CASE NO. 18-1366

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,	)
	)
Plaintiff–Appellee,	)
	)
v.	)
	)
JAMSHID MUHTOROV,	)
	)
Defendant–Appellant.	)

On Appeal from the United States District Court
for the District of Colorado
The Honorable John L. Kane, Senior U.S. District Judge
D.C. Case No. 1:12-cr-00033-JLK-1

APPELLANT'S REPLY BRIEF

PATRICK TOOMEY
ASHLEY GORSKI
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500

VIRGINIA L. GRADY
Federal Public Defender

JOHN C. ARCECI
Assistant Federal Public Defender
633 17th Street, Suite 1000
Denver, Colorado 80202
(303) 294-7002

April 7, 2020

Table of Contents

Table of Authorities iv

Introduction 1

Argument 2

I. The government's warrantless surveillance of Mr. Muhtorov was unconstitutional and the resulting evidence must be suppressed. 2

A. The government's warrantless backdoor searches rendered the surveillance here unlawful. 2

1. A new ruling by the Foreign Intelligence Surveillance Court confirms that the surveillance of Mr. Muhtorov violated the Fourth Amendment. 2

2. The government's querying of Mr. Muhtorov's communications was a "separate Fourth Amendment event" that required a warrant. 7

B. No Fourth Amendment exception excuses the government's warrantless surveillance of Mr. Muhtorov. 12

1. The government cannot evade the warrant requirement simply by "targeting" the foreign end of Americans' communications. 13

2. The incidental overhear cases do not establish an exception to the warrant requirement. 15

3. No foreign intelligence exception to the warrant requirement applies. 18

C. There are reasonable safeguards that would protect Americans' privacy. 20

D. The warrantless surveillance of Mr. Muhtorov violated Article III of the Constitution. 24

E. The good-faith exception does not apply. 26

II. FISA and due process require the disclosure of Section 702 and FISA materials. 28

A. This Court reviews the district court's decision to deny disclosure de novo. 29

B. Disclosure is "necessary" in cases involving complex issues, like Mr. Muhtorov's. 29

C. Widespread FISA abuses identified by the DOJ Inspector General underscore the need for disclosure and adversarial litigation here 30

D. The government's public disclosures of Section 702 and FISA materials show that its blanket claim of secrecy cannot be justified. 32

III. Mr. Muhtorov is entitled to notice and the opportunity to challenge the other novel surveillance tools the government used in its investigation 33

A. This Court reviews de novo the legal question of whether Mr. Muhtorov is entitled to notice. 34

B. The Constitution, statutory law, and the Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice of the government's surveillance tools 34

1. The Fourth and Fifth Amendments entitle Mr. Muhtorov to notice 35

2. 18 U.S.C. § 3504 entitles Mr. Muhtorov to notice. 37

3. The Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice 39

4. *Carpenter* and *Clapper* show that notice is essential. 40

C. The district court erred in allowing the government to conceal novel surveillance of Mr. Muhtorov through CIPA. 42

1. *Alderman* forecloses ex parte CIPA litigation over Fourth Amendment suppression issues. 42

2. The CIPA framework compels disclosure.....43

IV. The over six-year delay violated Mr. Muhtorov's constitutional speedy trial right.....45

Certificates of Compliance, Digital Submission, and Service.....48

Table of Authorities

Cases

[*Redacted*],
2011 WL 10945618 (FISC Oct. 3, 2011) 3, 7

[*Redacted*],
402 F. Supp. 3d 45 (FISC 2018)..... *passim*

[*Redacted*],
Mem. Op. (FISC Nov. 6, 2015).....7

[*Redacted*],
Mem. Op. (FISC Sept. 4, 2019).....6

ACLU v. Clapper,
785 F.3d 787 (2d Cir. 2015) 40

Alderman v. United States,
394 U.S. 165 (1969)..... 12, 36, 42, 43

Berger v. New York,
388 U.S. 41 (1967)..... *passim*

Carpenter v. United States,
138 S. Ct. 2206 (2018)..... 18, 40

City of Los Angeles v. Patel,
135 S. Ct. 2443 (2015).....25

DaimlerChrysler Corp. v. Cuno,
547 U.S. 332 (2006).....24

Dalia v. United States,
441 U.S. 238 (1979)..... 35, 36

El Encanto, Inc. v. Hatch Chile Co.,
825 F.3d 1161 (10th Cir. 2016) 29, 34

Illinois v. Krull,
480 U.S. 340 (1987)..... 27, 28

In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC,
No. Misc. 19-02 (FISC Dec. 17, 2019).....31

In re Directives,
551 F.3d 1004 (FISCR 2008) 7, 19

Katz v. United States,
389 U.S. 347 (1967)..... 11, 13, 17

Maryland v. King,
569 U.S. 435 (2013).....11

Mathews v. Eldridge,
424 U.S. 319 (1976).....33

Matter of Grand Jury,
524 F.2d 209 (10th Cir. 1975) 38

Riley v. California,
573 U.S. 373 (2014)..... 8, 9, 17

Roviaro v. United States,
353 U.S. 53 (1957)..... 33, 44

Smith v. Black,
904 F.2d 950 (5th Cir. 1990) 37

Terry v. Ohio,
392 U.S. 1 (1968).....8

United States v. Apple,
915 F.2d 899 (4th Cir. 1990) 38

United States v. Belfield,
692 F.2d 141 (D.C. Cir. 1982).....29

United States v. Carey,
172 F.3d 1268 (10th Cir. 1999) 9, 22

United States v. Chun,
503 F.2d 533 (9th Cir. 1974) 35

United States v. Daoud,
755 F.3d 479 (7th Cir. 2014) 30

United States v. Donovan,
429 U.S. 413 (1977)..... 16, 35

United States v. Duggan,
743 F.2d 59 (2d Cir. 1984) 23

United States v. Figueroa,
757 F.2d 466 (2d Cir. 1985) 16

United States v. Gamez-Orduno,
235 F.3d 453 (9th Cir. 2000) 37

United States v. Glover,
736 F.3d 509 (D.C. Cir. 2013).....27

United States v. Hamide,
914 F.2d 1147 (9th Cir. 1990) 38

United States v. Hanna,
661 F.3d 271 (6th Cir. 2011) 43

United States v. Hasbajrami,
945 F.3d 641 (2d Cir. 2019) ..... *passim*

United States v. Krueger,
809 F.3d 1109 (10th Cir. 2015) 26

United States v. Leon,
468 U.S. 897 (1984)..... 27, 41

United States v. Lustyik,
833 F.3d 1263 (10th Cir. 2016) 34

United States v. Martinez,
643 F.3d 1292 (10th Cir. 2011) 11

United States v. Megahey,
553 F. Supp. 1180 (E.D.N.Y. 1982) 25

United States v. Rice,
478 F.3d 704 (6th Cir. 2007) 27

United States v. Scafe,
822 F.2d 928 (10th Cir. 1987) 40

United States v. Sedaghaty,
728 F.3d 885 (9th Cir. 2013) 9, 10, 22, 43

United States v. Soto-Zuniga,
837 F.3d 992 (9th Cir. 2016) 40

United States v. Stewart,
590 F.3d 93 (2d Cir. 2009) 16

United States v. Tortorello,
480 F.2d 764 (2d Cir. 1973) 16

United States v. U.S. Dist. Court (Keith),
407 U.S. 297 (1972)..... 18, 24

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990).....14

Statutes

18 U.S.C. app. III 43

18 U.S.C. § 2518.....45

18 U.S.C. § 3504..... 37, 38, 39

50 U.S.C. § 1801..... 13, 18, 22

50 U.S.C. § 1805..... 19, 23

50 U.S.C. § 1806..... 26, 29, 36, 45

50 U.S.C. § 1881a 25, 26

Other Authorities

2 Fed. Prac. & Proc. Crim. § 254 (4th ed.) 39

Appellants' Reply, *United States v. Moalin*, No. 13-50572 (9th Cir. Sept. 2, 2016) 41

Brief of Amici Curiae Church Committee Staff 29

Brief of Amici Curiae David Medine & Sharon Bradford Franklin 4, 8

Brief of Amicus Curiae Brennan Center 16

Charlie Savage, et al., *Hunting for Hackers, NSA Secretly Expands Internet Spying at U.S. Border*, N.Y. Times, June 4, 2015 20

DOJ Office of the Inspector General, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019) 30, 31

DOJ Office of the Inspector General, *Management Advisory Memorandum* (Mar. 2020) 31, 32

FBI Section 702 Minimization Procedures (2015) 33

Georgetown University, *Foreign Intelligence Law Collection* 33

H.R. Rep. No. 95-1720 (1978) 23

Orin Kerr, *The Surprisingly Weak Reasoning of* Mohamud, Lawfare (Dec. 23, 2016) 13, 17

Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ..... *passim*

Wayne R. LaFave, et. al., 5 Crim. Proc. § 20.3(c) (4th ed.) 40

Rules

Federal Rule of Criminal Procedure 16 ..... 39, 40

Introduction

Mr. Muhtorov's claims have only grown stronger since he filed his opening brief. In a newly declassified opinion, the Foreign Intelligence Surveillance Court ("FISC") found serious constitutional infirmities with Section 702 surveillance. And the Second Circuit has explained that the government's backdoor searches targeting Americans must independently satisfy constitutional requirements. Both rulings point in the same direction: the government's prolific use of warrantless searches to comb through the emails of Americans like Mr. Muhtorov is intolerable under the Fourth Amendment. These decisions provide this Court all it needs to conclude that Mr. Muhtorov's Fourth Amendment rights were violated.

