

**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 REPLY TO GOVERNMENT’S RESPONSE (DOC. 559, 569)

INTRODUCTION

Jamshid Muhtorov’s motion to suppress concerns the suspicionless and warrantless surveillance of a U.S. person’s international communications under the FISA Amendments Act (“FAA”). See Doc. 520.¹ This surveillance violated the Fourth Amendment because it occurred without a warrant, without individualized suspicion, and under a program that lacks the limitations that courts have deemed necessary for electronic-surveillance regimes to be reasonable. The surveillance also violated Article III of the Constitution because it proceeded under programmatic orders issued by the Foreign Intelligence Surveillance Court (“FISC”) absent any constitutional “case or controversy.” As a remedy, this Court should suppress the fruits of that surveillance.

¹ “Doc.” Refers to the Clerk’s Docket.

The Court should permit Mr. Muhtorov discovery of evidence that would be helpful and material to his defense and that would permit him to understand and challenge the role that the FAA played in the government's investigation of him.

Mr. Muhtorov will address each of the government's arguments made in its response. However, it is important not to lose sight of the broader import of the government's theory. The government's theory is that Americans have no constitutionally protected privacy interest in their international communications. *See* Doc. 559 at 35. To accept the government's arguments is to accept that the National Security Agency may collect Americans' international communications, individually or in bulk, "incidentally" or directly, without having to answer to the Constitution. Under the government's logic, the NSA may record every international phone call and copy every international text message and email. It may search those communications without limitation—for evidence of criminal activity, for foreign-intelligence information, or for anything else the government may be interested in learning. The government endeavors to obscure the implications of its theory; but to accept the theory is to accept a radically reimagined relationship between the governed and their government—one in which every cross-border missive, business transaction, or journalistic investigation takes place under the all-seeing and all-remembering gaze of the executive.

There is a narrower path—one that would accommodate the government's legitimate foreign-intelligence interests but also protect the privacy of innocent Americans and U.S. Persons. Congress could prohibit the government from intentionally

intercepting their international communications without a warrant, and require it to obtain a warrant retroactively to retain any such communications obtained unintentionally. Notably, then-Senator Obama proposed such a reform during the debate that preceded the enactment of the FAA. A foreign-intelligence scheme would not interfere with the government's ability to monitor foreign-to-foreign calls and emails, and it would permit the government to collect and retain Americans' international communications with judicial authorization. It would accommodate the government's legitimate interest without encroaching unnecessarily—and unconstitutionally—on the privacy rights of innocent Americans. The scheme Congress chose, however—the scheme under which Mr. Muhtorov's communications were surveilled—differs greatly from this one. It authorizes exactly the suspicionless surveillance the Constitution was meant to forbid.

ARGUMENT

I. THE GOVERNMENT'S SURVEILLANCE OF MR. MUHTOROV'S COMMUNICATIONS WAS UNCONSTITUTIONAL.

A. The government's surveillance of Mr. Muhtorov's communications violated the Fourth Amendment.

i. The "incidental overhear" rule does not render the warrant requirement inapplicable.

The government contends that "incidental capture of a U.S. person's communications during surveillance that lawfully targets non-U.S. persons abroad" does not engage the warrant clause. Doc. 559 at 38. But the rule the government cites—sometimes called the "incidental overhear" rule—has no application here.

First, the surveillance of Americans' communications under the FAA is not merely "incidental." Intelligence officials who advocated passage of the FAA (and of the Protect America Act ("PAA") before it) indicated that their principal aim was to allow the government broader authority to monitor Americans' international communications.² When legislators proposed language that would have required the government to obtain probable-cause warrants before accessing Americans' international communications, the White House issued a veto threat.³ One cannot reasonably say that the surveillance of Americans' communications under the FAA is "incidental" when permitting such surveillance was the purpose of the Act.

Nor can one reasonably say that the surveillance of Americans' international communications is "incidental" when the FAA allows large-scale collection of those communications. While the FAA prohibits "reverse targeting," the prohibition is narrow—it applies only if the government's surveillance targets a "particular, known

² See, e.g., *FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. at 9 (2006), <http://1.usa.gov/1kbgHm3> (statement of NSA Director Michael Hayden) (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"); Privacy and Civil Liberties Oversight Board ("PCLOB"), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 114–15 (July 2, 2014), <http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf> ("PCLOB 702 Report") ("Executive and legislative branch officials have repeatedly emphasized to us that, with respect to terrorism, communications involving someone in the United States are some of the 'most important' communications acquired under the program.")

³ See Letter from Att'y Gen. Michael Mukasey & DNI John M. McConnell to Sen. Harry Reid, at 3–4 (Feb. 5, 2008), <http://1.usa.gov/1ihhf9A>.

person reasonably believed to be in the United States.” 50 U.S.C. § 1881a(b)(2). Outside that narrow prohibition, the statute allows the government to conduct surveillance to collect Americans’ international communications. This is precisely how the government uses the statute, and the government has acknowledged not only that it collects Americans’ communications under the statute but that it uses selectors associated with U.S. persons to search through the communications it collects. *See* Letter from Deirdre M. Walsh, Dir. of Legislative Affairs, Office of the Dir. of National Intelligence, to Sen. Ron Wyden (June 27, 2014), <http://1.usa.gov/V8lYTo> (“ODNI–Wyden Letter”) (acknowledging that various agencies, including the Federal Bureau of Investigation, conducted thousands of backdoor searches using U.S. identifiers in 2013 alone); Ellen Nakashima, *Obama Administration Had Restrictions on NSA Reversed in 2011*, Wash. Post, Sept. 7, 2013, <http://wapo.st/1hP9FWm>. The government relies heavily on *In re Directives*, 551 F.3d 1004 (FISCR 2008), but in that case the FISC found it significant that the government was *not* amassing the database it is concededly amassing here—let alone querying that database for information about Americans. *Id.* at 1015 (“The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary.”).

