24-1648 (L), 25-542 (CON)

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

AGRON HASBAJRAMI,

Defendant–Appellant.

On Appeal from the United States District Court
for the Eastern District of New York
Case No. 1:11-cr-623

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT AND REVERSAL IN PART

Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
andrew@eff.org

Patrick Toomey
Ashley Gorski
Sara Robinson
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
ptoomey@aclu.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Amici Curiae American Civil Liberties Union and Electronic Frontier Foundation state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: July 22, 2025

/s/ Patrick Toomey
Patrick Toomey

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES iii

INTEREST OF AMICI CURIAE 1

INTRODUCTION 2

BACKGROUND 4

ARGUMENT 9

I. Querying U.S. person communications under Section 702 is a "separate Fourth Amendment event." 9

II. The government's queries of Mr. Hasbajrami's communications violated the warrant requirement. 12

A. As Fourth Amendment searches, the queries of Mr. Hasbajrami's communications presumptively required a warrant. 12

B. Any "foreign intelligence" exception to the warrant requirement does not apply in this case. 14

III. Even if a warrant exception applied, the queries of Mr. Hasbajrami's communications were unreasonable under the Fourth Amendment. 22

A. Queries of U.S. person communications lack the core safeguards courts apply when assessing the reasonableness of electronic surveillance. 23

B. The district court correctly balanced the degree of intrusion and the government's interest in concluding that the queries were not reasonable. 26

CONCLUSION 31

CERTIFICATE OF COMPLIANCE 33

TABLE OF AUTHORITIES

Cases

[*Redacted*],
2011 WL 10945618 (FISC Oct. 3, 2011) 5, 26

[*Redacted*],
402 F. Supp. 3d 45 (FISC 2018) 7, 27, 28, 31

Arizona v. California,
460 U.S. 605 (1983) 12

Arizona v. Gant,
556 U.S. 332 (2009) 13

Berger v. New York,
388 U.S. 41 (1967) 23, 25

Camara v. Mun. Ct. of City & Cnty. of San Francisco,
387 U.S. 523 (1967) 28

City of Los Angeles v. Patel,
576 U.S. 409 (2015) 13, 14

Clapper v. Amnesty Int'l USA,
568 U.S. 398 (2013) 1

In re Certified Question of Law,
858 F.3d 591 (FISCR 2016) 16, 20

In re Directives,
551 F.3d 1004 (FISCR 2008) 15, 16, 20, 26

In re NSA Telecomm. Recs. Litig.,
671 F.3d 881 (9th Cir. 2011) 1

In re Sealed Case,
310 F.3d 717 (FISCR 2002) 23, 24, 25

In re Terrorist Bombings,
552 F.3d 157 (2d Cir. 2008) 15, 17, 26

Jewel v. NSA,
673 F.3d 902 (9th Cir. 2011) 1

Johnson v. United States,
333 U.S. 1 0 (1948).....30

Jones v. United States,
357 U.S. 493 (1958)..... 3, 12, 15

Katz v. United States,
389 U.S. 347 (1967)..... 12, 24

Kentucky v. King,
563 U.S. 452 (2011).....22

Maryland v. King,
569 U.S. 435 (2013)..... 13, 14

Pretzantzin v. Holder,
736 F.3d 641 (2d Cir. 2013) 14

Riley v. California,
573 U.S. 373 (2014)..... 9, 13, 14

Rodriguez v. United States,
575 U.S. 348 (2015).....10

Terry v. Ohio,
392 U.S. 1 (1968).....10

United States v. Abu-Jihaad,
630 F.3d 102 (2d Cir. 2010) 19

United States v. Ackerman,
831 F.3d 1292 (10th Cir. 2016) 26

United States v. Biasucci,
786 F.2d 504 (2d Cir. 1986) 23

United States v. Bobo,
477 F.2d 974 (4th Cir. 1973) 23

United States v. Brown,
484 F.2d 418 (5th Cir. 1973) 18

United States v. Butenko,
494 F.2d 593 (3d Cir. 1974) 18

United States v. Donovan,
429 U.S. 413 (1977).....25

United States v. Duggan,
743 F.2d 59 (2d Cir. 1984) 24

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

United States v. Hasbajrami,
No. 11-cr-623, 2025 WL 447498 (E.D.N.Y. Feb. 10, 2025) ..... passim

