muhtorov, or were used in applications

for additional surveillance authority, including under 50 U.S.C. § 1861(b)(2)(A) (Section 215), *id.* § 1842 (FISA pen-register and trap-and-trace provision), and 18 U.S.C. § 2709 (national security letters provision).

5. Intelligence reports and other materials produced in reliance on any of Mr. Muhtorov's communications collected under the FAA.

6. Documents indicating when and how the government established that Mr. Muhtorov was a U.S. person.

7. Applications, certifications, orders, and directives relating to the government's surveillance of Mr. Muhtorov under the FAA, including the applicable targeting and minimization procedures.

8. Applications, certifications, orders, and directives relating to the government's surveillance of Mr. Muhtorov under traditional FISA, in order to understand their reliance on FAA-obtained information.

9. Materials indicating which of Mr. Muhtorov's FAA-collected communications were disseminated to other agencies, including the FBI, and when they were disseminated.

CONCLUSION

The surveillance of Jamshid Muhtorov under the FAA was unconstitutional, and the fruits of that surveillance must be suppressed. In addition, Mr. Muhtorov asks the Court to order the disclosure of information that would permit him and the Court to understand the role that the FAA played in the government's investigation of him, and that would enable him to challenge the specific manner in which the FAA was used in his case.

Date: January 29, 2014

Respectfully submitted,

VIRGINIA L. GRADY
Federal Public Defender

/s/ Warren R. Williamson
WARREN R. WILLIAMSON
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, Colorado 80202
Telephone: (303) 294-7002
Fax: (303) 294-1192
Rick.Williamson@fd.org

/s/Brian Rowland Leedy
Brian Rowland Leedy
Assistant Federal Public Defender
633 Seventeenth Street
#1000
Denver, CO 80202
303-294-7002
Fax: 303-294-1192
Brian_Leedy@fd.org

/s/ Kathryn J. Stimson
Kathryn J. Stimson,
Attorney at Law
1544 Race Street
Denver, CO 80206
Telephone: (720) 638-1487
kathryn@stimsondefense.com

Attorneys for Jamshid Muhtorov

On the brief:

Jameel Jaffer
Alex Abdo
Patrick Toomey
Brett Max Kaufman
Nathan Freed Wessler
Attorneys at Law
American Civil Liberties Union Foundation
125 Broad St., 18th Floor
New York, NY 10004
Telephone: (212) 519-7816
Fax: (212) 549-2654
jjaffer@aclu.org

Mark Silverstein
Sara J. Rich
Attorneys at Law
ACLU Foundation of Colorado
303 E. 17th Avenue, Suite 350
Denver, Colorado 80203
Telephone: (303) 777-5482
Fax: (303) 777-1773
msilverstein@aclu-co.org

CERTIFICATE OF SERVICE

I hereby certify that on January 29, 2014, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following email address:

Gregory A. Holloway
Assistant U.S. Attorney
Email: gregory.holloway@usdoj.gov

Erin Martha Creegan
National Security Division for the U.S. Dept. of Justice
Email: erin.creegan@usdoj.gov

David B. Savitz, Esq., Counsel for Bakhtiyor Jumaev
Email: savmaster@aol.com

Mitchell Baker, Esq., Counsel for Bakhtiyor Jumaev
Email: mitchbaker@estreet.com

I hereby certify that I have mailed or served the document or paper to the following non CM/ECF participant in the manner (mail, hand-delivery, etc.) indicated by the non-participant's name:

Mr. Jamshid Muhtorov *(Via U.S. Mail)*

/s/ Warren R. Williamson
WARREN R. WILLIAMSON
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, Colorado 80202
Telephone: (303) 294-7002
Fax: (303) 294-1192
Rick.Williamson@fd.org

Attorney for Defendant