Second, the “incidental overhear” cases cited by the government involved surveillance predicated on warrants—that is, they involved circumstances in which courts had found probable cause regarding the government’s targets and had limited with

particularity the facilities and communications to be monitored. *See, e.g., United States v. Kahn*, 415 U.S. 143 (1974); *United States v. Figueroa*, 757 F.2d 466 (2d Cir. 1985). The “incidental overhear” rule was invoked where a court had carefully circumscribed the government’s surveillance and limited the government’s intrusion into the privacy of third parties. *See United States v. Donovan*, 429 U.S. 413, 436 n.15 (1977) (holding that while a warrant is not made unconstitutional by “failure to identify every individual who could be expected to be overheard,” the “complete absence of prior judicial authorization would make an intercept unlawful”); *United States v. Yannotti*, 399 F. Supp. 2d 268, 274 (S.D.N.Y. 2005) (finding lawful an incidental intercept because the government had obtained a judicial warrant that “did not give the monitoring agents unfettered discretion to intercept any conversations whatsoever occurring over the target cell phone”); PCLOB 702 Report at 95 (“Where a wiretap is conducted in a criminal investigation pursuant to a warrant, satisfaction of the three requirements of the warrant clause . . . renders the wiretap constitutionally reasonable—both as to the intended subjects of the surveillance and as to any persons who end up being incidentally overheard, the full range of whom the government can never predict.”).

Surveillance conducted under the FAA is not similarly limited. Quite the opposite: the FAA does not require the government to establish probable cause or individualized suspicion of any kind concerning its targets; it does not require the government to identify to any court the facilities it intends to monitor; and it does not require the government to limit which communications it acquires—so long as the

programmatic purpose of its surveillance is to obtain foreign-intelligence information.

Surveillance is not particularized. The rule of the “incidental overhear” cases cannot be extended to this context.

Third, the *volume* of communications intercepted “incidentally” in surveillance under the FAA differs dramatically from the volume of communications intercepted incidentally in surveillance conducted under original FISA or Title III. Unlike original FISA and Title III, the FAA allows the government to monitor individuals without regard to whether those individuals are suspected criminals or foreign agents. PCLOB 702 Report 116 (“[T]he expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications.”). Under the government’s theory, the statute even allows the NSA to scan millions of people’s communications for information “about” the government’s targets. The government’s use of the term “incidental” conveys the impression that its collection of Americans’ communications under the FAA is a *de minimis* byproduct common to all forms of surveillance. But whereas surveillance under Title III or the original FISA might lead to the incidental collection of a handful of people’s communications, surveillance under the FAA invades the privacy of thousands or even millions of people. *See [Redacted]*, No. [Redacted], 2011 WL 10945618, at *27 (FISC Oct. 3, 2011) (observing that “the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in

absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial”); *id.* at *26 (“[T]he Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a *very* large number.”); *see id.* at *27 (noting that the government collects over 250 million communications each year under the FAA); President’s Review Group on Intelligence & Communications Technologies, *Liberty and Security in a Changing World* 149 (Dec. 12, 2013), <http://1.usa.gov/1be3wsO> (“PRG Report”) (“incidental interception is significantly more likely to occur when the interception takes place under section 702 than in other circumstances”); *see also Riley v. California*, Nos. 13-132 & 13-212, 2014 WL 2864483, at *13–16 (U.S. June 25, 2014) (recognizing that the broad collection of data raises different constitutional questions); *United States v. Jones*, 132 S. Ct. 945, 963–64 (2013) (Alito, J., concurring) (similar); *Jones*, 132 S. Ct. at 954–57 (Sotomayor, J., concurring).⁴

The government’s effort to stretch the incidental overhear doctrine to cover its dragnet collection of Americans’ communications reflects a view that constitutional rules and exceptions designed for an era of individualized surveillance can be applied willy-

⁴ The district court in *United States v. Mohamud* erred in finding that incidental collection under the FAA does not “differ sufficiently from previous foreign intelligence gathering to distinguish prior case law”—a finding upon which the court based its conclusion that the FAA “does not trigger the warrant clause.” *See* No. 3:10-CR-00475, 2014 WL 2866749, at *15 (D. Or. June 24, 2014). Besides being from a different circuit, and not from a higher court, under 10th Cir. Rule 32.1(A) while this decision, if unpublished, may be cited for its persuasive value, it is not precedential.

nilly to vast programs of suspicionless surveillance. This view is wrong. *See Riley*, 2014 WL 2864483; *Jones*, 132 S. Ct. 945; *United States v. Knotts*, 460 U.S. 276 (1983).

The government makes one further argument against application of the warrant requirement: It argues that it would be unworkable because “imposition of a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection.” Doc. 559 at 39. This is a red herring. The Fourth Amendment does not require the government to obtain prior judicial authorization for surveillance of foreign targets merely because those foreign targets might, at some unknown point, communicate with U.S. persons. But compliance with the warrant clause requires at least two things: that the government avoid warrantless acquisition of Americans’ international communications where it is reasonably possible to do so, and that it avoid warrantless review of such communications when it collects them inadvertently or incidentally.⁵

⁵ The NSA could easily implement the first restriction by automatically excluding American phone numbers or internet protocol addresses from its collection. It could also exclude from its collection any communications sent or received by accounts, addresses, or identifiers that it separately has reason to believe are associated with U.S. persons. The NSA apparently maintains a list of such accounts, addresses, and identifiers to prevent *targeting* errors; there is no reason that it could not do the same to protect Americans’ privacy more fully. *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 3* (July 28, 2009), <https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf> (“Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons.”).