Also in the last few months, the Department of Justice's Inspector General has issued two reports documenting widespread problems in the government's FISA applications going back years. The new reports underscore Mr. Muhtorov's arguments that adequate disclosure and adversarial litigation are vital when the government employs novel and complex surveillance tools. That the government continues to contend that it had essentially no disclosure obligations, despite clear constitutional and statutory law to the contrary, further necessitates this Court's intervention.

Finally, Mr. Muhtorov continues to join Mr. Jumaev's constitutional speedy trial challenge. The government's indifference to the nearly six-and-a-half years

Mr. Muhtorov spent in pretrial detention, as well as its own role in causing that delay, speaks volumes, and this Court should not condone this Sixth Amendment violation.

Argument

I. The government's warrantless surveillance of Mr. Muhtorov was unconstitutional and the resulting evidence must be suppressed.

A. The government's warrantless backdoor searches rendered the surveillance here unlawful.

New decisions by the FISC and the Second Circuit demonstrate that the government's warrantless surveillance of Mr. Muhtorov was unlawful. The government's rampant use of backdoor searches to target Americans, absent any individualized judicial approval, goes far beyond its claimed interest in surveilling foreigners. Just as the Supreme Court held the wiretapping procedures in *Berger* inadequate, this Court should hold that the Fourth Amendment requires greater protection when agents seek to query and use the communications of Americans like Mr. Muhtorov. *Berger v. New York*, 388 U.S. 41, 54-60 (1967).

1. A new ruling by the Foreign Intelligence Surveillance Court confirms that the surveillance of Mr. Muhtorov violated the Fourth Amendment.

The government claims that "[e]very court to reach the issue has held that surveillance under Section 702 is reasonable under the Fourth Amendment," Gov't Br. 15—but that is false. The FISC has found Section 702 surveillance

unreasonable on at least two occasions, including in a decision just recently disclosed.

Since Mr. Muhtorov filed his opening brief, the public learned of a new FISC decision holding that the FBI's Section 702 surveillance violated the Fourth Amendment. [*Redacted*], 402 F. Supp. 3d 45, 73-88 (FISC 2018). The FISC's decision was based on the FBI's "maximal" use of backdoor searches to investigate Americans, and the absence of basic safeguards. *See id.* at 80, 87-88 ("The government is not at liberty to do whatever it wishes with those U.S.-person communications."). Because the FBI's procedures suffered from the same flaws when Mr. Muhtorov was surveilled and subjected to backdoor searches, this Court need go no further than the FISC to find the warrantless surveillance in this case unreasonable.[1]

In holding that the procedures governing the FBI's backdoor searches rendered the surveillance unreasonable, the FISC recognized the same problems that Mr. Muhtorov identified, Def. Br. 24-25: the vast scale of these searches, their intrusiveness, and glaring weaknesses in the FBI's rules.

First, the FISC underscored the staggering scale of the FBI's backdoor searches and their impact on Americans, not just foreigners. According to the

[1] As Mr. Muhtorov noted in his opening brief, Def. Br. 61, the FISC has found Section 702 surveillance unreasonable on at least one other occasion. [*Redacted*], 2011 WL 10945618, at *23-28 (FISC Oct. 3, 2011).

FISC, FBI agents conducted more than *3.1 million* warrantless queries of Section 702 databases in 2017 alone, a "significant percentage" of which likely involved Americans. [*Redacted*], 402 F. Supp. 3d at 75. The FISC found that the privacy interests implicated by these queries are "substantial," *id.* at 87—precisely because the government acquires the "full contents" of vast numbers of communications under Section 702, and queries allow FBI agents to sift through that trove of information for the communications of particular Americans. *Id.* at 75, 88. Despite these substantial privacy interests, the FBI's policy has been to encourage "maximal querying of Section 702 information." *Id.* at 78.

Second, as the FISC noted, the FBI's queries are especially intrusive because the FBI uses them to repurpose Section 702 into a tool for all manner of domestic investigations. *See id*. at 75, 87. Although Section 702 is nominally targeted at more than 160,000 foreigners, FBI agents routinely use queries to focus on Americans instead—including at the earliest "assessment" stages of unrelated investigations. *See id*. at 80. Without any showing of suspicion, an FBI agent can type in an American's name, email address, or phone number, and pull up whatever communications the FBI's Section 702 collection has vacuumed into its databases over the past five years. Queries are a free pass for accessing protected communications that, otherwise, would be off-limits. *See* Br. of Amici Curiae David Medine & Sharon Bradford Franklin 9-15.

Third, chronic weaknesses in the FBI's rules have undermined the protections for Americans still further—and this, in the FISC's view, proved fatal. To search for an American's communications in the pool of Section 702 data, an FBI agent must simply have a "reasonable basis to believe" that the query is "likely" to return foreign intelligence information or evidence of a crime—two extremely broad and elastic categories. [*Redacted*], 402 F. Supp. 3d at 76. On top of that, the rules imposed little accountability. Not only were agents free to bypass the bedrock requirement that they obtain a warrant, the FBI did not even require agents to *write down* their reasons for targeting an American with a backdoor search. *Id.* at 52-53, 79. The absence of such a basic requirement made effective oversight difficult, if not impossible. *Id.*

Predictably, these lax rules led to large numbers of unauthorized backdoor searches. Across thousands of queries, FBI agents sought information about Americans that was not reasonably likely to result in foreign intelligence information or evidence of a crime, including searches for information concerning relatives, potential witnesses, and potential informants. *Id.* at 76-78, 87 (finding that "the FBI has conducted tens of thousands of unjustified queries of Section 702 data").

Ultimately, the FISC found that the FBI's permissive rules for searching through Americans' communications rendered the surveillance unreasonable under

the Fourth Amendment. *Id.* at 86-88. The court concluded that given the frequency of the FBI's backdoor searches, the sensitivity of Americans' communications, and the FBI's domestic focus, its procedures failed to adequately safeguard Americans' privacy interests. The FBI subsequently adopted strengthened procedures, and it continues to conduct Section 702 surveillance on that basis today. [*Redacted*], Mem. Op. (FISC Sept. 4, 2019), https://bit.ly/2x3tRC9. But those changes cannot save the government's flawed surveillance of Mr. Muhtorov in this case.

The government tries to brush off the FISC's decision in a footnote, saying that the opinion addresses the FBI's 2018 procedures "but not the lawfulness of querying under earlier minimization procedures applicable in this case." Gov't Br. 40 n.16. But by all available accounts, the same deficiencies and inadequate safeguards that the FISC faulted in 2018 plagued the FBI's procedures in 2011 when Mr. Muhtorov was investigated. *See* PCLOB Report 59 (describing routine FBI querying of Americans' communications); *United States v. Hasbajrami*, 945 F.3d 641, 658 (2d Cir. 2019) (improved querying rules "were not in place" when the defendant was surveilled in 2011). The government does not even argue that the FBI procedures governing the surveillance of Mr. Muhtorov were any more protective than those the FISC found unreasonable.

