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.

Appeal from the United States District Court
for the District of Colorado (Judge John L. Kane)
No. 1:12-cr-00033-JLK-1

BRIEF OF AMICI CURIAE DAVID MEDINE AND SHARON BRADFORD FRANKLIN IN SUPPORT OF DEFENDANT–APPELLANT AND URGING REVERSAL

Andrew C. Lillie
Jessica Black Livingston
Nathaniel H. Nesbitt
Mark D. Gibson
HOGAN LOVELLS US LLP
1601 Wewatta Street, Suite 900
Denver, CO 80202
(303) 899-7339
Counsel for Amici Curiae David Medine and Sharon Bradford Franklin

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes, Regulations, and Rules

Other Authorities

IDENTITY, INTEREST, AND AUTHORITY OF AMICI

David Medine chaired the Privacy and Civil Liberties Oversight Board ("PCLOB") from May 2013 to July 2016. The PCLOB is an independent agency within the Executive Branch. 42 U.S.C. § 2000ee(a). Its mission is to ensure a balance between the federal government's efforts to prevent terrorism and the need to protect privacy and civil liberties. *Id.* § 2000ee(c)(1). It also strives "to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism." *Id.* § 2000ee(c)(2). The President, with the advice and consent of the Senate, selects the PCLOB's members "solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience." *Id.* § 2000ee(h)(1)–(2). Medine graduated from Hampshire College and the University of Chicago Law School.

Sharon Bradford Franklin is the policy director for New America's Open Technology Institute. She is also the codirector of New America's Cybersecurity Initiative. Her work encompasses many issues, including government surveillance and privacy. From 2013 to 2017, she served as the PCLOB's executive director. Among other things, in that role she reviewed government surveillance programs and other counterterrorism activities. Previously, she served as senior counsel at

the Constitution Project, where she worked on diverse issues involving national security and privacy and civil liberties, including surveillance policies and individual privacy. Franklin graduated from Harvard College and Yale Law School.

In July 2014, having spent months scrutinizing the section-702 program, the PCLOB issued its *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014) [hereinafter *PCLOB Report*], https://tinyurl.com/oouh63e. At that time, Medine chaired the PCLOB, and Franklin supported the PCLOB's members in developing the report. The PCLOB's inquiry included reviewing classified materials, and the PCLOB requested and obtained declassification of much information about section-702 surveillance.[1] The *PCLOB Report* provides the most comprehensive unclassified description of how the section-702 program works. Since the report's release, Medine and Franklin have written extensively about government surveillance under section 702. They have a vital interest in ensuring that the courts interpret and apply section 702 in a way that safeguards Americans' privacy, civil liberties, and Fourth Amendment rights.

[1] This brief was prepared relying solely on publicly available, unclassified information. Neither amici nor their counsel have referred to or reviewed any classified information to prepare this brief.

Under Federal Rule of Appellate Procedure 29(a)(2), amici have authority to file this brief because all parties have consented to its filing.[2]

SUMMARY OF THE ARGUMENT

Under section 702, the government incidentally seizes colossal quantities of Americans' private communications containing deeply personal information. These communications include phone calls, e-mails, love letters, text messages, and other communications revealing medical records, financial statements, academic transcripts, photographs, and other confidential information. The government not only retains these communications for years; it searches—or "queries"—them routinely. It does so both to investigate crime and to gather foreign intelligence. And it does so without a warrant or any other kind of prior individualized judicial approval.

The Fourth Amendment does not permit these warrantless "backdoor searches" of Americans' section-702 communications. Here, the government searched Muhtorov's section-702 communications without a warrant or other prior

[2] No party's counsel authored this brief in whole or in part. No party or party's counsel contributed money intended to fund preparing or submitting this brief. And no person contributed money intended to fund preparing or submitting the brief.

individualized judicial approval. Those searches therefore violated the Fourth Amendment. The Court should reverse.

BACKGROUND

In 2008, Congress passed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 ("FISA Amendments Act").[3] This law amended the Foreign Intelligence Surveillance Act of 1978 ("FISA").[4] Among other things, the FISA Amendments Act added a new section to FISA: section 702. *PCLOB Report* at 5.