There is no practical reason why these limitations—which have the effect of imposing a warrant requirement only for *Americans’* international communications—could not be imposed here. During the debate that preceded the passage of the FAA, then-Senator Barack Obama co-sponsored an amendment that would have codified these limitations by prohibiting the government from (1) acquiring a communication without a warrant if it knew “before or at the time of acquisition that the communication [was] to or from a person reasonably believed to be located in the United States,” and (2) accessing Americans’ communications collected under the FAA without a warrant based on probable cause. *See* S.A. 3979, 110th Cong. (2008). More recently, the President’s Review Group concluded that a warrant requirement should be imposed, and the House of Representatives passed an appropriations bill that would impose one. *See* PRG Report 28–29; H.R. 4870, 113th Cong. § 8127 (2014).

ii. Even if there is a foreign-intelligence exception, the exception is not broad enough to make the surveillance of Mr. Muhtorov constitutional.

As Mr. Muhtorov has explained, Doc. 520 at 27–30, there is no foreign-intelligence exception to the Fourth Amendment’s requirements of individualized suspicion and a warrant. Even if this exception existed it is not broad enough to make the government’s surveillance of Mr. Muhtorov constitutional. The cases the government cites involve a crucial limitation missing here: the surveillance was directed at foreign powers or their agents and predicated on an individualized finding of suspicion. *See, e.g., United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d

717, 720 (FISCR 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980); *see also* Doc. 520 at 31–32 (discussing cases).

The government relies heavily on *In re Directives*, 551 F.3d 1004 (FISCR 2008), a case that only underscores Mr. Muhtorov’s point. *In re Directives* addressed the constitutionality of surveillance directives issued under the PAA, Executive Order 12,333, and certain Defense Department regulations. Although the PAA did not itself require individualized suspicion or particularity, the surveillance program considered by the Foreign Intelligence Surveillance Court of Review (“FISCR”) required both. *See id.* at 1007 (“The certifications require certain protections above and beyond those specified by the PAA.”); *id.* at 1013–14 (describing a “matrix of safeguards” that included both a particularity and probable cause requirement). Throughout its opinion, the FISCR emphasized this point again and again, observing that “[c]ollectively, these procedures require a showing of particularity, a meaningful probable cause determination, and a showing of necessity.” *Id.* at 1016.

While the FISCR recognized a foreign-intelligence exception to the warrant requirement, that exception was narrow:

[W]e hold that a foreign intelligence exception to the Fourth Amendment’s warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and *is directed against foreign powers or agents of foreign powers* reasonably believed to be located outside the United States.

551 F.3d at 1012 (emphasis added). The surveillance considered by the FISCR was premised on an individualized finding of probable cause documented and certified by the Attorney General himself. *See In re Directives*, 551 F.3d at 1014.

The foreign-intelligence exception the government proposes is far broader than the one recognized by the FISCR in *In re Directives*. Here, the government has invoked the foreign-intelligence exception not in defense of surveillance directed at “foreign powers or agents of foreign powers reasonably believed to be located outside the United States,” but in defense of a statute that permits surveillance directed at *any* non-citizen located outside the United States and that permits dragnet surveillance of *Americans’* international communications without individualized suspicion or probable cause. The FISCR has never recognized a foreign-intelligence exception sweeping enough to render constitutional the surveillance that Mr. Muhtorov challenges here. *See* PCLOB 702 Report 90 n.411 (acknowledging that “it is not necessarily clear that the Section 702 [FAA] program would fall within the scope of the foreign-intelligence exception recognized by [earlier] decisions, which were limited to surveillance directly authorized by the Attorney General, targeting foreign powers or their agents, and/or pursuing foreign intelligence as the primary or sole purpose of the surveillance”).

iii. The surveillance of Mr. Muhtorov's communications was unreasonable.

No exception to the Fourth Amendment's warrant and probable-cause requirements applies here. Even if one did, however, the surveillance of Mr. Muhtorov under the FAA would be unconstitutional as unreasonable. *See* Doc. 520 at 33–34.

The FAA is unreasonable under the Fourth Amendment because it exposes virtually every American's international communication to suspicionless and warrantless surveillance. *See* Doc. 520 at 33–43. It abandons the limits that courts have identified as key to the constitutionality of electronic surveillance statutes, including FISA—individualized suspicion, prior judicial review, and particularity.⁶ Rather than dealing directly with these defining features of the FAA, the government argues that the statute is similar to the surveillance program held reasonable in *In re Directives*; that it is justified because of the government's overriding interest in countering terrorism; that Americans have little to no expectation of privacy in their international communications; and that “multiple safeguards” make the FAA reasonable.