United States v. Kirk Tang Yuk,
885 F.3d 57 (2d Cir. 2018) 13

United States v. Maher,
120 F.4th 297 (2d Cir. 2024) 26

United States v. Mesa-Rincon,
911 F.2d 1433 (10th Cir. 1990) 23

United States v. Mohamud,
843 F.3d 420 (9th Cir. 2016) 15

United States v. Muhtorov,
20 F.4th 558 (10th Cir. 2021) 1

United States v. Place,
462 U.S. 696 (1983).....10

United States v. Truong,
629 F.2d 908 (4th Cir. 1980) 18, 20

United States v. U.S. Dist. Court (Keith),
407 U.S. 297 (1972) 15, 21

United States v. Weaver,
9 F.4th 129 (2d Cir. 2021) 13

Vernonia Sch. Dist. 47J v. Acton,
515 U.S. 646 (1995) 20

Zweibon v. Mitchell,
516 F.2d 594 (D.C. Cir. 1975) 18

Statutes

50 U.S.C. § 1801 *et seq* 4

50 U.S.C. § 1805 ..... 4, 19, 22

50 U.S.C. § 1806 2

50 U.S.C. § 1881a 4, 5

FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-
118, 132 Stat. 3 (2018) 31

Other Authorities

Appellant's Reply Br., *United States v. Muhtorov*, No. 18-1366 (10th
Cir. Apr. 7, 2020), Doc. No. 010110330621 2

FBI Section 702 Querying Procedures (Mar. 1, 2024) 31

FISA Court Orders 1979-2023, Elec. Priv. Info. Ctr. 19

Gov't Br., *United States v. Hasbajrami*, No. 11-cr-623 (E.D.N.Y. May
5, 2022), ECF No. 196 ..... 11, 14, 29

Mem. Op. & Order, [Redacted], (FISC Apr. 21, 2022) 29

Noah Chauvin, *Why Congress Must Reform FISA Section 702*,
Brennan Ctr. for Just. (Apr. 9, 2024) 8

NSA Slides Explain the PRISM Data-Collection Program, Wash. Post (Jun. 6, 2013) 5

Off. Dir. Nat'l Intel., *Annual Statistical Transparency Report* (2022) 7

President's Review Group, *Liberty and Security in a Changing World* (2013).....25

Priv. & Civ. Lib. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702* (2014)..... 6, 16

Priv. & Civ. Lib. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2023)..... passim

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit organization dedicated to the principles of liberty and equality embodied in the Constitution. The ACLU has appeared before the courts in many cases involving the Fourth Amendment and foreign-intelligence surveillance, including this one. *See, e.g.*, *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (amicus); *United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021).

The Electronic Frontier Foundation ("EFF") is a civil liberties organization working to protect innovation, free speech, and privacy in the online world. EFF represents the interests of technology users in court cases involving the application of law in the digital age. *See, e.g.*, *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011); *In re NSA Telecomm. Recs. Litig.*, 671 F.3d 881 (9th Cir. 2011).

[1] All parties consent to the filing of this brief. No party or party's counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

INTRODUCTION

This case concerns the government's widespread practice of warrantlessly searching U.S. persons' communications collected under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). Few courts have addressed this significant aspect of Section 702 surveillance. Thus, while Mr. Hasbajrami has challenged only the district court's application of the good-faith exception on appeal, amici write to underscore why the court was correct to conclude that the warrantless querying of Mr. Hasbajrami's communications violated the Fourth Amendment.[2]

As this Court previously held, when FBI agents move beyond targeting foreigners under Section 702 to deliberately searching through the massive pool of collected data for the private communications of Americans, that is a "separate Fourth Amendment event" that must be independently justified under the Constitution. *United States v. Hasbajrami*, 945 F.3d at 646, 670 (2d Cir. 2019) ("*Hasbajrami I*"). The district court, on remand, faithfully applied this holding to the record before it. *United States v. Hasbajrami*, No. 11-cr-623, 2025 WL 447498

[2] Although amici address the merits of the district court's decision, amici agree with Mr. Hasbajrami that the good-faith exception does not apply here. When a court concludes that Section 702 queries were unlawful, suppression is mandatory under FISA's statutory suppression provision. *See* 50 U.S.C. § 1806(g); Appellant's Reply Br. at 26-27, *United States v. Muhtorov*, No. 18-1366 (10th Cir. Apr. 7, 2020), Doc. No. 010110330621 (addressing this argument).