The government is also wrong to suggest that the Court can simply ignore its backdoor searches in resolving this case. Gov't Br. 45. It is black-letter Fourth

Amendment law that the reasonableness of electronic surveillance is evaluated under "the totality of the circumstances"—which includes the rules dictating how sensitive communications may be acquired, retained, and *used*. *See, e.g.*, *In re Directives*, 551 F.3d 1004, 1012 (FISCR 2008); [*Redacted*], 2011 WL 10945618, at *27-28 (FISC Oct. 3, 2011). Elsewhere, the government has conceded that the querying rules bear directly on reasonableness. [*Redacted*], Mem. Op. at 40 (FISC Nov. 6, 2015), https://bit.ly/3487WWE. The querying rules go to the heart of this analysis because, as the FISC recognized, they have dramatic implications for the privacy of Americans. [*Redacted*], 402 F. Supp. 3d at 87.

The government does not deny that Mr. Muhtorov was subjected to warrantless backdoor searches in the course of the government's investigation. The rules governing those searches are therefore an inescapable part of the Court's Fourth Amendment analysis. Because those rules encouraged "maximal" querying with minimal protections, they are unreasonable. The Court need go no further than the FISC to hold that the surveillance of Mr. Muhtorov was unlawful.

2. The government's querying of Mr. Muhtorov's communications was a "separate Fourth Amendment event" that required a warrant.

The Second Circuit's recent decision in *Hasbajrami* provides another ground for holding the surveillance here unlawful: because the government's querying of an American's communications under Section 702 is a "separate Fourth

Amendment event" that must independently satisfy constitutional requirements. 945 F.3d at 670. Regardless of whether the *initial seizure* of Mr. Muhtorov's emails was permissible, the government was required to obtain a warrant or individualized judicial approval before agents deliberately queried Mr. Muhtorov's protected communications. Def. Br. 29, 37; *see* Br. of Amici Curiae Medine & Franklin 15-19.

Although the government takes issue with the Second Circuit's conclusions, Gov't Br. 42, it has not appealed that decision. The Second Circuit was right: when agents set out to query an American's communications under Section 702, that represents a separate Fourth Amendment event. At that point, the target of the surveillance has changed, and so has the nature and degree of the intrusion on protected communications. As the Supreme Court has recognized in a variety of contexts—including digital searches—a search that relies on an exception to the warrant requirement is strictly limited by its original justification. *Terry v. Ohio*, 392 U.S. 1, 19 (1968); *Riley v. California*, 573 U.S. 373, 400-01 (2014); *see also Hasbajrami*, 945 F.3d at 670-71 (reviewing cases). To intrude further, the government must obtain new authority. *Riley*, 573 U.S. at 404.

The government's effort to distinguish this line of cases is unpersuasive. The government admits that courts have required an "additional" Fourth Amendment showing when "the government obtained information that was beyond the scope of

the original warrant *or warrant exception*." Gov't Br. 42 (emphasis added). Here, the warrant exception invoked by the government is based solely on the foreign target's lack of Fourth Amendment rights. When government agents turn their focus instead to querying and examining a specific American's private communications—communications the government knows *are* protected—it can no longer rely on the original warrant exception. At that point, the Fourth Amendment requires a higher showing sufficient to satisfy the American's rights.

The government suggests that agents conducting backdoor searches are not really "obtaining" new information because the communications have already been collected, Gov't Br. 42, but that is no defense. In *Riley* and *Sedaghaty*, the government had already lawfully seized the entire contents of the cell phones and computer hard drives at issue. *Riley*, 573 U.S. at 402; *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013). Nonetheless, agents were required to seek further judicial approval before examining that protected data in new ways or for a new purpose. *See also United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999). The government argues that its minimization procedures already permit agents to "review" collected communications, Gov't Br. 43; but that says nothing

about whether the Fourth Amendment requires more when an agent uses a query to specifically target an American.[2]

Indeed, there are two practical reasons why backdoor searches are a categorically different kind of intrusion from the possibility of manual review. First, many communications collected under Section 702 are never manually reviewed. PCLOB Report 128-29 ("NSA analysts do not review all or even most communications."). The scale of the surveillance is too vast, with billions of communications stored for years, and thus many communications would never be examined by an agent absent a backdoor search. *See Hasbajrami*, 945 F.3d at 671; [*Redacted*], 402 F. Supp. 3d at 75. Second, a query is comprehensive. Where an agent might review a small subset of communications in the course of pursuing a foreign target, a backdoor search is a deliberate effort to retrieve *all* of an American's communications sitting in the Section 702 databases. *See Hasbajrami*, 945 F.3d at 672 ("[Q]uerying is problematic because it may make it easier to target wide-ranging information about a given United States person.").

The government falls back on cases involving DNA matching to defend its backdoor searches here, Gov't Br. 41, but those cases are inapt. They uniformly

[2] *Sedaghaty* illustrates this point. In cases involving computer hard-drive searches, agents are also permitted to review the entire contents of the hard-drive to find evidence responsive to the original warrant. But when agents decide to look for evidence of a new crime, they must "obtain a new warrant." 728 F.3d at 913.

hold that such matching—which involves comparing "noncoding" segments of DNA—does not implicate a reasonable expectation of privacy in the first place. *See, e.g.*, *Maryland v. King*, 569 U.S. 435, 464 (2013) (stating that the DNA segments "do not reveal the genetic traits of the arrestee"). In contrast, here, it has been well-established since *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a reasonable expectation of privacy in their electronic communications. When agents query and then read through Americans' emails, they are indisputably intruding on protected privacy interests.

* * *

The government makes one final attempt to keep the Court from ruling on its backdoor searches of Mr. Muhtorov: it claims that its evidence was not "obtained or derived" from those specific searches. Gov't Br. 45. That argument, however, was waived. The government did not raise it below. Nor did the district court address it. Instead, the government argued at length that its warrantless backdoor searches of Section 702 information were lawful. V1 at 817-21. Absent a showing of good cause, which the government has not made here, this Court will not consider suppression arguments raised for the first time on appeal. *See United States v. Martinez*, 643 F.3d 1292, 1298 (10th Cir. 2011) (refusing to consider new government argument).

If the Court considers this new claim at all, including arguments in the government's classified brief, it must provide Mr. Muhtorov the opportunity to inquire into the underlying facts and to address how Fourth Amendment suppression rules apply. FBI agents conduct backdoor searches so frequently that they may have contributed to the investigation of Mr. Muhtorov in multiple ways, not only through the government's FISA application. Questions about whether evidence is "derived from" a search are legally and factually complex, yet the defense has not received access to any of the facts as due process requires. *See Alderman v. United States*, 394 U.S. 165, 182-85 (1969). The Court should not entertain this new claim at all, but certainly not on the basis of a secret, one-sided submission.

B. No Fourth Amendment exception excuses the government's warrantless surveillance of Mr. Muhtorov.

Regardless of whether the Court holds the government's backdoor searches unlawful, the warrantless collection and use of Mr. Muhtorov's emails violated the Fourth Amendment.

The government makes a practical argument that should be dispensed with at the outset. It claims that if a warrant protected the communications of Americans here, the government would be required to obtain a warrant before it could ever target *any* foreigner—on the off-chance that an American's communications might be swept up. Gov't Br. 23. That is a straw man. The government could satisfy the

Fourth Amendment by requiring judicial approval to retain and use Americans' communications *after* the initial seizure, just as Congress has done for analogous surveillance directed at foreign powers on U.S. soil. *See* 50 U.S.C. § 1801(h)(4); Part I.C, *infra*.

For the reasons below, the government's legal arguments—which seek to establish a sweeping exception to the warrant requirement—fare no better.

1. The government cannot evade the warrant requirement simply by "targeting" the foreign end of Americans' communications.

Government agents have never been permitted to intercept Americans' international phone calls or emails without a warrant simply by claiming they are "targeting" a foreigner on the other end. But that is the novel theory the government advances here. Gov't Br. 22. The breadth of this argument is some of the clearest proof that it is wrong.