First, the government's reliance upon *In re Directives*, *see* Doc. 559 at 54–55, is misplaced. The FISC found its ruling upon several factors that are absent here, including that, under the scheme considered, the government could acquire the communications only of “overseas foreign agents,” 551 F.3d at 1011; and the

⁶ *See In re Directives*, 551 F.3d at 1013 (“[T]he more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds.”).

determination that each target was a foreign agent was made by the Attorney General himself, *id.* at 1014. Also significant to the reasonableness of the scheme, the FISC said, was that the government did not “maintain a database of incidentally collected information from non-targeted United States persons.” *Id.* at 1015.⁷

None of these factors is present here, and their absence is critical. Because it permits the government to monitor any foreigner overseas and not just foreign agents, the FAA eliminates the primary criterion relied upon by every appellate court to find a scheme of foreign-intelligence surveillance reasonable: individualized suspicion. By transferring targeting authority away from the Attorney General of the United States, the FAA permits low-level NSA analysts to decide whom to target. *See also* Glenn Greenwald, *XKeyscore: NSA Tool Collects ‘Nearly Everything a User Does on the Internet’*, Guardian, July 31, 2013, <http://gu.com/p/3hy4h> (describing interface through which NSA analysts can initiate FAA surveillance “by clicking a few simple pull-down menus designed to provide both legal and targeting justifications”). And, finally, the FAA permits the government to assemble—and the government *has* assembled—“a database of incidentally collected information from non-targeted United States persons.” As explained in Mr. Muhtorov’s motion, Doc. 520 at 18, the government routinely uses

⁷ The government compares the PAA to the FAA in a manner that suggests that *In re Directives* upheld the PAA facially. *See* Doc. 559 at 53–55. That is not so. The FISC analyzed the PAA only “as implemented” in the case before it. *In re Directives*, 551 F.3d at 1009–10.

his database, which contains hundreds of millions of communications, to target U.S. persons through so-called “backdoor searches.” *See also* ODNI–Wyden Letter.

Second, the government’s claim that the FAA is “crucial to the government’s efforts against terrorism and other threats,” Doc. 559 at 56, is an evasion. Mr. Muhtorov does not challenge the government’s warrantless acquisition of foreign-to-foreign communications, only of foreign-to-U.S. communications. The real question is whether the government’s interest would be thwarted if it had to demonstrate individualized suspicion or to obtain a warrant before acquiring or reviewing Americans’ communications.

On this question, the government’s brief is silent. Instead, it claims with deliberate vagueness that, in ““54 counterterrorism investigations . . . information obtained under section 702 contributed *in some degree* to the success of the investigation.”” Doc. 559 at 57 (emphasis added) (quoting PRG Report 144–45). There are several problems with this argument. As an initial matter, the government has not specified the “degree” to which the FAA has contributed to its investigations. In Senate testimony, the government has admitted that only thirteen “had some nexus to the United States.” *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. at 52:33 (2013), <http://1.usa.gov/TPpSQb> (Sen. Leahy: “Would you agree that the fifty-four cases that keep getting cited by the administration were not all plots, and of the fifty four only thirteen had some nexus to the United States? Would you agree with that, yes or no?”);

Keith Alexander, Director, NSA: “Yes.”). The government has not explained how requiring that it demonstrate individualized suspicion or that it acquire a warrant in a handful of cases over a five- or six-year period would frustrate its surveillance efforts, particularly given that the government may conduct such surveillance without a warrant in exigent circumstances.⁸

Third, the government’s claim that Americans have no privacy interest in their international communications is without support. *See* Doc. 559 at 35 (“the privacy interests of U.S. persons in international communications are significantly diminished, if not completely eliminated, when those communications have been transmitted to or obtained from non-U.S. persons located outside the United States”); *see also id.* at 58–61. If it were true that Americans had no expectation of privacy in their international communications, then the government could target those communications for surveillance directly. It could dispense altogether with the doublespeak of “incidental collection” and collect and store all Americans’ every international call and email. Accepting this argument would mean the government has unfettered discretion to scrutinize every word that crosses the country’s borders. The government appears to be doing something along those lines by scanning every nearly cross-border communication

⁸ The recently released report by the PCLOB also fails to address this question. It states that “[a]pproximately fifteen of the cases we reviewed involved some connection to the United States,” PCLOB 702 Report 110, but it does not address whether requiring the government to obtain a warrant or demonstrate individualized suspicion when acquiring or reviewing Americans’ communications would have prevented the government from investigating those fifteen cases.

for information “about” its targets. *See* Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, <http://nyti.ms/1cez5ZK>; *see also* PCLOB 702 Report 121–22. Neither doctrine relied upon by the government—the border-search doctrine and the third-party doctrine, *see* Doc. 559 at 59–61—justifies such sweeping surveillance.

The border-search doctrine does not justify the surveillance of communications, and it does not justify the surveillance of them absent individualized suspicion. The government cites no cases suggesting that the doctrine even applies beyond the context of individuals or property physically at a border. The Supreme Court has clarified that the doctrine exists to serve the government’s interest in “stopping and examining *persons* and *property* crossing into this country.” *United States v. Ramsey*, 431 U.S. 606, 616 (1977) (emphasis added); *accord United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). In its seminal case on the matter, the Court noted that, under the regulations, “envelopes are opened at the border only when the customs officers have reason to believe they contain other than correspondence, while the reading of any correspondence inside the envelopes is forbidden.” *Ramsey*, 431 U.S. at 624. It is not a surprise that “[e]ven at the border, [courts have] rejected an ‘anything goes’ approach.” *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (requiring reasonable suspicion before a thorough review of a laptop at the border), *cert. denied*, 134 S. Ct. 899 (2014); *see also Lamont v. Postmaster Gen. of the United States*, 381 U.S. 301 (1965) (invalidating registration requirement for recipients of certain foreign mail).