Under section 702, "the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year …, the targeting of persons reasonably believed to be located outside of the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Government agencies conduct section-702 surveillance from within the United States. *PCLOB Report* at 5. This targeting is permissible when three elements are present: (1) the target is a

[3] Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. §§ 1812, 1881, 1881a–1881g, 1885, 1885a–1885c).

[4] Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 18 and 50 U.S.C.)

non-U.S. person;[5] (2) the government reasonably believes that the target is located outside the United States; and (3) the surveillance is for acquiring "foreign intelligence" information, which FISA defines broadly to mean virtually any information bearing on the United States' foreign affairs. *See* 50 U.S.C. § 1801(e); *PCLOB Report* at 6. The government cannot intentionally target an American (whether within the United States or abroad). *PCLOB Report* at 6. Nor can it intentionally target anyone (American or otherwise) located within the United States. *Id.* at 6. And the surveillance must be to gather foreign intelligence. *Id.*

Before the government can conduct section-702 surveillance, it must annually get a general authorization from the Foreign Intelligence Surveillance Court ("FISC"). *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 404 (2013). To be clear, the FISC does not approve individual targeting decisions under section 702. David Medine, *Prepared Statement for the Senate Committee on the Judiciary on Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties* at 2 (2016) [hereinafter *Medine Statement*], https://tinyurl.com/y33tvzvz. Instead, the FISC provides an annual general authorization. The FISC must approve the government's targeting procedures, minimization procedures, and certifications describing the foreign-

[5] U.S. persons include U.S. citizens, legal permanent residents, and corporations incorporated in the United States. 50 U.S.C. § 1801(i).

intelligence topics for which it intends to collect information. *Clapper*, 568 U.S. at 405; *Medine Statement* at 2.

As for targeting procedures, the FISC assesses whether those procedures are reasonably designed "(1) to ensure that an acquisition … is limited to targeting persons reasonably believed to be located outside the United States and (2) to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known … to be located in the United States." *Clapper*, 568 U.S. at 405–06 (omissions in original). Section 702 also requires the FISC to assess whether the targeting procedures accord with the statute. *Id.* at 406. The following overview of the National Security Agency's targeting procedures provides a good example of what these targeting procedures look like:

> [A]n NSA analyst can identify non-U.S. persons outside of the United States as potential surveillance targets. In addition to identifying a valid foreign intelligence purpose derived from the list certified by the FISA Court, an analyst must follow a detailed set of targeting procedures. These procedures require a careful examination of the target and the email address, phone number, or other selector associated with the target, to verify that they are sufficiently foreign. Once an analyst has documented a valid foreign intelligence purpose and the steps taken to ensure the target is foreign, she must obtain approval of two senior NSA analysts. If approval is obtained, an electronic communications service provider can be compelled to gather communications about the target through tasking.

Medine Statement at 2.

The statute also mandates "minimization procedures," which are essentially rules for collecting and sharing communications collected under section 702. 50 U.S.C. § 1881a(e). "Every agency that accesses Section 702 information must have its own set of minimization procedures that are approved by the FISA Court." *Medine Statement* at 3. These procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). The FISC reviews these minimization procedures, *id.* § 1881a(j)(1)(A), but it has recognized that its review is "narrowly circumscribed," *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. 08-01, 2008 WL 9487946, at *2 (FISA Ct. Aug. 27, 2008). Its review consists of analyzing "whether the [agency's specific] minimization procedures meet the definition of minimization procedures under section 1801(h) …, as appropriate," and whether the procedures are consistent with FISA and the Fourth Amendment. *Clapper*, 568 U.S. at 406 (omission in original).

As for the government's certifications, the FISC assesses whether they contain the required attestations. *Id.* at 405. Among other things, the government's certifications must attest to the following:

> (1) procedures are in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC] that are reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States; (2) minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons, as appropriate; (3) guidelines have been adopted to ensure compliance with targeting limits and the Fourth Amendment; and (4) the procedures and guidelines referred to above comport with the Fourth Amendment.