The Fourth Amendment's protections do not depend on whom the government purports to be "targeting." They turn on *what* it is searching. *See* Orin Kerr, *The Surprisingly Weak Reasoning of* Mohamud, Lawfare (Dec. 23, 2016), https://bit.ly/2PfkPWx ("There is no 'targeting' doctrine in Fourth Amendment law."). The critical issue for Fourth Amendment purposes—including in the wiretapping context—is whether there is a protected privacy interest in the communications the government is searching. *See Katz*, 389 U.S. at 352-53. When

it comes to emails and phone calls involving Americans, it is undisputed that such a privacy interest is present. That fact alone sets this case apart from *Verdugo-Urquidez*, which involved the physical search of a Mexican citizen's residence in Mexico. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 278 (1990) (Kennedy, J., concurring) ("The rights of a citizen, as to whom the United States has continuing obligations, are not presented by this case."). The Fourth Amendment analysis has a different starting-point here, where the government is compelling U.S. companies to divulge emails involving a U.S. resident in Colorado. When an American's constitutional interests are in jeopardy, the government cannot ignore those interests by focusing exclusively on the foreign end.[3]

The government's targeting theory is quite new and quite radical, not least because it would sweep far beyond Section 702. Consider ordinary criminal investigations: FBI agents, DEA agents, and even municipal police departments regularly investigate transnational crimes, including financial fraud, theft of trade secrets, and drug trafficking. Yet those agents have never been permitted to warrantlessly listen in on cross-border phone calls that involve Americans, or warrantlessly seize Americans' international emails, simply by insisting that they

[3] Contrary to the government's claim, the location of the surveillance also matters. *Verdugo-Urquidez* involved searches on foreign soil—where no U.S. court had authority to issue a warrant. The same cannot be said of searches under Section 702, which occur on U.S. soil and are well within the reach of legal process.

are "targeting" the foreign end. They have never been permitted to dispense with Americans' core Fourth Amendment protection so easily. Yet that is exactly the upshot of the government's claim here.

2. The incidental overhear cases do not establish an exception to the warrant requirement.

Both the government and *Hasbajrami* (in a separate portion of the opinion) rely heavily on incidental overhear cases involving traditional wiretaps. But those cases do not save the surveillance here for at least three reasons.

First, Section 702 surveillance is not analogous to a traditional Title III wiretap, where multiple preconditions strictly limit the extent of any "overhearing." Under Title III, the government must make a predicate showing of probable cause and necessity; minimization takes place in real time; and officers must limit collection to conversations that are evidence of criminal activity. The resulting collection is narrow. Under Section 702, by contrast, the government surveils more than 160,000 individuals and groups with no showing of suspicion; there is no real-time minimization; and the government is amassing all of the communications to and from its targets, regardless of what they contain, in vast databases available to agents around the country. PCLOB Report 128-29. The resulting collection is immense.

Second, the incidental overhear cases all involve a threshold showing that is absent here—a government showing of probable cause and particularity that

satisfies the Fourth Amendment rights of Americans. For a domestic wiretap, that initial showing provides all the constitutional authority the government needs. Def. Br. 30-32. The Second Circuit's opinion in *Hasbajrami* glossed over this critical fact. *See* 945 F.3d at 663-64. But as the cases cited in *Hasbajrami* show, the incidental overhear rule applies when the original search was authorized by a judge based on a finding of probable cause. *See United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973) ("If probable cause has been shown as to one such participant, the statements of the other participants may be intercepted if pertinent to the investigation."); *United States v. Donovan*, 429 U.S. 413, 428 (1977); *United States v. Figueroa*, 757 F.2d 466, 470-71 (2d Cir. 1985); *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009). Because the warrants operated to safeguard the privacy interests of any Americans who were overheard on the wiretaps, the government was not required to obtain further judicial approval. *See* Br. of Amicus Curiae Brennan Ctr. 14-24.

Under Section 702, however, the government does not make a comparable showing that would satisfy the Fourth Amendment interests of the Americans it is surveilling. Instead, the government justifies its warrantless collection based on nothing more than the fact that its target is one of several billion non-U.S. persons abroad. There is no basis to find that a foreigner's lack of Fourth Amendment rights eliminates *Mr. Muhtorov's* core constitutional protections. Americans

remain entitled to Fourth Amendment safeguards, at least where the government retains and uses communications that it knows involve an American—as it did here.

In extending the incidental overhear cases to sweeping *warrantless* surveillance, the Second Circuit made a dramatic leap. It reasoned that the incidental overhear doctrine applies whenever surveillance is "lawful." *Hasbajrami*, 945 F.3d at 664. But that reasoning is circular. The very question the Court is considering in this case is whether the surveillance was lawful. The Second Circuit presumed that the lawfulness of the surveillance could be assessed based on the "target" alone, but that approach is at odds with Fourth Amendment law. The target is only half the picture. Communications typically have at least two participants, and what matters for Fourth Amendment purposes is whether *either* of those individuals has a protected privacy interest in the communications. *See Katz*, 389 U.S. at 352-53; *supra* Kerr, *The Surprisingly Weak Reasoning of* Mohamud.

Third, the implications of the government's novel legal theory are far-reaching. Its argument would transform the overhear rule, which has long been tethered to an initial showing of probable cause, into a license to intercept and then exploit Americans' international communications without any showing of cause. Rules developed in the era of individualized surveillance cannot be applied blindly to sweeping programs of suspicionless surveillance. *See Riley*, 573 U.S. at 392-93;

Carpenter v. United States, 138 S. Ct. 2206, 2217-18 (2018) (recognizing that broad collection of data raises different constitutional questions).

3. No foreign intelligence exception to the warrant requirement applies.

Despite the government's claims, no court of appeals has endorsed a foreign intelligence exception as broad as the one the government asserts here. FBI agents and NSA analysts have never had the power to intrude on Americans' protected communications simply because they claim to be seeking "foreign intelligence information"—an expansive, nebulous category that includes any information relating to the "foreign affairs" of the United States. 50 U.S.C. § 1801(e). Rather, such an exception has consistently involved surveillance directed at foreign agents or foreign powers, and it has been based on a finding of probable cause by the Attorney General or the President. Def. Br. 35 (citing cases); PCLOB Report 90 n.411. Those limitations ensure that any warrantless surveillance for foreign intelligence purposes is narrow and is not improperly exploited. *See United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 320 (1972).

The Supreme Court's decision in *Keith* recognized these dangers and warned against them—including the dangers of incidental collection. *Keith*, 407 U.S. at 316-21, 326 ("Even the most innocent and random caller who uses or telephones into a tapped line can become a flagged number in the Government's data bank."). The framework contemplated by *Keith* was not a regime of warrantless

surveillance, as the government suggests, but the framework found in the original provisions of FISA, which was enacted after the Supreme Court's decision and after the Church Committee's watershed findings. *See* 50 U.S.C. § 1805. While FISA modified the probable-cause showing, it still required individualized court approval. Neither FISA nor *Keith* authorized the government to intercept Americans' phone calls and read their messages without that protection.

Lastly, the government concedes that the foreign intelligence exception recognized in *In re Directives* was far narrower than the one it urges here. Gov't Br. 27. It tries to explain away that decision by claiming that the court was addressing only surveillance "targeting" U.S. persons. Yet nothing in the court's discussion of the foreign intelligence exception distinguishes between U.S. person and non-U.S. person targets. *See In re Directives*, 551 F.3d at 1010-12. That is unsurprising given that the communications of innocent U.S. persons may be swept up in large quantities regardless of whether the original targets are U.S. persons or not.

In short, no court of appeals has ever recognized a foreign intelligence exception that would, in one fell swoop, extinguish the warrant requirement for every American who happens to communicate with the 160,000 foreigners targeted under Section 702.

C. There are reasonable safeguards that would protect Americans' privacy.

Even if the Court finds that the warrant requirement affords no protection to Americans in these circumstances, the surveillance of Mr. Muhtorov was unreasonable. The government's mass surveillance regime is broader and more intrusive than the government acknowledges. Most importantly, the government has reasonable alternatives that would allow it to access the communications of its foreign targets while adequately protecting Americans' privacy.

The government protests that Section 702 is not "bulk" collection, arguing that it is "sufficiently focused." Gov't Br. 35. But Section 702 does not involve particularity in any sense the Fourth Amendment would recognize. The standards governing this surveillance are extraordinarily permissive on virtually every axis, allowing the government to ingest vast quantities of communications. For example, the government says that it targets "specific non-U.S. person[s]," *id.*, but it omits the fact that "persons" are not only individuals, "but also groups, entities, associations, corporations, or foreign powers." PCLOB Report 20-21. Thus, an entire foreign government can be a single target. *Id.* Moreover, for each targeted individual or group, the government may surveil any and all "selectors"—phone numbers, email addresses, IP addresses, or other identifiers—that it believes are associated with the target. *See* Charlie Savage, et al., *Hunting for Hackers, NSA Secretly Expands Internet Spying at U.S. Border*, N.Y. Times, June 4, 2015,

https://nyti.ms/2RfT9Uz. Some of these selectors may be used by hundreds of different people. Because the threshold for targeting a person or group is so low, and because the FISC never reviews a single targeting decision, the number of surveillance targets has ballooned to more than 160,000 per year. Every single communication between an American and one of these individuals or groups is collected and stored in the government's databases.[4]

Against this backdrop, stronger safeguards for Americans are reasonable and necessary.