The government's reliance upon the third-party doctrine is equally misplaced. *See* Doc. 559 at 59–60. Mr. Muhtorov unquestionably enjoys a reasonable expectation of privacy in his communications, whether sent conventionally or using modern technologies. *See, e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (“a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP” (quotation marks omitted)). The government's argument, therefore, applies at most to a narrow subset of Mr. Muhtorov's communications: those received by his foreign contacts (i.e., not in transit) and obtained by the government outside of the United States. The argument would not apply at all to FAA surveillance, which involves the acquisition of communications in transit, received by U.S. persons, or residing on the servers of U.S. companies. The government's argument amounts to an impermissible attempt to bootstrap away Americans' expectation of privacy in their international communications by focusing myopically on only the foreign end of the communications.

Finally, the government claims the FAA is reasonable because of “multiple safeguards” in place to protect Americans' privacy. Doc. 559 at 62–73. As Mr. Muhtorov has explained in his motion to suppress, those supposed safeguards are weak and riddled with exceptions. They permit the government to target virtually any foreigner for surveillance—even where another party to the communication is a U.S. person, *see* Doc. 520 at 35–36; and, for the U.S. persons inevitably swept up by that international dragnet, the only safeguards are minimization procedures that provide little

meaningful protection, *see* Doc. 520 at 36–42.⁹ The government’s response inadequately addresses two key facts.

First, while FAA surveillance is subject to minimization procedures, the minimization procedures do not account for the FAA’s failure to require 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 surveillance target. Under the FAA there is no first-level protection, because the statute does not call for individualized judicial authorization of surveillance targets (or of facilities to be monitored or communications to be acquired). Unlike FISA and Title III, the FAA permits dragnet surveillance of Americans’ international communications. In this context, it is an indictment of the FAA, not a defense, to say, as the government does, that the FAA’s minimization rules are analogous to the minimization rules that apply under FISA and Title III.¹⁰

Second, unlike the surveillance at issue in *In re Directives*, FAA surveillance permits the government to “maintain a database of incidentally collected information

⁹ The Supreme Court recently warned against excessive reliance on “government agency protocols” to safeguard Americans’ privacy. *See Riley*, 2014 WL 2864483, at *16 (“[T]he Founders did not fight a revolution to gain the right to government agency protocols.”).

¹⁰ The government’s suggestion that Yahoo!’s challenge in *In re Directives* amounted to a full adversarial proceeding is unfounded. *See* Doc. 559 at 54 n.33. The court there was clear that it considered at least some of the relevant procedures on an *ex parte* basis. *See* 551 F.3d at 1013.

from non-targeted United States persons,” 551 F.3d at 1015, and to later search that database using the names, email addresses, or other identifiers of U.S. persons. The government defends this practice—known as “backdoor searching”—by claiming this practice does not “implicate any reasonable expectation of privacy beyond that implicated in the initial collection.” Doc. 559 at 67. This is incorrect. The minimization procedures in surveillance schemes are a part of the terms of access. Courts uphold the reasonableness of the schemes—as with FISA and Title III—only if those terms are reasonable. *See Scott v. United States*, 436 U.S. 128, 140–43 (1978) (reviewing surveillance minimization practices for reasonableness); *United States v. Ganius*, No. 12-240, 2014 WL 2722618 (2d Cir. June 17, 2014) (suppressing evidence where government obtained files and searched them for information beyond the terms of the warrant). Here, the terms of access omit a limitation that the FISC viewed as essential to the constitutionality of a much narrower program. *See In re Directives*, 551 F.3d at 1015. If the government were correct, then the “multiple safeguards” on which it rests its case would be entirely superfluous as a constitutional matter.¹¹

¹¹ If the government conducted one or more backdoor searches of Mr. Muhtorov’s communications, that would violate both the Fourth Amendment and the FAA, and it would provide an independent basis for suppression. The FAA prohibits the targeting of a foreigner overseas for the purpose of targeting “a particular, known person” inside the United States. 50 U.S.C. § 1881a(b)(2). Backdoor searching of the government’s extensive database of Americans’ “incidentally” collected communications violates this prohibition, and the Fourth Amendment, by enabling the surveillance of particular, known U.S. persons without a warrant.

B. The government’s warrantless surveillance of Mr. Muhtorov’s communications violated Article III.

The FAA violates Article III’s “case or controversy” requirement because the statute requires FISC judges to issue advisory opinions addressing the constitutionality of abstract procedures absent concrete facts. *See* Doc. 520 at 47. It is plain that a federal court could not adjudicate, at the mere urging of the Denver Police Department, the constitutionality of the department’s newly devised internal policies governing its officers’ use of force. Nor could a court take up a request by the Transportation Security Administration to pass upon the reasonableness of new agency procedures concerning secondary airport screening before their application to a particular passenger. So too here—and none of the government’s arguments to the contrary has merit.