(E.D.N.Y. Feb. 10, 2025) ("*Hasbajrami II*"). The court examined the FBI's multiple warrantless queries of Mr. Hasbajrami to determine whether they complied with the Fourth Amendment, concluding that no exception to the warrant requirement applied in this case. The court held that while exigency or another "carefully drawn" exception might apply to other queries in other cases, *Jones v. United States*, 357 U.S. 493, 499 (1958), the facts presented here did not support such an exception. In particular, the district court properly rejected the government's sweeping claim that merely because agents claimed to be seeking "foreign intelligence"—a vague, expansive category—that excused them from complying with the warrant requirement. Such a claim has never been sufficient to eliminate the bedrock protection of a warrant, and the consequences of accepting that argument would be dire for the privacy rights of Americans.

While the district court ultimately denied Mr. Hasbajrami's motion to suppress on good-faith grounds, it first addressed the Fourth Amendment merits, as this Court instructed. *See Hasbajrami I*, 945 F.3d at 646, 673, 676. In the event this Court considers those questions on appeal, amici discuss how Section 702 queries are routinely used to gain access to Americans' private communications, why the warrant requirement applies to these searches, and why the querying of Mr. Hasbajrami's communications violated the Fourth Amendment.

BACKGROUND

Section 702, codified at 50 U.S.C. § 1881a, authorizes the government to search U.S. person communications on U.S. soil without a warrant.

This provision, enacted in 2008 as an amendment to FISA, 50 U.S.C. § 1801 *et seq*., revolutionized and dramatically expanded the government's surveillance authorities. In its original form, FISA generally required the government to obtain individualized judicial approval of each person it sought to target. *See* 50 U.S.C. § 1805. The statute created a secret Article III court, the Foreign Intelligence Surveillance Court ("FISC"), and authorized surveillance only after a FISC judge found "probable cause" that each target was a "foreign power" or "agent of a foreign power." *Id.* § 1805(a)(2)(A)-(B). Thus, the government generally could not intercept or search phone calls or emails inside the United States, even for foreign-intelligence purposes, unless it first made a probable-cause showing before a neutral magistrate about the particular targets of its surveillance.

Section 702 significantly altered this regime by abandoning these requirements for targets who are non-U.S. persons abroad. Like surveillance under traditional FISA, Section 702 surveillance takes place on U.S. soil. But under Section 702, surveillance occurs without any finding of probable cause or judicial review of individual targets. 50 U.S.C. § 1881a. The government need not demonstrate to any court that the people it seeks to surveil are agents of foreign

powers, engaged in criminal activity, or connected even remotely with terrorism. Instead, Section 702 generally permits the government to target *any* foreigner located outside the United States to obtain foreign-intelligence information and to retain their communications with anyone, including U.S. persons. *Id.* § 1881a(a). The FISC's role consists principally of an annual review of broad, programmatic guidelines that the government uses to conduct surveillance.

The government carries out this surveillance with the cooperation of major American telecommunication companies and internet service providers, such as Google, Facebook, Microsoft, and Verizon. With the compelled assistance of these companies, Section 702 reaches virtually every form of modern electronic communication: emails, text messages, web browsing, telephone calls, video calls, and online chats.[3]

Because the rules are so permissive and because the surveillance spans so many forms of communication, Section 702 collection is incredibly broad in practice. In 2011, when the events at issue in this appeal occurred, the government relied on Section 702 to collect about 250 million internet communications each year.[4] [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011). The intercepted

[3] *See NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post (Jun. 6, 2013), http://wapo.st/J2gkLY.

[4] Some aspects of Section 702 surveillance have changed since 2011. For example, the breadth of the collection has expanded, government agencies have

communications inevitably—and intentionally—include the communications of U.S. persons who correspond with the government's targets. Given the volume of intercepted communications, government analysts are unable to individually and contemporaneously review every communication collected. *See* Priv. & Civ. Lib. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702* at 55-60, 128-29 (2014), https://perma.cc/WD5R-5GKE ("2014 PCLOB Report") ("NSA analysts do not review all or even most communications."); *Hasbajrami I*, 945 F.3d at 671 (similar).[5] Instead, the collected communications are simply added to the government's massive databases, to await later searching and use.

Although the government's initial collection is targeted at foreigners abroad, many of its subsequent searches of that data are directed at Americans—a warrantless backdoor it has widely exploited. 2014 PCLOB Report at 129-31; 2023 PCLOB Report at 184-90. The government justifies its warrantless collection

---

modified their minimization procedures in certain respects, and agencies have developed procedures governing querying. *See* Priv. & Civ. Lib. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2023), https://perma.cc/GJL6-DVRM ("2023 PCLOB Report").