Most significantly, the procedures fail to require individualized judicial approval at any point—even after the fact, and even when the government seeks to retain and use the communications of a *known* U.S. person. The limited record in this case does not resolve how agents came to review Mr. Muhtorov's communications in the first place, and without a proper factual inquiry, the Court should not presume or conclude that it was simply accidental. But even if that review was initially inadvertent, the Fourth Amendment requires agents to pause,

[4] The government suggests that Americans have a "diminished" privacy interest in these communications because they have been transmitted to someone else. Gov't Br. 30. This vague claim is at odds with black-letter law. *See* Def. Br. 45 n.18. Virtually every protected email or phone call is transmitted to someone else. In addition, Section 702 communications are not obtained directly from foreign recipients at all, but from U.S. companies who transmit communications privately. If the Court were to accept the claim that these online messages are somehow "less" protected, it would wreak havoc on protections for modern communication.

segregate the American's protected communications, and obtain court authorization before reviewing or exploiting those communications further.

This basic safeguard is precisely what the Court requires in the context of other electronic searches that present similar risks of overreaching. When government agents are reviewing a hard-drive pursuant to a warrant for evidence of one crime and happen upon evidence of another, they must stop and obtain a second warrant to pursue that second crime. *See Carey*, 172 F.3d at 1276; *Sedaghaty*, 728 F.3d at 913.

Likewise, when government agents are reviewing communications intercepted while targeting a foreign embassy and happen instead upon the communications of an American, they must stop and obtain an order from the FISC. *See* 50 U.S.C. § 1801(h)(4). The government says that even though this kind of warrantless surveillance may closely resemble Section 702, embassy wiretaps are different because the statute requires the government to avoid Americans' communications at the outset. Gov't Br. 36-37. The government's argument, it seems, is that since Section 702 is broader at the outset, it need not have comparable protections for Americans on the back end either. But that is entirely backwards. If Section 702 collection is more likely to sweep in Americans' communications—because it allows the government to warrantlessly surveil a far larger group of targets—then Fourth Amendment reasonableness requires *stronger*

protections on the back end. The special rules for embassy wiretaps exist because Congress recognized in FISA that it would be unlawful for the government to collect Americans' communications under the guise of targeting foreign powers. *See* H.R. Rep. No. 95-1720, at 24-26 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048.

Even with stronger protections for Americans in place, investigators would have multiple avenues to retain, access, and use the communications of Americans where necessary. In exigent circumstances, the government would not need a court order to use communications that revealed an imminent threat. In other cases, it could establish probable cause to believe that either the foreign target or the U.S. person was an agent of a foreign power under FISA. *See* 50 U.S.C. § 1805. Alternatively, it could make a traditional probable-cause showing that the communications would provide evidence of a crime. Finally, even if the government were unable to immediately show probable cause, the communications could be segregated and preserved for a reasonable period of time, ensuring that they remained available upon an adequate showing of need.

There may be other reasonable approaches, which could be implemented through strengthened procedures. *See United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (observing that the warrant requirement is flexible). The Court need not prescribe the exact procedures here, just as the Supreme Court did not resolve all

such questions in *Berger* or *Keith*. *See Berger*, 388 U.S. at 60; *Keith*, 407 U.S. at 321-24. The Court need only hold that the protections in this case were inadequate.

D. The warrantless surveillance of Mr. Muhtorov violated Article III of the Constitution.

Section 702 violates Article III's "case or controversy" requirement because the statute requires FISC judges to issue advisory opinions addressing the constitutionality of abstract procedures in the absence of concrete facts. Def. Br. 47-50. It is plain that a federal court could not adjudicate, at the request of the Denver Police Department, the constitutionality of the department's new policies governing its officers' use of force. Nor could a court take up a request by the Transportation Security Administration to pass generally upon the reasonableness of new agency procedures concerning airport screening. "If 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). So too here—and none of the government's arguments to the contrary has merit.

The government's attempt to analogize the FISC's annual review of Section 702 procedures to the individualized review of "warrant and wiretap applications" is far-fetched. Gov't Br. 46-47. The problem is not that the FISC's review is one-sided, but that it is a free-floating review of general procedures, divorced from any actual case. A warrant or wiretap application presents a "case or controversy"

because it requires courts to determine whether the specific facts presented by the government amount to probable cause, and whether the specific search contemplated is consistent with the Fourth Amendment. *See United States v. Megahey*, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982). Review of Section 702 could not be more different. The FISC doesn't review facts, but multiple sets of abstract procedures—rules the agencies propose to use in surveilling an unspecified number of people targeted for unspecified reasons using a variety of different techniques. 50 U.S.C. § 1881a. The application of these procedures to actual people and facts is performed by low-level intelligence analysts, not by any judge. PCLOB Report 42. In short, the FISC is asked to opine on the lawfulness of an entire year's worth of mass surveillance without reviewing a single targeting decision and without knowing how any one of these searches affects Americans.

The government also errs in likening the FISC's role to that of a court examining the facial constitutionality of a statute in a civil challenge. Gov't Br. 47. Before a court entertains a facial challenge, it must still be presented with an actual "case or controversy" under Article III—that is, a party that suffered a concrete injury flowing from the searches. *See City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2448 (2015) (plaintiff motel operators had been "subjected to mandatory record inspections" under the challenged ordinance). By contrast, under Section 702, there is no party before the FISC describing how the surveillance has injured them, nor

do the government's procedures or certifications identify any particular person who will be injured by the surveillance.

Finally, the government's argument that Mr. Muhtorov has not shown that this violation of Article III injures him is wrong. The government intercepted Mr. Muhtorov's communications based on the FISC's annual authorization, invading his privacy and ultimately using the intercepted communications to prosecute him. Those are well-recognized injuries. *See Berger*, 388 U.S. at 45-53. If the claim is that these injuries are not attributable to the FISC's improper role, but solely to the government, that is untenable. The government could not have conducted the challenged searches without the FISC's approval. 50 U.S.C. § 1881a. Indeed, the government repeatedly argues that it is the FISC's blessing that makes this surveillance lawful. *See* Gov't Br. 34, 38. When a court acts beyond its power to authorize a search, a defendant clearly may challenge the resulting intrusion. *See United States v. Krueger*, 809 F.3d 1109, 1113 (10th Cir. 2015); *id.* at 1123-24 (Gorsuch, J., concurring).

E. The good-faith exception does not apply.

The good-faith exception to the exclusionary rule does not apply to FISA's statutory suppression remedy.

The suppression remedy that Congress enacted in FISA is mandatory. 50 U.S.C. § 1806(g). Accordingly, if the Court finds that the government's

surveillance of Mr. Muhtorov was unlawful, it must order suppression under Section 1806(g). Because suppression is required by the statute, it "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). In other words, the limits on the *judicially created* exclusionary rule do not apply to the *statutory* exclusionary rule at issue here. As with Title III wiretaps, the good-faith exception to the Fourth Amendment's exclusionary rule simply 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."). Simply put, when the Supreme Court first recognized the good-faith exception in 1984, *see United States v. Leon*, 468 U.S. 897 (1984), it could not have retroactively amended the mandatory suppression requirement that Congress imposed in FISA in 1978.[5]

The government nonetheless argues, based on *Illinois v. Krull*, 480 U.S. 340 (1987), that the good-faith exception applies because agents acted in "objectively reasonable reliance on a statute." Gov't Br. 49. This argument is untenable. First, unlike the statute at issue in *Krull*, FISA has its own suppression provision.

[5] The Tenth Circuit has not decided "whether the good-faith exception applies in the Title III context." *United States v. Barajas*, 710 F.3d 1102, 1110 (10th Cir. 2013).

Congress conducted its own balancing of interests in choosing this remedy, and there is no basis for the courts to overturn that legislative judgment. Indeed, to apply the good-faith exception here would effectively nullify FISA's statutory suppression remedy. It would allow the government to circumvent Congress's chosen remedy simply by pointing back to the statute itself. That plainly is not what Congress intended. Finally, even under *Krull*, reasonable government officials "should have known that the statute was unconstitutional," 480 U.S. at 355, given its manifest and multiple infirmities. *See* Def. Br. 13-50; *supra* Part I.A-D.