Id. (alteration in original).

Significantly, these FISC-approved procedures permit the government to conduct "U.S.-person queries" of section-702 communications. *PCLOB Report* at 55–59; *Medine Statement* at 8. A U.S.-person query, also known as a backdoor search, involves searching section-702 databases using terms for a specific U.S. person. *PCLOB Report* at 55–56. Although the details differ in some ways, the NSA's, CIA's, and FBI's minimization procedures all permit these queries. *Id.* at 55–56 (discussing the NSA's procedures); *id.* at 57–58 (discussing the CIA's procedures); *id.* at 58–59 (discussing the FBI's procedures).

Here, the public record shows that the government searched the section-702 communications of Jamshid Muhtorov, a U.S. person under FISA, during its investigation. *United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1244, 1256, 1258 (D. Colo. 2015); *see PCLOB Report* at 59 ("[W]henever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired information from a variety of sources, including Section 702, for information relevant to the investigation or assessment.").

ARGUMENT

I. The warrantless collection of Americans' communications under section 702 is broad and raises significant privacy concerns.

A. The government incidentally collects a huge volume of Americans' communications when it conducts surveillance under section 702.

Since section 702 became law, the government has intercepted billions of international communications from hundreds of thousands of individuals. In 2011, for example, section 702 allowed the government to collect more than 250 million communications. [*Redacted*], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011). The number of targets has nearly doubled since 2013, so the government likely collects hundreds of millions of communications under section 702 every year. *See* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities* at 13 (2019), [hereinafter *ODNI Report*],

https://tinyurl.com/y6mohb7e; *PCLOB Report* at 116. These communications take multiple forms, including telephone calls, e-mails, video calls, texts, and online chats.

Many of these communications are sent or received by Americans. Even though the government cannot target an American under section 702, the government "incidentally" collects Americans' communications when, for example, "a U.S. person communicates with a non-U.S. person who has been targeted." *PCLOB Report* at 6. Any time an American communicates with one of the government's targets, the government may collect and store that communication. The government can target any non-U.S. person abroad who is likely to communicate "foreign intelligence information"—which can include virtually any information related to the "foreign affairs of the United States." 50 U.S.C. § 1801(e)(2). Targets are not limited to suspected bad actors—such as terrorists. *PCLOB Report* at 145. So it's highly likely that ordinary Americans routinely communicate with targets of section-702 surveillance.

The precise number of Americans swept up in section-702 surveillance is unknown. Even though members of Congress have repeatedly asked the government to provide this figure, the government has refused to provide even an estimate. But we know that section-702 surveillance allows the government to get

"substantial quantities of information concerning United States persons and persons located inside the United States who are entitled to Fourth Amendment protection." [*Redacted*], No. [Redacted], slip op. at 24 (FISA Ct. Aug. 30, 2013), https://perma.cc/GR62-FNQC. That's because "[t]he Section 702 program has collected hundreds of millions of Internet communications," so "[e]ven if only a small percentage of those communications are to or from an American, the total number of Americans' communications is likely significant." *PCLOB Report* at 151.

B. Section-702 surveillance creates significant concerns for Americans' privacy.

Because section-702 surveillance captures many Americans' communications, that surveillance raises at least three significant privacy concerns.

First, the communications can contain sensitive, personal, and confidential information. For instance, "they can include family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges." *Medine Statement* at 7.

Second, the government retains these communications for years. "U.S. persons' communications are not typically purged or eliminated from the government's Section 702 databases before the end of their default retention periods, even when the communications pertain to matters unrelated to foreign

intelligence or crime." *PCLOB Report* at 128. Under the NSA's minimization procedures, for instance, the government can, at a minimum, retain "communications of or concerning a United States person" for "five years from the expiration date of the certification authorizing the collection." Nat'l Security Agency, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 3(b)(1) (2016), https://tinyurl.com/y56hbzhf. None of the agencies' procedures requires analysts to review Americans' communications at the collection stage to determine whether to keep, share, or purge them, and the CIA's and FBI's procedures do not even require that agents purge communications when the communications involve Americans and contain no foreign-intelligence information. *PCLOB Report* at 128–29. As a result, purging Americans' communications from section-702 databases "rarely happens." *Medine Statement* at 5.