[5] The district court may have misunderstood this important fact. *See Hasbajrami II*, 2025 WL 447498 at *9 (describing review as "compulsory"). The PCLOB has emphasized that many communications are never reviewed unless queried. *See, e.g.*, 2014 PCLOB Report at 128-29 (communications often remain "unreviewed until they are retrieved in response to a database query"). The volume of communications collected under Section 702 is too immense to review each one.

under Section 702 on the theory that its foreign targets lack Fourth Amendment rights. But the government then claims a windfall: the ability to deliberately query its Section 702 databases for the communications of *known Americans*. *Id.* The government's routine querying of Americans' private communications, without any individualized judicial approval, goes far beyond its claimed interest in surveilling foreigners. Agents instead use Section 702 queries to investigate people in the United States, bypassing the warrant requirement that would ordinarily constrain those domestic investigations.

What is more, the agency rules governing these searches are extraordinarily lax—a problem that was even more acute in 2011, when the FBI queried Mr. Hasbajrami's communications. For years, the FBI's policy was to encourage "maximal" querying of Section 702 data, [*Redacted*], 402 F. Supp. 3d 45, 78, 80, 87-88 (FISC 2018), resulting in *millions* of warrantless searches for Americans' communications annually, *id.* at 75.[6] To search for an American's communications within the pool of Section 702 data, an FBI agent needed only a "reasonable basis to believe" that the query was "likely" to return foreign intelligence information or evidence of a crime—two broad and elastic categories. *Id.* at 76. Without any court approval, an FBI agent can type in an American's name, email address, or phone

[6] *See also, e.g.*, Off. Dir. Nat'l Intel., *Annual Statistical Transparency Report* at 24 (2022), http://bit.ly/3TPUDoD.

number, and pull up whatever communications the FBI's Section 702 collection has vacuumed into its databases over the past five years.[7]

This is exactly what happened with Mr. Hasbajrami. The government collected his communications under Section 702 in the course of targeting foreigners, and it stored and retained those communications in government databases. Over a period of at least six months, agents then repeatedly searched for and accessed Mr. Hasbajrami's communications without obtaining a warrant or any individualized judicial authorization. *Hasbajrami II*, 2025 WL 447498, at *11-12. Thus, even as Mr. Hasbajrami became the subject of a domestic criminal investigation, agents relied on Section 702 queries to gain access to his private communications, bypassing the judicial procedures that protect people in the United States. *Id.*

[7] The PCLOB recently reviewed the FBI's warrantless Section 702 queries and found little justification for the nearly 5 million U.S. person queries conducted between 2019 and 2022. *See* 2023 PCLOB Report at 196. FBI agents have used Section 702 queries to search for the communications of protestors, journalists, 19,000 donors to a congressional campaign, and even members of Congress. *See* Noah Chauvin, *Why Congress Must Reform FISA Section 702*, Brennan Ctr. for Just. (Apr. 9, 2024), https://perma.cc/PGV9-HVNX (collecting sources).

ARGUMENT

I. Querying U.S. person communications under Section 702 is a "separate Fourth Amendment event."

In its prior ruling, this Court held that the search of stored Section 702 data has "important Fourth Amendment implications," which "counsel in favor of considering querying a separate Fourth Amendment event." *Hasbajrami I*, 945 F.3d U.S. at 670. The Court recognized that Section 702 queries directed at U.S. persons like Mr. Hasbajrami represent a fundamentally different intrusion on privacy than the initial collection targeting foreigners. As discussed below, the district court properly applied that holding and its reasoning.

This Court described three core reasons for its conclusion that Section 702 queries of Americans' communications should be analyzed separately from collection of those communications under the Fourth Amendment.

First, it held that the government's justification for warrantlessly *collecting* the communications of foreigners abroad, who lack Fourth Amendment protection, does not justify its subsequent *searching* of that data for the private communications of Americans. As the Court recognized, the lawful collection of communications "is not always enough to justify a future search," and, as a result, "additional probable cause or reasonableness assessments" may be required to support such searches. *Id.* at 670 (citing *Riley v. California*, 573 U.S. 373, 401

(2014) and other cases).[8] Second, the Court recognized that the broad scope of Section 702, its technological capacity to vacuum up many kinds of modern communications, and the ability of domestic law enforcement to search Section 702 databases based "solely on the speculative possibility that evidence of interest" may be found, make Section 702 queries look like forbidden "general warrants." *Id.* at 671-72. Third, the Court highlighted that queries were especially "problematic" because they allow agents to seek "wide-ranging information" about a given U.S. person "when the government knows it is investigating such a person." *Id.* at 672. It observed that the data collected about a U.S. person under Section 702 may resemble what would have been gathered had that person been directly targeted in the first place, and so "[t]reating querying as a Fourth Amendment event" provides "a backstop to protect the privacy interests" of Americans. *Id*.