II. FISA and due process require the disclosure of Section 702 and FISA materials.

The government spends barely two pages contending with the claim that the defense was entitled to disclosure of key surveillance materials. It appears to believe that the disclosure provisions Congress enacted in FISA are simply a nullity. But this cursory treatment is sharply at odds with mounting evidence—compiled by the Department of Justice's Inspector General—of widespread problems in the government's FISA applications. Especially when the government employs novel and complex surveillance tools, as it did here, disclosure is necessary for a district court to accurately determine whether the surveillance was lawful.

A. This Court reviews the district court's decision to deny disclosure de novo.

The government asserts, incorrectly, that this Court should review the district court's disclosure decision for abuse of discretion. Gov't Br. 49. Here, the district court legally erred. Def. Br. 56-63. This legal interpretation is reviewed de novo. Def. Br. 52-53; *El Encanto, Inc. v. Hatch Chile Co.*, 825 F.3d 1161, 1162 (10th Cir. 2016) (Gorsuch, J.).

B. Disclosure is "necessary" in cases involving complex issues, like Mr. Muhtorov's.

The government suggests that FISA effectively bars disclosure to defense counsel, Gov't Br. 51, but that is flatly incorrect. The statute, Congress, and the courts all recognize that disclosure may be necessary in FISA cases—including where, as here, factual or legal issues are particularly complex. Def. Br. 55-56.

By categorically denying disclosure, courts have not "uniformly followed" FISA's procedure. Gov't Br. 51. The government's claim ignores the fact that FISA itself requires disclosure in at least some cases—complex ones—and contains procedures to facilitate such disclosure. *See* 50 U.S.C. §1806(f); *United States v. Belfield*, 692 F.2d 141, 147-48 (D.C. Cir. 1982); Br. of Amici Curiae Church Committee Staff. That other courts have denied disclosure in other cases cannot alter the statute or Congress's plain intent. Moreover, courts have increasingly recognized that the complete absence of disclosure is in conflict with

defendants' constitutional rights. *See United States v. Daoud*, 755 F.3d 479, 485-86 (7th Cir. 2014) (Rovner, J., concurring). Yet the government simply ignores Mr. Muhtorov's arguments that FISA must be construed to require disclosure consistent with the Fourth and Fifth Amendments. Def. Br. 63-66.

Notably, the government also fails to dispute the complexity of any of the legal, factual, or technological questions raised by the surveillance of Mr. Muhtorov. Def. Br. 56-63. Because this case is indisputably complex, disclosure is required.

C. Widespread FISA abuses identified by the DOJ Inspector General underscore the need for disclosure and adversarial litigation here.

Recent revelations about egregious errors in the FBI's applications to surveil Carter Page, and chronic problems found in other FISA applications, underscore the critical need for disclosure. Two DOJ Inspector General reports demonstrate the risk of error inherent in an ex parte process: they show that courts simply are not in a position to identify, by themselves, material misrepresentations and omissions that appear in the government's FISA applications. That risk of error is even greater here, given the complexity of the surveillance at issue.

In December 2019, the DOJ Inspector General released a report examining the FBI's surveillance of Carter Page under FISA. *See* DOJ OIG, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019), https://bit.ly/2sOu8H4. The report's conclusions were

sobering. The Inspector General identified seventeen separate problems with the FBI's applications to the FISC—including repeated misrepresentations, factual inaccuracies, and material omissions. *See id.* at viii–xii.

The problems documented by the Inspector General went to the heart of the government's applications, undercutting its claims that there was probable cause to intercept Page's communications. And nothing suggests that the Page applications were unique in their defects. To the contrary, one would have expected FBI and DOJ officials to exercise special care in seeking to surveil a former campaign official. *See id.* at xiv. In response, the FISC expressed pointed concern that the errors in the Page applications are part of a larger, systemic pattern. "The frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable." Order at 3, *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02 (FISC Dec. 17, 2019), http://bit.ly/2sRChus.

In a subsequent audit, the Inspector General confirmed that similar problems have plagued the FBI's FISA applications for years. DOJ OIG, *Management Advisory Memorandum* (Mar. 2020), https://bit.ly/2XdEqxk. The audit examined dozens of cases to determine whether the FBI had complied with agency

procedures that are supposed to ensure its FISA applications are "scrupulously accurate." *Id.* at 2-3. The Inspector General found problems in every single one.

These widespread problems have revealed a persistent blind spot in the ex parte process by which FISA applications are reviewed: neither the FISC, nor any other court, is in a position to singlehandedly assess whether the government's applications are accurate and complete. Until now, many courts seem to have accepted the notion that the FISA process was immune to serious error. That view is no longer tenable. The Court should require disclosure of the FISA materials because it is "necessary" to ensure that the surveillance of Mr. Muhtorov was lawful. Def. Br. 68.

D. The government's public disclosures of Section 702 and FISA materials show that its blanket claim of secrecy cannot be justified.

The government does not even defend its claim that every last word in its Section 702 and FISA materials is genuinely sensitive. Its silence is unsurprising, because the government's extensive public disclosures show that the claim is not remotely true. As just one example: the government has disclosed the various FBI Section 702 minimization procedures in effect between 2014 and 2019, but it has

refused to disclose to Mr. Muhtorov the same procedures that were in effect when he was surveilled.[6]

The government's withholding of these crucial materials based on overbroad claims of secrecy violates due process. When the government's claims of secrecy are false or exaggerated, they cannot overcome a defendant's constitutional interest in a fair, adversarial proceeding. *See Roviaro v. United States*, 353 U.S. 53, 60-61 (1957); *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976).

At a minimum, as Mr. Muhtorov detailed in his opening brief, he was entitled to disclosure of FISA materials comparable to those the government has already released to the public without harm. Def. Br. 67-68.

III. Mr. Muhtorov is entitled to notice and the opportunity to challenge the other novel surveillance tools the government used in its investigation.

In conducting wide-ranging surveillance of Mr. Muhtorov's activities and communications, the government undoubtedly relied on surveillance tools beyond Section 702 and FISA, such as Executive Order 12,333. Def. Br. 71-76. The government claims that Mr. Muhtorov has no right to notice of these other surveillance techniques, and that any use of the Classified Information Procedures

[6] *See*, *e.g.*, FBI Section 702 Minimization Procedures (2015), https://perma.cc/G3X4-FT92; Georgetown University, *Foreign Intelligence Law Collection*, https://bit.ly/2vm4URD (cataloging hundreds of FISA opinions, orders, and other materials that have been declassified and released).

Act ("CIPA") to conceal them was lawful. But the government's argument is entirely at odds with longstanding Supreme Court precedent. The law is clear: Mr. Muhtorov is entitled to notice and an opportunity to meaningfully challenge the government's surveillance of him.

A. This Court reviews de novo the legal question of whether Mr. Muhtorov is entitled to notice.

Contrary to the government's claim, Gov't Br. 53, this Court reviews de novo the legal questions of whether Mr. Muhtorov is entitled to notice of the surveillance techniques used against him, and whether due process forecloses the government from using CIPA to secretly litigate "fruit of the poisonous tree" issues. Def. Br. 71; *United States v. Lustyik*, 833 F.3d 1263, 1267 (10th Cir. 2016); *El Encanto, Inc*, 825 F.3d at 1162 (legal error is per se an abuse of discretion).

B. The Constitution, statutory law, and the Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice of the government's surveillance tools.

The government contends that neither *Brady*, nor the Federal Rules of Criminal Procedure, nor any other authority entitles Mr. Muhtorov to notice of the government's surveillance tools. Gov't Br. 53. That view is wrong.

The government muddies the waters by suggesting that Mr. Muhtorov's request for notice is far broader than it actually is. *See id.* Mr. Muhtorov is not seeking to rummage through the government's files. Nor is he urging this Court to

conclude that he has a general constitutional right to discovery. Instead, he is simply asking this Court to apply controlling law, which requires tailored disclosures about the government's surveillance of Mr. Muhtorov.

1. The Fourth and Fifth Amendments entitle Mr. Muhtorov to notice.

Three distinct lines of precedent make clear that the Fourth and Fifth Amendments entitle Mr. Muhtorov to notice. In its response, the government either half-heartedly attempts to distinguish these cases or ignores them altogether. This Court should reject the government's efforts to brush aside controlling case law and should hold that notice is constitutionally required here.