Third, as explained below, the government routinely searches this vast universe of communications, containing potentially deeply personal matters, without a warrant or any other prior individualized judicial review, for information about Americans. *See* Geoffrey Stone & Michael Morell, *The One Change We Need to Surveillance Law*, Wash. Post (Oct. 9, 2017), https://tinyurl.com/yxgt9voo

(contending that the law should not permit the government to search section-702 communications "for information on Americans without first obtaining a warrant," because Americans should not lose full protection of their privacy "merely because the government has information in a foreign intelligence database that it legally acquired").

II. The government routinely searches Americans' section-702 communications.

Once the government acquires communications under section 702, they are housed in federal national-security or law-enforcement databases at the NSA, CIA, and FBI. The government often then searches these databases during later investigations, including domestic criminal investigations unrelated to foreign intelligence. *PCLOB Report* at 59. Although the procedures governing database queries differ from agency to agency, all agencies allow trained agents or analysts to search or "query" these communications using specific terms or identifiers—including terms and identifiers specific to U.S. persons. *Id.* at 55. The government calls this practice conducting "U.S. person queries," but privacy advocates call them "backdoor searches," because that term "provides a clearer picture of how the government is attempting to evade the individualized judicial review that the Fourth Amendment generally requires." Sharon Bradford Franklin, *What Happened at the Court: The Hasbajrami Oral Argument on Section 702 of FISA and the*

Fourth Amendment, Just Security (Aug. 29, 2018), https://tinyurl.com/y5kmtl6u. The NSA and CIA have reported that they conduct these searches tens of thousands of times a year. *ODNI Report* at 13–16. And the FBI, which conducts these searches as a routine matter, including "with some frequency" for criminal investigations, is not generally required to count how often it performs them. *PCLOB Report* at 59; *see* 50 U.S.C. § 1873(d)(2)(A).

Intelligence agencies such as the NSA and CIA often search Americans' section-702 communications to gather foreign-intelligence information. *See Medine Statement* at 8.

The FBI often searches Americans' section-702 communications not only to gather foreign intelligence but also to investigate crime. *Id.* Those purposes are frequently intertwined. In response to a recommendation in the *PCLOB Report*, the FBI itself made this clear when it amended its minimization procedures in 2015: "[I]t is a routine and encouraged practice for the FBI to query databases containing lawfully acquired information, including FISA-acquired information, in furtherance of the FBI's authorized intelligence and law enforcement activities, such as assessments, investigations and intelligence collection." Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such

Certifications and Amended Certifications at 7, https://tinyurl.com/yxj56do2. The FBI added this language to its minimization procedures to reflect existing practice, not to mark a change in practice: "The government added this language to more clearly reflect the FBI's existing practice for conducting United States person queries, rather than for the purpose of altering the standards governing such queries." *Id.* at 8. This means "the FBI can search through years of a U.S. person's communications for information that may lead to criminal charges without a warrant or any kind of external oversight." *Medine Statement* at 9.

Searching Americans' section-702 communications without a warrant or any other kind of prior individualized judicial approval does not accord with the Fourth Amendment.

III. The Fourth Amendment bars the government from searching Americans' section-702 communications without a warrant or any other kind of prior individualized judicial approval.

The Fourth Amendment applies to these backdoor searches because it protects U.S. persons' communications. *See Katz v. United States*, 389 U.S. 347, 353 (1967) (holding that recording and reviewing a person's communications "constituted a 'search and seizure' within the meaning of the Fourth Amendment"). The Fourth Amendment not only applies to backdoor searches; it bars them. The warrantless backdoor searches of Muhtorov's section-702

communications had a law-enforcement component, and it is bedrock Fourth Amendment law that, with only a few limited exceptions not present here (e.g., exigent circumstances), such warrantless searches are "*per se* unreasonable" and violate the Fourth Amendment. *Id.* at 357. But even if the Court were to conclude that the warrant requirement does not apply, it is unreasonable for the government to search Americans' section-702 communications without *any kind* of prior individualized judicial approval. *See United States v. U.S. Dist. Ct.* (*Keith*), 407 U.S. 297, 320–21 (1972) (holding that the government must get prior judicial approval before conducting domestic surveillance to safeguard national security). Here, FBI agents obtained and searched Muhtorov's protected communications without individualized judicial review of any kind. That surveillance violated the Fourth Amendment.