The “case or controversy” requirement ensures that Article III courts do “not engage in *adjudicatory or decisional functions* except in those ‘cases’ and ‘controversies’ referred to in Article III.” *Application of President’s Comm’n on Organized Crime*, 763 F.2d 1191, 1203 (11th Cir. 1985) (emphasis added) (quotation marks omitted). By limiting the jurisdiction of Article III courts to live, concrete disputes, the “case or controversy” requirement closes the courthouse doors to requests for advisory opinions or “abstract declaration[s] of the law.” *In re Summers*, 325 U.S. 561, 567 (1945); *see United States v. Fruehauf*, 365 U.S. 146, 157 (1961) (characterizing advisory opinions as “advance expressions of legal judgment upon issues which remain unfocused because they” lack “clear concreteness”). As the Supreme Court recently explained, “[i]f a

dispute is not a proper case or controversy, the courts have no business deciding it, or expounding the law in the course of doing so.” *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006); *see Chi. & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 113 (1948); *United States v. Burlington N. R.R. Co.*, 200 F.3d 679, 699 (10th Cir. 1999).¹²

The government misconstrues Mr. Muhtorov’s “case or controversy” argument—and it cites cases that rejected very different Article III challenges. Mr. Muhtorov’s “case or controversy” argument has little in common with the failed Article III challenges in *Morrison v. Olson*, 487 U.S. 654 (1988), and *Mistretta v. United States*, 488 U.S. 361 (1989), which concerned congressional statutes granting *executive* and *administrative* functions to federal judges. *See Morrison*, 487 U.S. at 680–82 (rejecting Article III challenge to Congress’s assignment of administrative and executive functions to special court charged with role in the appointment of independent counsel); *Mistretta*, 488 U.S. at 411 (rejecting Article III challenge to “nonadjudicatory” functions of judges on U.S. Sentencing Commission). Likewise, Mr. Muhtorov’s argument is of a different flavor than objections to the administrative role of Article III judges in promulgating federal rules of procedure. *See Mistretta*, 488 U.S. at 391. And Mr. Muhtorov does not, like

¹² *See also Norvell v. Sangre de Cristo Dev. Co., Inc.*, 519 F.2d 370, 375 (10th Cir. 1975) (“It is fundamental that federal courts do not render advisory opinions and that they are limited to deciding issues in actual cases and controversies. A justiciable controversy is distinguished from a difference or dispute of a hypothetical character or from one that is academic.” (citations omitted)); *see also Klinger v. Conan Doyle Estate, Ltd.*, No. 14-1128, 2014 WL 2726187, at *2 (7th Cir. June 16, 2014) (Posner, J.) (“It would be very nice to be able to ask federal judges for legal advice But that would be advisory jurisdiction, which” is “inconsistent with Article III’s limitation of federal jurisdiction to actual disputes, thus excluding jurisdiction over merely potential ones”).

other criminal defendants challenging traditional FISA, base his Article III complaint in the fact that the FISC acts in secret and *ex parte*. See *In re Sealed Case*, 310 F.3d 717, 732 n.19 (FISCR 2002); *In re Kevork*, 634 F. Supp. 1002, 1013 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986); *United States v. Megahey*, 553 F. Supp. 1180, 1196 (E.D.N.Y. 1982), *aff'd sub nom.*, *United States v. Duggan*, 743 F.2d 59, 73–74 (2d Cir. 1984); see also *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 144 (E.D. Va. 2011). Rather, Mr. Muhtorov’s Article III argument is that the FAA asks judges *to judge* absent a constitutionally required “case or controversy” in which to do so. See *Application of President’s Comm’n on Organized Crime*, 763 F.2d at 1203.

When the government addresses Mr. Muhtorov’s *actual* Article III challenge, its arguments are unpersuasive. The government contends that FISC opinions approving or disapproving of targeting and minimization procedures under the FAA are “no more advisory” than other kinds of Fourth Amendment assessments that “courts regularly undertake.” Doc. 559 at 79.¹³ But while “[a]nalyzing the reasonableness of electronic surveillance . . . is a traditional judicial function,” Doc. 559 at 79, an Article III court cannot conduct such an analysis absent a “case or controversy.” The government likens the FISC’s FAA review to judicial rulings on traditional search warrants or wiretap

¹³ The government’s suggestion that the FISC’s FAA review is not advisory because its orders “ha[ve] legal effect,” Doc. 559 at 77, is misguided. All statutes and regulations have “legal effect.” This does not mean that an Article III court can adjudicate their constitutionality in the absence of any case or controversy.

applications, *see* Doc. 559 at 77, even as it concedes that “warrant or wiretap applications for law enforcement purposes typically involve a more fact-specific form of review” than that required by the FAA, Doc. 559 at 80.¹⁴ But the concession that traditional warrant assessments are “more” fact-specific minimizes the crucial difference—where warrant and wiretap applications almost invariably involve particular targets or premises and unique, articulable facts, the FISC’s FAA review involves *none*.

Finally, the government mistakes that when courts engage in Fourth Amendment review of warrant and wiretap schemes they *always* do so consistent with Article III. Yet that overlooks, again, what makes a “case or controversy.” Consistent with Article III, courts may engage in a Fourth Amendment review of such schemes only when presented with a concrete legal question at the behest of an individual affected by them. A court may adjudicate the Fourth Amendment reasonableness of statutory schemes governing domestic wiretaps for law-enforcement purposes or administrative warrants in the public-health context. *See* Doc. 559 at 79–80 (citing *United States v. Tortorello*, 480 F.2d 764, 772–73 (2d Cir. 1973); *Camara v. Municipal Court*, 387 U.S. 523, 537–38 (1967)). And courts may also assess surveillance schemes for constitutional reasonableness. *See, e.g., Berger v. New York*, 388 U.S. 41 (1967). But there would have been no “case or

¹⁴ The government provides no citation for its bare and circular assertion that these differences are “because the Fourth Amendment or Title III require[] more particularity in those contexts—not because of anything in Article III,” Doc. 559 at 80. And, in fact, in advocating passage of FISA in 1978, the executive branch defended the constitutionality of the law against Article III objections by pointing to precisely the type of specificity that is lacking under the FAA. *See* Doc. 520 at 46–47.

controversy” in *Tortorello* without Arthur Tortorello, nor in *Camara* without Roland Camara, nor in *Berger* without Ralph Berger—nor, here, without Jamshid Muhtorov. The government is correct that a court *could* evaluate the government’s proposed targeting and minimization procedures “as applied to specific, technical tools through which the government implements” the FAA. Doc. 559 at 79. But because the FAA asks the FISC to make that assessment absent a concrete dispute, the statute violates Article III.