First, the Supreme Court and appellate courts have long recognized that the Constitution requires notice of government searches—especially surreptitious searches. Def. Br. 78 (citing *Berger*, 388 U.S. at 60, and *Dalia v. United States*, 441 U.S. 238, 247-48 (1979)); *Donovan*, 429 U.S. at 429-30 & n.19 (Title III's notice provisions "satisfy constitutional requirements"); *United States v. Chun*, 503 F.2d 533, 536-38 & n.6 (9th Cir. 1974) (same).

Faced with the weight of this authority, the government has little to say. It contends that *Berger* and *Dalia* do not "establish a right to disclosure of each surveillance technique used by the government," Gov't Br. 55-56, but the cases make clear that the Constitution requires notice of secret government searches. While *Berger* and *Dalia* do not require disclosure of every last technical detail

about the government's surveillance techniques, they require notice of basic information about the searches, so that (among other things) a defendant may bring an informed motion to suppress. *See Berger*, 388 U.S. at 60; *Dalia*, 441 U.S. at 247-48. Moreover, there is simply no basis for concluding that this constitutional notice requirement evaporates in the foreign intelligence context. *See* Gov't Br. 56. Congress has legislated in recognition of the principle that notice of foreign intelligence surveillance is required. *See* 50 U.S.C. § 1806(c) (requiring notice of FISA surveillance in criminal proceedings).

Second, due process entitles defendants to a meaningful opportunity to pursue the suppression remedy. Def. Br. 63-64. The government does not disagree with this contention. As a matter of logic, then, it follows that notice is required, because notice is indispensable to the exercise of that due process right. *Id.* at 75. *Alderman* strongly supports the proposition that the government must disclose surveillance materials to defendants as a matter of due process, even in national security cases. Def. Br. 78. The government attempts to distinguish *Alderman* because the government there had conceded that its surveillance was illegal. Gov't Br. 54. But the Supreme Court's holding did not turn on that fact, *see Alderman*, 394 U.S. at 183-85, and such a rule would be incoherent. A defendant's right to seek suppression cannot depend on whether the government agrees that its search was unlawful.

Third, at a minimum, the rights articulated in *Brady* require disclosure of information that could affect the outcome of a suppression hearing. *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000); *Smith v. Black*, 904 F.2d 950, 965-66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992). Notice of secret surveillance is plainly information that could affect the outcome of a suppression hearing. While the government acknowledges that *Brady* is one source of its disclosure obligations, Gov't Br. 53, it fails to address the cases holding that *Brady* requires disclosure here.

2. 18 U.S.C. § 3504 entitles Mr. Muhtorov to notice.

As to 18 U.S.C. § 3504, the government contends that its response regarding E.O. 12,333 surveillance was sufficient, and that it had no further disclosure obligations under the statute. It is wrong on both counts.

First, the government's carefully worded response was plainly insufficient. The government never denied that Mr. Muhtorov was subjected to surveillance under EO 12,333; instead, it denied that its trial evidence was the product of such surveillance or that Mr. Muhtorov was "aggrieved." Gov't Br. 62-63. But that gets it backwards.

Section 3504 does not permit the government to condition notice on its *own* determination of whether its evidence was tainted. Rather, upon a colorable claim like Mr. Muhtorov's, the statute requires the government to affirm or deny the

surveillance. *See* 18 U.S.C. § 3504(a)(1); *United States v. Apple*, 915 F.2d 899, 904-06 (4th Cir. 1990). It is *then* up to the parties to litigate whether the surveillance was unlawful and which evidence flowed from it. *See United States v. Hamide*, 914 F.2d 1147, 1149 (9th Cir. 1990); *Apple*, 915 F.3d at 906, 909-10. This Court should reject the government's attempt to avoid notice by preemptively resolving these questions in its own favor. *See Matter of Grand Jury*, 524 F.2d 209, 216 (10th Cir. 1975) (per curiam) ("[I]f the government's position is to be denial, it should be given in absolute terms . . . . This is no place for ambivalent statements or loopholes.").

Next, the government argues that it had no further disclosure obligations because Mr. Muhtorov didn't make the necessary showing. But the government ignores that the threshold is low: a cognizable claim for notice entails a "mere assertion" that illegal surveillance has taken place and a "colorable basis" that the party was aggrieved. *Apple*, 915 F.2d at 905.[7] And Mr. Muhtorov offered far more than just speculation or suspicion. He pointed to specific facts in his case indicative

[7] The government's attempt to discount *Apple* is unavailing because it focuses on the wrong facts. "[U]nlike in most" Section 3504 cases, in *Apple* there was no question about the existence, and type, of surveillance—a tapped phone. In that unusual posture, the Fourth Circuit concluded that a defendant who claimed she had a conversation on that line made a sufficient Section 3504 showing, while another defendant who made no such claim did not. That's sensible enough under the circumstances, since specificity was possible, but it doesn't provide much instruction here, where the government continues to conceal so much about the surveillance.

of surveillance, along with public disclosures of an array of novel surveillance techniques the government employs. *E.g.*, V1 at 1134-44, 1152, 1231-39; V3 at 364-82.

Finally, the government observes that Section 3504 applies to the use of a "device" in violation of law, in an effort to exempt location data and call records from the statute. Gov't Br. 60. That's a distraction. What's far more important is that the government does not contest that Section 3504 requires notice of other types of surveillance—including surveillance under E.O. 12,333. The government employed a variety of forms of surveillance in its investigation, V3 at 382; Def. Br. 71-75, but has refused to disclose many of those methods. Section 3504 was intended to provide a right to notice of surreptitious surveillance in precisely these circumstances.

3. The Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice.

As to Rule 16, the government tries to complicate something that is simple. In fact, both provisions Mr. Muhtorov cited support his request for notice.

The government plainly surveilled Mr. Muhtorov in multiple ways, some still unknown. Far from a "fishing expedition," his targeted request for notice of surveillance techniques more than met Rule 16(a)(1)(E)'s "materiality" requirement. *See* 2 Fed. Prac. & Proc. Crim. § 254 (4th ed.) ("Too much should not be required in showing materiality."). He identified specific programs the

government likely relied on, ones that present significant constitutional problems. Def. Br. 71-77. And Rule 16(a)(1)(E) plainly "permits discovery related to the constitutionality of a search or seizure." *United States v. Soto-Zuniga*, 837 F.3d 992, 998, 1000-01 (9th Cir. 2016).

Nor is the government's representation that it provided Mr. Muhtorov with the "substance" of his "relevant" written or recorded statements sufficient to establish its compliance with Rule 16(a)(1)(B)(i). Gov't Br. 58. By its own terms, the rule speaks to "statements," not their "substance"; and it does not make the government the arbiter of relevance. *See generally* Wayne R. LaFave, et. al., 5 Crim. Proc. § 20.3(c) (4th ed.). Rather, the rule presumes broad disclosure of "a prior statement in the possession of the government," which this Court has recognized "may be the single most crucial factor in the defendant's preparation for trial." *United States v. Scafe*, 822 F.2d 928, 935-36 (10th Cir. 1987).

4. *Carpenter* and *Clapper* show that notice is essential.

For at least three reasons, the government's analysis of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), is incorrect.

First, the government misses the point of Mr. Muhtorov's discussion of these cases, Gov't Br. 56-58, which is to show the overriding importance of

adversarial litigation in a time of rapid technological advances. Nothing in the government's response undermines that commonsense conclusion.

Second, the government suggests that Mr. Muhtorov is not entitled to notice of the government's collection of his location data or call records, because he would not prevail on a motion to suppress. *See id.* This argument is entirely backwards. It would never be appropriate for the government to withhold *notice* based on its theory that the exclusionary rule might not apply down the line. *See United States v. Leon*, 468 U.S. 897, 906 (1984) (Fourth Amendment violations and the exclusionary rule must be analyzed separately). The question of whether the government violated Mr. Muhtorov's Fourth Amendment rights comes first. And notice is essential to fairly litigating that question.

Third, with respect to location data and call detail records, the good-faith and suppression analysis is considerably more complicated than the government claims. *See, e.g.*, Appellants' Reply 34-37, *United States v. Moalin*, No. 13-50572 (9th Cir. Sept. 2, 2016), ECF No. 63 (extensively briefing application of the good-faith exception to collection of call records). Regardless of whether location data was introduced at trial, Gov't Br. 56, the record shows that agents tracked Mr. Muhtorov's location using undisclosed methods. V1 at 182. That surveillance may well have tainted the trial evidence. This is precisely why notice must come first: so that a defendant has the opportunity to litigate core Fourth Amendment

questions, including whether the government's evidence is fruit of the poisonous tree.