[8] Another line of Supreme Court cases further supports this holding. Because the Fourth Amendment carries a continuing requirement of reasonableness, searches or seizures that are lawful when initiated may become unlawful when they involve new or additional intrusions. *See Rodriguez v. United States*, 575 U.S. 348, 354-55 (2015) (traffic stop that was lawful when initiated violated Fourth Amendment when officer's investigation expanded beyond original justification); *United States v. Place*, 462 U.S. 696, 709-10 (1983) (seizure lawful at its inception can nevertheless violate the Fourth Amendment based on agents' subsequent conduct); *Terry v. Ohio*, 392 U.S. 1, 19 (1968) ("The scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible.").

After reaching these conclusions about the applicable Fourth Amendment framework, the Court declined to go further based on the record before it. It remanded the case for further factual and legal development, and it tasked the district court with deciding "whether any such querying violated the Fourth Amendment." *Id.* at 646. That analysis required the district court to consider both whether the searches at issue required a warrant and, if not, whether they were reasonable. *Id.* at 667-68, 673.

On remand, the government attempted to relitigate this Court's central holding, arguing that its agents' queries were lawful because they were "not a substantial additional intrusion" on privacy and because certain minimization rules apply at the time of collection. *See* Gov't Br. at 18, *United States v. Hasbajrami*, No. 11-cr-623 (E.D.N.Y. May 5, 2022), ECF No. 196 ("Gov't Br."). But this Court already rejected those arguments when it concluded that querying was a "separate Fourth Amendment event." *See Hasbajrami I*, 945 F.3d at 670, 672 (recognizing that querying is "at odds with the bedrock Fourth Amendment concept that law enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search"); *id.* at 669 (rejecting the argument that merely because minimization procedures rendered *collection* reasonable, "the government could freely query information it had lawfully acquired without further Fourth Amendment inquiry"). This Court's

holdings on these points are now law of the case. *See Arizona v. California*, 460 U.S. 605, 618 (1983).

II. The government's queries of Mr. Hasbajrami's communications violated the warrant requirement.

It is well-settled that for a search to comply with the Fourth Amendment, the government must obtain a warrant unless one of the "jealously and carefully drawn" exceptions to the warrant requirement applies. *Jones*, 357 U.S. at 499. Because the government did not obtain a warrant and none of the exceptions—including the foreign-intelligence exception—attach here, the government's querying of Mr. Hasbajrami's communications under Section 702 violated the Fourth Amendment.

A. As Fourth Amendment searches, the queries of Mr. Hasbajrami's communications presumptively required a warrant.

Searches conducted without a warrant are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967).

The government below urged the district court to skip over an analysis of the warrant requirement and to proceed directly to a Fourth Amendment "reasonableness" analysis. *See Hasbajrami II*, 2025 WL 447498, at *6. But the court properly rejected those arguments. *See id.* As the Supreme Court has explained, when a court is confronted with a warrantless search, the analysis

begins with the "basic rule" that warrantless searches are presumptively prohibited by the Fourth Amendment. *Arizona v. Gant*, 556 U.S. 332, 338 (2009); *see also City of Los Angeles v. Patel*, 576 U.S. 409, 419 (2015) (similar); *United States v. Kirk Tang Yuk*, 885 F.3d 57, 78 (2d Cir. 2018) (similar); *United States v. Weaver*, 9 F.4th 129, 138 (2d Cir. 2021) (similar). The court then evaluates whether a well-established, well-delineated exception to the warrant requirement applies. *See, e.g.*, *Riley*, 573 U.S. at 382.

Here, the district court was tasked on remand with determining whether the queries in this case "violated the Fourth Amendment." *Hasbajrami I*, 945 F.3d at 646. That analysis required the district court to begin with the warrant requirement, to assess whether any recognized exception to the warrant requirement applied, and only *then* to assess "reasonableness" in light of any exception. Its methodical approach was consistent with this Court's instructions and with this Court's own approach to analyzing the collection phase of Section 702 surveillance under the Fourth Amendment. *See id.* at 667-68 (addressing the warrant requirement and *then* assessing the reasonableness of the collection of Mr. Hasbajrami's communications).