A. The government's searches of Muhtorov's section-702 communications were "searches" subject to the Fourth Amendment.

Contrary to the district court's conclusion, the Fourth Amendment applies at the query stage because the government's searches of Muhtorov's section-702 communications amounted to "searches" within the meaning of the Fourth Amendment.

The district court held that when the government searches Americans' section-702 communications, those searches do not count as "searches" under the Fourth Amendment. *Muhtorov*, 187 F. Supp. 3d at 1256. The court reasoned that "[a]ccessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information." *Id.* That reasoning is flawed because it fails to recognize the distinction between the government *seizing* Americans' communications under section 702 and the government then *searching* those communications.

Searches and seizures are different. *See Soldal v. Cook County*, 506 U.S. 56, 63 (1992). When the government incidentally collects an American's communications under section 702, that's a seizure. But when the government later searches Americans' communications gathered under section 702, that's a search for which an independent Fourth Amendment justification is required. *See, e.g.*, *Riley v. California*, 573 U.S. 373, 403 (2014) (requiring the government to get a warrant before searching a cellphone lawfully seized incident to an arrest); *United States v. Burgess*, 576 F.3d 1078, 1090 (10th Cir. 2009) (noting that the Fourth Amendment might not allow the government to search lawfully seized "laptop computers, hard

drives, flash drives or even cell phones" because of "their unique ability to hold vast amounts of diverse personal information").

The Supreme Court's *Riley* decision drives that point home. In that case, the government lawfully *seized* the defendants' cellphones during searches incident to arrest. *Riley*, 573 U.S. at 378–81. Even so, the Court held that the government needed a warrant before *searching* the cellphones. *Id.* at 403. It reached that holding, in large part, because allowing the government to search the cellphones would create a severe invasion of privacy. *Id.* at 391–98. After all, for many Americans, cellphones now hold (in both quantity and quality) the "privacies of life," *id.* at 403, for instance "an address, a note, a prescription, a bank statement, a video," *id.* at 394. The same is true here. Americans' section-702 communications also contain the privacies of life, for instance "family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges." *Medine Statement* at 7. As a result, the district court's conclusion that the government need not get a warrant before searching Americans' communications gathered under section 702 simply does not square with Supreme Court precedent.

Indeed, *Riley* holds that the government must get a warrant before searching a cellphone lawfully seized incident to arrest—even though arrestees have

"diminished expectations of privacy." 573 U.S. at 392. So the government surely must get a warrant before searching Americans' section-702 communications—given that ordinary Americans enjoy a greater expectation of privacy than arrestees.

B. The Fourth Amendment demands a warrant—or, at a minimum, *some* kind of individualized prior judicial approval—before the government searches an American's section-702 communications.

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness." *Id.* at 381. But the Supreme Court has recognized that " 'reasonableness' derives content and meaning through reference to the warrant clause," *Keith*, 407 U.S. at 309–10, and that "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, … reasonableness generally requires the obtaining of a judicial warrant," *Riley*, 573 U.S. at 382 (alteration in original). In fact, subject to a few limited exceptions (e.g., exigent circumstances), warrantless searches are "*per se* unreasonable." *Katz*, 389 U.S. at 357. The searches of Muhtorov's communications had, at a minimum, a law-enforcement component. After all, the FBI conducted those searches as part of its investigation and eventual prosecution of Muhtorov, just as it routinely does when investigating Americans for potential criminal prosecution. But the government had no warrant for those searches. They therefore violated the Fourth Amendment.