C. The district court erred in allowing the government to conceal novel surveillance of Mr. Muhtorov through CIPA.

By allowing the government to conceal its surveillance techniques through CIPA proceedings, the district court violated both the due process rights recognized in *Alderman* and the CIPA framework itself. The government's few arguments to the contrary are unavailing.

1. *Alderman* forecloses ex parte CIPA litigation over Fourth Amendment suppression issues.

As Mr. Muhtorov has explained, *Alderman* and due process forbid ex parte litigation over Fourth Amendment suppression issues. Def. Br. 84-87. But there is reason to believe that the government litigated precisely these issues in ex parte CIPA proceedings below. Specifically, the government may have argued that Mr. Muhtorov would not prevail on a motion to suppress, and that the surveillance information was thus "irrelevant" for purposes of CIPA. Def. Br. 81-84, 86-87.

To be clear, Mr. Muhtorov is not contesting, as a general matter, the lawfulness of ex parte proceedings under CIPA Section 4. Gov't Br. 67. He is instead challenging the government's use of CIPA to litigate Fourth Amendment suppression issues in one-sided proceedings. Def. Br. 84-87. The government entirely fails to address this argument. Gov't Br. 70.

Applying due process principles, *Alderman* squarely holds that litigation over whether the government's evidence is fruit of the poisonous tree must be adversarial. *Alderman*, 394 U.S. at 168, 180-85. Thus, the government cannot litigate ex parte the question of whether its trial evidence is "too attenuated" from its surveillance, whether it was obtained from an "independent source," or whether the "inevitable discovery" exception applies. Def. Br. 85-86.

2. The CIPA framework compels disclosure.

CIPA was designed to honor the due process rights recognized in *Alderman*, not to thwart them. CIPA "does not expand or restrict established principles of discovery." *Sedaghaty*, 728 F.3d at 904. That includes the disclosure of surveillance materials sufficient for a defendant to fairly litigate suppression issues.

Pursuant to CIPA, the defense should have received disclosures about the government's surveillance techniques—through, for example, declassified summaries or statements of admitted facts. *See* 18 U.S.C. app. III §§ 3-4. This information is plainly discoverable, *see supra* Part III.B, and is "relevant" and "helpful" to a motion to suppress, *United States v. Hanna*, 661 F.3d 271, 295 (6th Cir. 2011); Def. Br. 81-87. Accordingly, CIPA compels its disclosure—and provides secure mechanisms for the government to do so.[8]

[8] The government incorrectly argues that "national security concerns may, on balance, trump the defendant's need for the information that has been found to be relevant and helpful." Gov't Br. 67 n.23. This Court has never handed the

The government contends that information concerning the surveillance of Mr. Muhtorov is not "per se" relevant and helpful to a motion to suppress. Gov't Br. 69. But when the government conducts surveillance in secret, notice is plainly a precondition for any such motion. While the "relevant and helpful" assessment depends on "the particular circumstances of each case," *Roviaro*, 353 U.S. at 62, this is a case involving multiple kinds of intrusive surveillance and undisclosed surveillance tools. Def. Br. 71. Here, disclosure of basic information about which tools the government used is essential to Mr. Muhtorov's ability to seek suppression.

Indeed, the government concedes that at least some of this information is relevant and helpful. It contends that court-approved substitutions under CIPA gave Mr. Muhtorov "substantially the same ability to make his suppression arguments as would disclosure of the specific classified information at issue." Gov't Br. 70. What surveillance or substitutions is the government referring to? It still doesn't say. The government has never identified its CIPA substitutions within the voluminous discovery produced in this case. Nor, until now, had it ever informed defense counsel that those CIPA substitutions addressed surveillance

---

government an extra national-security trump card under CIPA, and it should not do so here. The statute's procedures are already designed to accommodate the government's interest in secrecy while preserving defendants' due process rights. Def. Br. 81, 84.

techniques beyond FISA and Section 702. Instead, the government opposed defense counsel's effort to obtain notice at every turn. V5 at 198-206; V3 at 597. The defense should not have to play a guessing game to ascertain what kinds of secret surveillance were used. That is not how effective notice has ever operated. *See* 50 U.S.C. § 1806(c) (FISA); 18 U.S.C. § 2518(8)(d) (Title III). Whatever the substitutions were, they were insufficient to satisfy the government's disclosure obligations.

Accordingly, Mr. Muhtorov respectfully requests that the Court grant the relief described in his opening brief, including by requiring the government to identify the types of surveillance that agents used in their investigation of Mr. Muhtorov. Def. Br. 87-88.

IV. The over six-year delay violated Mr. Muhtorov's constitutional speedy trial right.

Pursuant to Fed. R. App. P. 28(i), Mr. Muhtorov also joins Mr. Jumaev's reply brief (at 2-20, 25-26) as to the defendants' overlapping constitutional speedy trial claims.

Indeed, the government concedes that both defendants meet *Barker*'s first prong, and recognizes that their claims largely overlap on the second prong. Gov't Br. 71-74.

Beyond that overlap, the government doesn't deny its nearly two-year delay in providing notice to Mr. Muhtorov of Section 702 surveillance. It just says that

timing didn't delay the case's disposition. Gov't Br. 74. But that strains credulity. With earlier disclosure the Section 702 litigation could have been conducted alongside Mr. Muhtorov's earlier suppression motion—and all of it wrapped up nearly two years' earlier. Def. Br. 90-91. Moreover, as Mr. Jumaev explains, the reason the cases weren't ready for trial even after the suppression litigation was completed was because of *the government's* discovery delays.

As to the third prong, Mr. Muhtorov asserted his right in repeated motions to dismiss. And as Mr. Jumaev explains, both defendants' discovery litigation evidenced their intent to receive the information necessary to timely go to trial.

As to the fourth factor, given the length of the delay, Mr. Muhtorov, like Mr. Jumaev, does not need to show individualized prejudice. But in any event, he does for the reasons stated in his opening brief. The government doesn't deny any of those reasons, it just minimizes them. But far from being cumulative, the lost witness's testimony was vital to explaining Mr. Muhtorov's past and how his hatred of the Karimov regime explained his interest in conversing with a group like the IJU. And ultimately, there is simply nothing ordinary or acceptable about confining a presumptively innocent person for six-and-a-half years—to the contrary, it is precisely the type of prejudice contemplated by the right to a speedy trial.

All four *Barker* factors weigh in Mr. Muhtorov's favor, and reversal is necessary.

Respectfully submitted,

VIRGINIA L. GRADY
Federal Public Defender

/s/ John C. Arceci
JOHN C. ARCECI
Assistant Federal Public Defender
633 17th Street, Suite 1000
Denver, Colorado 80202
(303) 294-7002
Email: John_Arceci@fd.org
COX_10ecf@fd.org

/s/ Patrick Toomey
PATRICK TOOMEY
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500
Email: ptoomey@aclu.org

/s/ Ashley M. Gorski
ASHLEY M. GORSKI
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500
Email: agorski@aclu.org

Counsel for Appellant Jamshid Muhtorov

Certificates of Compliance, Digital Submission, and Service

As required by Fed. R. App. P. 32(g)(1), I certify that the foregoing ***Appellant's Reply Brief*** is proportionally spaced and contains 10,487 words. I relied on my word processor, Microsoft Word 2016, to obtain the count. I certify that the information on this form is true and correct to the best of my knowledge and belief formed after a reasonable inquiry.

I hereby certify that with respect to the foregoing ***Appellant's Reply Brief***: (1) all required privacy redactions have been made; (2) the ECF submission is an exact copy of the filed hard copy; and (3) the ECF submission was scanned for viruses with Symantec Endpoint Protection version 14.2.5569.2100, Virus Definition File Dated: Tuesday, April 7, 2020 r3, and, according to the program is free of viruses.

I hereby certify that on April 7, 2020, I electronically filed the foregoing ***Appellant's Reply Brief*** using the CM/ECF system, which will send notification of this filing to counsel for the government, James C. Murphy, at james.murphy3@usdoj.gov, and Joseph Palmer, at joseph.palmer@usdoj.gov. I further certify that I also will send a copy of this filing by email to Caleb Kruckenberg, Counsel for Appellant Bakhtiyor Jumaev, at caleb.kruckenberg@ncla.legal.

/s/ John C. Arceci
JOHN C. ARCECI
Assistant Federal Public Defender