As the district court recognized, the Supreme Court's decision in *Maryland v. King*, 569 U.S. 435 (2013), does not disturb this well-settled Fourth Amendment principle. *See Hasbajrami II*, 2025 WL 447498, at *6. While the government cited

King to argue that a warrant "is by no means inflexibly required," Gov't Br. at 17, that decision does not allow courts to simply bypass the warrant requirement when analyzing Fourth Amendment searches. *King* analyzed the privacy interests of arrestees at booking—a setting far removed from investigative searches of individuals who have not been arrested or detained, and whose privacy interests are therefore undiminished. *See King*, 569 U.S. at 461-64. Indeed, *King* itself adheres to the longstanding principle that a warrant is required unless a specific exception applies, as this Court has recognized. *See Pretzantzin v. Holder*, 736 F.3d 641, 648 (2d Cir. 2013) (discussing the "inventory or booking search exception" applied in *King*). And the Supreme Court in cases since *King* has reiterated the bedrock warrant rule. *See Riley*, 573 U.S. at 382; *Patel*, 576 U.S. at 419.

Here, the government did not obtain a warrant before searching its Section 702 databases for Mr. Hasbajrami's communications. Accordingly, unless an exception to the warrant requirement applies—and it does not for the reasons discussed *infra*—the search violated the Fourth Amendment.

B. Any "foreign intelligence" exception to the warrant requirement does not apply in this case.

The government argued below that its warrantless queries of Mr. Hasbajrami's communications should be permitted under a "foreign intelligence" exception to the warrant requirement. *Hasbajrami II*, 2025 WL 447498, at *11. But neither the Supreme Court nor this Court has ever recognized such an

exception. *See United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 308-09 (1972) (reserving decision on the existence of such an exception); *In re Terrorist Bombings*, 552 F.3d 157, 172 (2d Cir. 2008).[9] Although the exception has not been widely recognized, some appeals courts have adopted a narrow version of this exception where the surveillance is directed at the agent of a foreign power and other strict conditions are met. The district court here applied one of those decisions and correctly rejected the government's arguments, holding that "[n]one of the concerns that the foreign intelligence exception was designed to address are present," and, in particular, a warrant requirement would not have "impeded the government's 'ability to collect time-sensitive information.'" *Hasbajrami II*, 2025 WL 447498, *15 (quoting *In re Directives*, 551 F.3d 1004, 1011-12 (FISCR 2008)).

This Court should likewise reject any application of the foreign-intelligence exception. The government urged the district court to apply an unprecedented and extraordinarily broad version of this exception—one that is far from jealously drawn. *Jones*, 357 U.S. at 499. It argued that because the government's "programmatic purpose" in querying Section 702 information goes beyond "ordinary law enforcement" and implicates foreign intelligence gathering, the

[9] *See also, e.g.*, *United States v. Mohamud*, 843 F.3d 420, 441 & n.25 (9th Cir. 2016) (declining to address "any 'foreign intelligence exception'").

warrant requirement evaporates. *Hasbajrami II*, 2025 WL 447498 at *11. But no court of appeals has ever endorsed such a sweeping rule. If a foreign-intelligence exception exists at all, it applies only where (1) the surveillance in question is directed at foreign powers or their agents; (2) the surveillance is authorized by the Attorney General or a court after a finding, based on individualized suspicion, that the target is a foreign power or a foreign agent; and (3) obtaining a warrant would be impracticable because information "vital" to national security would be lost. *See In re Directives*, 551 F.3d 1004, 1010-12, 1014 (FISCR 2008); 2014 PCLOB Report at 90 n.411 (discussing cases).

The warrantless queries of Mr. Hasbajrami fail this test. Under Section 702, neither collection nor querying is confined to "foreign powers or agents of foreign powers"—a limitation the FISCR has deemed critical in its decisions. *See In re Directives*, 551 F.3d at 1012-16; *In re Certified Question of Law*, 858 F.3d 591, 607 (FISCR 2016).[10] Moreover, the few appellate cases applying the exception have generally done so only where the Attorney General or a court made an individualized finding that the target was a foreign power or foreign agent and authorized the surveillance. Yet there is no indication in the public record that the

[10] Instead, under Section 702, the government may target any non-citizen outside the United States to collect "foreign intelligence information," broadly defined; and, as of 2011, agents could query *any* U.S. person to seek evidence of a crime or foreign intelligence information. *See* 2014 PCLOB Report at 130.

government had probable cause to believe that Mr. Hasbajrami was an agent of a foreign power, or that the Attorney General approved the queries—and it is clear that these particular queries were not approved by any court.