Even if the Court were to conclude that the Fourth Amendment does not demand a traditional probable-cause warrant in the foreign-intelligence context, it still demands at least some kind of prior individualized judicial approval. That much follows from the Supreme Court's *Keith* decision. There, the Supreme Court recognized that even in the context of collecting intelligence to protect national security, the default rule under the Fourth Amendment is prior individualized judicial approval. *Keith*, 407 U.S. at 318–21. The Supreme Court has never recognized a foreign-intelligence exception even to the warrant requirement—much less a foreign-intelligence exception to the default rule of prior individualized judicial approval. *PCLOB Report* at 89–90.

One of the exceptions it has recognized is the so-called "special needs" cases. But warrantless backdoor searches of Americans' section-702 communications do not fit within that exception.

In the special-needs cases, the Supreme Court has held that the government need not get a warrant (1) when the search's purpose is not for ordinary law enforcement and (2) when getting prior individualized judicial approval would be impracticable. *See, e.g.*, *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995).

As to the first element, the FBI routinely conducts these searches as part of ordinary law enforcement. *PCLOB Report* at 59. And gathering foreign intelligence

and investigating crime are often intertwined. *See In re Sealed Case*, 310 F.3d 717, 736 (FISA Ct. Rev. 2002) (per curiam) (noting that "ordinary crimes might be inextricably intertwined with foreign intelligence crimes").

Regardless, as to the second element, it would not be impracticable in most cases for the government to get prior individualized judicial approval before searching Americans' section-702 communications. In *Keith*, the Court held that it would not be impracticable for the government to get prior individualized judicial approval to gather *domestic* intelligence to safeguard national security. 407 U.S. at 320–21. There is no reason to believe that it would be impracticable for the government to get prior individualized judicial approval to gather *foreign* intelligence to safeguard national security. In fact, the government already does seek prior judicial approval in a closely analogous context: whenever the government wants to surveil or search an American for foreign-intelligence purposes, it must get prior individualized judicial approval from the FISC. 50 U.S.C. §§ 1805, 1824. Backdoor searches of Americans' section-702 communications allow the government, in effect, to target an American just as it would under Titles I and III of FISA—they just wrongfully allow the government to skip FISC review before doing so.

Caselaw confirms that the Fourth Amendment requires the government to get prior individualized judicial approval before searching Americans' section-702 communications. Prior individualized judicial approval is a core Fourth Amendment safeguard that the courts have relied on to uphold the constitutionality of electronic surveillance in other contexts. *In re Sealed Case*, 310 at 739–40 (FISA); *United States v. Duggan*, 743 F.2d 59, 73–74 (2d Cir. 1984) (FISA); *United States v. Tortorello*, 480 F.2d 764, 772–73 (2d Cir. 1973) (Title III).

Prior individualized judicial review is especially critical here for two reasons.

First, the privacy interests at stake could hardly be more acute. Under section 702, the government collects vast quantities of Americans' communications containing "the privacies of life." *Riley*, 573 U.S. at 403; *Medine Statement* at 7. And government agencies do not contemporaneously review communications at the collection stage to determine whether to keep, share, or purge them. Instead, those communications typically remain within government databases for five years by default. *PCLOB Report* at 128. Backdoor searches allow the government to rummage through those communications.

Second, the procedures at the collection stage under the section-702 program are extremely permissive. The FISC, for example, does not approve any of the tens of thousands of individual targeting decisions. Nor does it determine whether

there is probable cause to believe that the surveillance will yield foreign intelligence. Simply put, there is no individualized judicial review at the front end. To compensate for the lack of individualized judicial review at the collection stage, the totality-of-the-circumstances test demands individualized judicial review at the "back end," when the government conducts U.S.-person queries to search Americans' section-702 communications. But the government currently conducts these backdoor searches without "the deliberate, impartial judgment of a judicial officer." *Katz*, 389 U.S. at 357. This means there is never any individualized judicial review of the decision to seek information about a particular U.S. person. Rather, the government's decision to search through section-702 communications for information about particular Americans is simply left to Executive Branch analysts. The Fourth Amendment's baseline reasonableness test demands more. In the electronic-surveillance context, reasonableness requires that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger v. New York*, 388 U.S. 41, 58 (1967). Because the government collects significant amounts of Americans' communications under section 702, searching those communications can be lawful under the reasonableness test only if the minimization procedures *at least* require individualized judicial review after collection, but before conducting U.S.-person