II. THE GOOD FAITH EXCEPTION DOES NOT APPLY.

The good-faith exception to the exclusionary rule does not apply to FISA’s statutory suppression remedy. And even if it did, it would have no application here.

If the Court “determines that the surveillance was not lawfully authorized or conducted, it *shall* . . . suppress the evidence which was unlawfully obtained or derived” from such surveillance. 50 U.S.C. § 1806(g) (emphasis added). “This ground for suppression plainly includes constitutional challenges to FISA itself.” David S. Kris & J. Douglas Wilson, 2 *National Security Investigations and Prosecutions* § 32:3 (2d ed. 2012); *see also id.* § 32:3 & n.2 (“[The] judge reviewing [a] motion to suppress FISA evidence ‘is also free to review the constitutionality of the law itself.’” (quoting FISA H. Rep. at 92–93)); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (“The Constitution is law” to determine whether FISA surveillance was “‘lawfully authorized and conducted.’”). If the Court finds that the government’s surveillance of Mr. Muhtorov’s communications under the FAA was unconstitutional, it must order

suppression under § 1806(g). This is required by the statute, and “does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights.” *United States v. Giordano*, 416 U.S. 505, 524 (1974). The limits on the *judicially created* exclusionary rule do not apply to the *statutory* exclusionary rule. As with Title III, the good-faith exception to the Fourth Amendment’s exclusionary rule does not apply. *United States v. Glover*, 736 F.3d 509, 515–16 (D.C. Cir. 2013); *United States v. Rice*, 478 F.3d 704, 711–14 (6th Cir. 2007) (“The language and legislative history of Title III strongly militate against engrafting the good-faith exception into Title III warrants.”); *id.* at 713–14 (criticizing contrary holdings of the Eighth and Eleventh Circuits).¹⁵

Even if the good-faith exception applied to § 1806(g), it would not be properly invoked here. The government contends that suppression is unwarranted because it relied in good faith on “orders issued by neutral magistrates—the judges of the FISC,” Doc. 559 at 81 (citing *United States v. Leon*, 468 U.S. 897 (1984)), on a facially constitutional statute, *id.* at 80–81 (citing *Illinois v. Krull*, 480 U.S. 340 (1987)), and on appellate precedent from the FISA Court of Review, *id.* at 81 (citing *Davis v. United States*, 131 S. Ct. 2419 (2011)). These arguments are misplaced. The good-faith exception announced in *Leon* does not apply because this case does not involve reliance on an individualized warrant authorizing the search of particularly described communications or locations.

¹⁵ The Tenth Circuit has not yet had occasion to decide “whether the good-faith exception applies in the Title III context.” *United States v. Barajas*, 710 F.3d 1102, 1110 (10th Cir. 2013).

See Leon, 468 U.S. at 920–21; *United States v. Ning Wen*, 477 F.3d 896, 897–98 (7th Cir. 2006) (discussing reliance on individualized FISA warrants). For FAA surveillance, the FISC approves only general procedures proposed by the government, and, on the basis of those procedures alone, the government determines whom to monitor, when, and for how long. *See* 50 U.S.C. § 1881a. No judge approves the target of the surveillance or makes an individualized assessment of probable cause. Therefore, there is no warrant upon which the government can rely within the meaning of *Leon*.

Reliance on the statute does not justify application of the good-faith exception either. To so hold would render the § 1806(g) statutory suppression remedy moot when the government has violated the Fourth Amendment. It makes no sense that reliance on the terms of an unconstitutional statute functions to erase the suppression remedy explicitly provided by that same statute for unconstitutional searches. Further, the government may have violated the statute itself during its surveillance of Mr. Muhtorov, which would trigger application of the § 1806(g) suppression remedy. *See* Doc. 520 at 38 (discussing “about searches”); *id.* at 39 (discussing “backdoor searches”); [Redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011) (finding that government’s minimization procedures contradict the FAA’s requirements). Reasonable government officials “should have known that the statute was unconstitutional,” *Krull*, 480 U.S. at 355, given its manifest and multiple infirmities. *See* Doc. 520 at 20–47; *supra* Part I.

Finally, reliance on *In re Directives*—an inapposite opinion of the FISC—does not justify application of the good-faith exception under *Davis*. *Davis* suspends operation

of the exclusionary rule when the government conducts a search “in objectively reasonable reliance on binding judicial precedent.” 131 S. Ct. at 2428–29. As the Eleventh Circuit has explained, “precedent on a given point must be unequivocal.” *United States v. Davis*, 598 F.3d 1259, 1266 (11th Cir. 2010), *aff’d* 131 S. Ct. 2419; *accord United States v. Buford*, 632 F.3d 264, 276 n.9 (6th Cir. 2011). The sole appellate precedent the government cites as justifying the surveillance of Mr. Muhtorov is *In re Directives*, in which the Court of Review evaluated a distinct and now-expired statute, the PAA, based on different criteria and different facts, including limitations on the surveillance not provided here. *See supra* Part I.A. *In re Directives* is not on point. And even if it were, the government fails to explain how an opinion of a nonadversarial court that conducts proceedings in secret and has, to the public’s knowledge, convened only twice in its 36-year history constitutes binding appellate precedent within the meaning of *Davis*. *See United States v. Madden*, 682 F.3d 920, 927 (10th Cir. 2012) (stating that *Davis* applies when there is “well-settled law of *this* court” (emphasis added)). The good-faith exception does not apply.