Perhaps most importantly, the foreign-intelligence exception cases address the *collection* phase of surveillance, where delays could in theory risk undermining the government's ability to acquire information at all. But here, the government seeks to apply the exception to an entirely novel context: the subsequent *querying* of Americans' communications. *See Hasbajrami I*, 945 F.3d at 670-71 (reasoning that the justifications for collection do not automatically impute to querying); *Hasbajrami II*, 2025 WL 447498, at *15 (explaining that the risks of delayed collection of foreign intelligence do not apply to delayed querying). This Court should decline to endorse such a dramatic expansion of the doctrine.

The history of the foreign-intelligence exception also confirms that, insofar as it exists, it must be narrowly applied. Prior to the enactment of FISA, a handful of circuit decisions approved warrantless surveillance under the President's authority to address foreign security matters. But this Court has expressly declined to follow these pre-FISA cases. *See In re Terrorist Bombings*, 552 F.3d at 172. In any event, these cases are nothing like this one: they involved individualized approval of the surveillance by the Attorney General; the surveillance was directed at foreign powers or their agents; and most courts further limited the exception to

surveillance conducted "solely" or "primarily" for foreign intelligence purposes. *See United States v. Truong*, 629 F.2d 908, 912-16 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 604-06, 621 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-26 (5th Cir. 1973). And the pre-FISA cases were not unanimous on whether a foreign-intelligence exception existed. *See Zweibon v. Mitchell,* 516 F.2d 594, 651 (D.C. Cir. 1975) (en banc) (plurality op.); *id.* at 689 (Wilkey, J. concurring) (reserving decision on existence of exception). As the *Zweibon* plurality explained, "given the way in which almost any activity can be said to relate, at least remotely, to foreign affairs or foreign policy making, the potential scope of such an exception to the warrant requirement is boundless, and thus a substantial danger to the values the Fourth Amendment was fashioned to protect." *Id.* at 654.[11]

Moreover, even the narrow foreign-intelligence exception in *Truong*, *Butenko*, and *Brown* was undercut by Congress's enactment of FISA in 1978. Following revelations about decades of executive branch surveillance abuses, Congress imposed strict judicial limits on foreign-intelligence surveillance. While the pre-FISA cases expressed concern that a warrant requirement would "seriously fetter the Executive," *Butenko*, 494 F.2d at 605, the country's experience with

[11] One other pre-FISA circuit opinion, *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977), approved warrantless wiretaps in passing, with no legal analysis or discussion of the underlying facts.

FISA over nearly 50 years has profoundly undermined that rationale. In the intervening years, the FISC has granted more than 43,000 applications for foreign-intelligence surveillance—showing that courts are entirely capable of overseeing such surveillance while allowing the executive branch to obtain sensitive information.[12]

Case law since FISA's enactment further illustrates the narrowness of any foreign-intelligence exception. Unlike criminal warrants, Title I of FISA requires the government to establish probable cause to the FISC that the target of the surveillance is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805. Over the decades, defendants have challenged traditional Title I FISA surveillance on various grounds, including that FISA orders are not truly "warrants" under the Fourth Amendment. Nevertheless, this Court and others have upheld the constitutionality of Title I of FISA—reasoning that FISA's procedures flexibly "implement" the Fourth Amendment's warrant requirement. *United States v. Abu-Jihaad*, 630 F.3d 102, 121 (2d Cir. 2010) (explaining that because FISA satisfies the warrant requirement, the Court need not consider whether a warrant exception applies). While these Title I decisions uphold narrow modifications to the Fourth Amendment's probable-cause requirement, they do not sanction the categorical warrant exception that the government seeks to apply here.

[12] *FISA Court Orders 1979-2023*, Elec. Priv. Info. Ctr., https://bit.ly/451s3pu.