queries and reviewing Americans' communications. Minimization procedures are not procedural niceties tacked on after the fact to address the handling of lawfully collected communications; they are part and parcel of the package needed to meet constitutional requirements. *See Amnesty Int'l USA v. Clapper*, 667 F.3d 163, 176 (2d Cir. 2011) (Raggi, J.) (dissenting from the denial of rehearing en banc).

C. Stronger safeguards would bring the government's searches of Americans' section-702 communications into compliance with the Fourth Amendment.

The Court need go no further in this case than to declare that the Fourth Amendment bars the government from searching Americans' section-702 communications without prior individualized judicial approval. The Court need not resolve how exactly to effectuate that principle. If the Court were to determine that the warrant requirement does not apply, it can and should leave the remedial work to the Executive Branch and Congress, just as the Supreme Court did when it held that the government's surveillance in the renowned *Keith* and *Berger* cases violated the Fourth Amendment. *See Keith*, 407 U.S. at 324 (stating that "prior judicial approval is required for the type of domestic security surveillance involved in this case and ... such approval may be made in accordance with such reasonable standards as the Congress may prescribe"); *Berger*, 388 U.S. at 58 (describing the statute at issue as "offensive" to the Fourth Amendment, and holding that

government intrusions into private communications must be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions" of privacy).

That said, the government could readily implement new safeguards. It could, for example, amend its minimization procedures to provide stronger protections. Of utmost importance is that "an impartial, life-tenured federal judge [have] the final say over access to Americans' personal communications collected incidentally under Section 702." *Medine Statement* at 8. When the government wants to search an American's section-702 communications, it should do at least two things: it should seek authorization from a court, and it should submit its proposed U.S.-person search terms and other search parameters (e.g., date-range limitation) to the court and receive the court's approval. *Id.*

CONCLUSION

The Fourth Amendment forbids the government from searching Americans' section-702 communications without any form of prior individualized judicial approval. Because the government searched Muhtorov's section-702 communications without prior individualized judicial approval—of any kind—those searches violated the Fourth Amendment. The district court thus erred in

denying Muhtorov's suppression motion. The Court should reverse that order and remand for further proceedings.

Respectfully submitted,

s/ Andrew C. Lillie
Andrew C. Lillie
Jessica Black Livingston
Nathaniel H. Nesbitt
Mark D. Gibson
HOGAN LOVELLS US LLP
1601 Wewatta Street, Suite 900
Denver, CO 80202
(303) 899-7339
andrew.lillie@hoganlovells.com
jessica.livingston@hoganlovells.com
nathaniel.nesbitt@hoganlovells.com
mark.gibson@hoganlovells.com

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation under Rule 29(a)(5) because it contains 5081 words. I certify that this brief complies with the typeface requirements of Rule 32(a)(5) and the type-style requirements of Rule 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Equity Text.

CERTIFICATE OF PRIVACY REDACTIONS

Under Tenth Circuit Rule 25.5, I certify that I have made all required privacy redactions.

CERTIFICATE OF EXACT COPIES

I certify that the hard copies of this brief that I will submit to the Court are exact copies of the electronic version filed using the ECF system.

CERTIFICATE OF VIRUS SCAN

I certify that I scanned this brief for viruses with the most recent version of Symantec Endpoint Protection and, according to the program, this brief is free of viruses.

s/ Andrew C. Lillie
Andrew C. Lillie

CERTIFICATE OF SERVICE

I certify that on October 7, 2019, I filed this brief with the Clerk of Court for the United States Court of Appeals for the Tenth Circuit using the ECF system, which will serve the brief on all counsel of record.

s/ Andrew C. Lillie
Andrew C. Lillie