III. MR. MUHTOROV IS ENTITLED TO DISCOVERY.

The government contends this Court’s *in camera*, *ex parte* review of materials at issue in Mr. Muhtorov’s motion satisfies the statute and the Due Process Clause. Doc. 559 at 87–88. Though the statute empowers the Court to conduct such a review, Mr. Muhtorov has provided the basis for this Court to order disclosure to his counsel, subject to appropriate protective orders. Doc. 520 at 47–66. Such disclosure is “necessary”

under the statute, 50 U.S.C. § 1806(f), and the Court should reject the government’s cramped reading of that term. *See Cellular Telecomms. & Internet Ass’n v. FCC*, 330 F.3d 502, 509–10 (D.C. Cir. 2003) (explaining that “necessary” has a flexible meaning informed by context and often “mean[s] less than absolutely essential” (internal quotation marks omitted)). The legislative history clarifies that Congress fully intended there to be disclosure and adversary proceedings in at least some FISA cases because “[t]he defendant’s constitutional guarantee of a fair trial could be seriously undercut if he is denied the materials needed to present a proper defense. The committee believes that a just, effective balance has been struck in this section.” S. Rep. No. 95-701, at 59 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4028. Congress contemplated that “[c]ases may arise, of course, where the court believes that disclosure is necessary.” *Id.* at 65, *reprinted in* 1978 U.S.C.C.A.N. at 4034. The government’s reading of the statute would foreclose any possibility of such cases arising and frustrate Congress’s intent.

As support for the claim that no disclosure is warranted here, the government cites cases addressing run-of-the-mill surveillance under individualized FISA surveillance orders. Doc. 559 at 89–91. But characterizing Mr. Muhtorov’s arguments as mere rehashing of these prior cases trivializes the novel complexities. Mr. Muhtorov challenges the constitutionality of the more complex surveillance program operated under the FAA. No appeals court has addressed the constitutionality of this statute, nor of

collection of particular U.S. persons' communications under it.¹⁶ *See supra* Parts I–II. Determining the constitutionality of FAA surveillance of Mr. Muhtorov requires assessment not only of the statutory scheme, but also of the government's targeting and minimization procedures, of its application of those procedures, and of complicated, factually contingent questions such as whether and precisely how Mr. Muhtorov's communications were obtained via “about” or “backdoor” searches. Addressing the constitutionality of the surveillance of Mr. Muhtorov's communications requires insight into the surveillance, which is not possible without access to the underlying records.

Surveillance and searches under FISA and the FAA present especially acute difficulties to defendants seeking to vindicate their Fourth Amendment rights under *Franks v. Delaware*, 438 U.S. 154 (1978). But that does not mean that the necessity of the *Franks* procedure in FISA cases is diminished in any way: “*Franks* serves as an indispensable check on potential abuses of the warrant process, and means must be found to keep *Franks* from becoming a dead letter in the FISA context.” *United States v. Daoud*, No. 14-1284, 2014 WL 2696734, at *7 (7th Cir. June 16, 2014) (Rovner, J., concurring). The government concedes that *Franks* applies to FAA surveillance. Doc. 559 at 95. And although it contends that the Court's *in camera*, *ex parte* review of classified FAA materials identifies and adjudicate any Fourth Amendment violations, *see id.* at 91, this non-adversarial process provides only a pale shadow of the protection

¹⁶ The government asserts that the FISA Court of Review's decision in *In re Directives* settles these issues, but as explained above, that case is not on point. *See supra* Parts I.A, II.

contemplated by *Franks*. As Judge Rovner explained, “although a court may be able to discover inconsistencies in the FISA materials, its ability to discover false statements and omissions is necessarily limited, as it has only the government’s version of the facts. . . . [A] court cannot conduct more than a limited *Franks* review on its own.” *Daoud*, 2014 WL 2696734, at *15–16.

Here, however, the Court need not be hobbled by such limited process. Contrary to the government’s suggestion, Mr. Muhtorov does not seek a *Franks* hearing solely “based on evidence of misrepresentations in some other case.” Doc. 559 at 91 n.53. Rather, unlike in *Daoud*, 2014 WL 2696734, at *4, 6, he has identified evidence, in a declassified FISC opinion, that the FISC’s approval of programmatic FAA surveillance *when his communications were collected under that authority* was tainted by government misrepresentations of fact. Doc. 520 at 53–54, 56–57 (citing *[Redacted]*, 2011 WL 10945618 (FISC Oct. 3, 2011)). This meets the threshold set by *Franks*, 438 U.S. at 171–72, and requires disclosure of the government’s application(s) to the FISC (subject to appropriate protective orders) and an adversarial hearing on Mr. Muhtorov’s motion.¹⁷

¹⁷ Moreover, *Daoud* was argued and decided as a case raising issues under traditional FISA principles, and the opinion does not purport to address discovery and disclosure issues under the FAA.

Dated: July 3, 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, Suite 1000
Denver, CO 80202
Telephone: 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
Phone: (303) 777-5482;
Fax: (303) 777-1773
msilverstein@aclu-co.org

CERTIFICATE OF SERVICE

I hereby certify that on July 3, 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