The only contemporary court of appeals to apply a foreign-intelligence exception is the FISCR, and only under far more restrictive conditions than those urged by the government. The FISCR has applied the exception only at the *collection* phase of surveillance; only where the surveillance was targeted at foreign powers or their agents; and only where a warrant requirement "would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011-12, 1014; *see also In re Certified Question of Law*, 858 F.3d at 606 (similar). The FISCR reasoned by analogy to the "special needs" line of case law, where needs "beyond the normal need for law enforcement[] make the warrant and probable-cause requirement[s] impracticable." *In re Directives*, 551 F.3d at 1010 (quoting *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)).[13] In applying even this narrow exception, the court openly acknowledged it was breaking new ground that it had previously "avoided." *Id.*

[13] The FISCR also cited *Truong*, 629 F.2d at 915, for the proposition that "'the government has the greatest need for speed, stealth, and secrecy'" when "the object of a surveillance is a foreign power or its collaborators." *In re Directives*, 551 F.3d at 1011. However, as the district court correctly noted, "stealth" and "secrecy" alone "do not justify a departure from the Fourth Amendment warrant requirement," because these dangers can be "minimized by proper administrative measures," as the Supreme Court found in *Keith*. *Hasbajrami II*, 2025 WL 447498, at *13 n.19.

Even assuming that the FISCR's adoption of the foreign-intelligence exception was proper, the government's queries of Mr. Hasbajrami's communications fail the FISCR's test. As discussed above, the district court correctly held that obtaining a warrant before querying Mr. Hasbajrami's communications would not have impeded the collection of time-sensitive information. *Hasbajrami II*, 2025 WL 447498 at *15 (citation omitted). For many of the queries, the government entirely failed to explain how obtaining a warrant prior to the query would have hindered its objectives. *Id.* at *14. For other queries, the court found it "*inconceivable* that the government's aims would have been frustrated by securing a warrant at any time over the course of many months." *Id.* (emphasis added). There was no fast-moving investigation; the communications at issue were already "securely stored" in government databases; and there was no danger of evidence being destroyed or becoming inaccessible. *Id.* at *14-15.

Even if the government had a foreign-intelligence purpose when querying Mr. Hasbajrami's communications, that fact alone would not render the warrant and probable-cause requirements impracticable. In *Keith*, the Supreme Court expressly rejected the government's argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316-21. That logic applies with equal force here, where the government's

searches were directed at an American's communications and not at obtaining foreign intelligence from foreign targets.

Finally, the possibility of exigent or emergency circumstances is no basis for eliminating the warrant requirement wholesale when it comes to Section 702 queries. If the government encounters genuine exigency, it may rely on the exigent-circumstances exception. *See Kentucky v. King*, 563 U.S. 452, 455 (2011). Not only that, but as the district court observed, if the government believes there is an emergency, FISA itself allows the Attorney General to authorize an emergency search and subsequently make an application to the FISC for retroactive approval. *Hasbajrami II*, 2025 WL 447498, at *14 (citing 50 U.S.C. § 1805(e)). These exceptions confirm that the general Fourth Amendment rule—a warrant based on probable cause—is indeed practicable.

III. Even if a warrant exception applied, the queries of Mr. Hasbajrami's communications were unreasonable under the Fourth Amendment.

Assuming *arguendo* that an exception to the warrant requirement applies, the Section 702 queries of Mr. Hasbajrami's communications still violated the Fourth Amendment because they were unreasonable. Searches of U.S. person communications under Section 702 lack the core safeguards courts typically look for as indicia of reasonableness. Even if a warrant is not required, the procedures governing Section 702 queries must be sufficiently robust to ensure that government agents cannot indiscriminately intrude on protected privacy interests.

Given the complete absence of such safeguards when Mr. Hasbajrami was surveilled, the district court was correct to conclude that the substantial degree of intrusion associated with the queries outweighed the government's legitimate interests.

A. Queries of U.S. person communications lack the core safeguards courts apply when assessing the reasonableness of electronic surveillance.

In the context of electronic surveillance, reasonableness requires that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger v. New York*, 388 U.S. 41, 58 (1967); *see United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973).

Courts assessing the lawfulness of electronic surveillance have looked to the core safeguards in Title III—individualized judicial review, a finding of probable cause, and particularity—as measures of reasonableness. *See United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986) ("[W]e deem it wise, if not necessary, to look to the more precise standards Congress adopted in Title III" in assessing whether another type of electric surveillance was reasonable); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1437-39 & n.5 (10th Cir. 1990) (looking to the safeguards in Title III in assessing the reasonableness of video surveillance); *In re Sealed Case*, 310 F.3d 717, 737 (FISCR 2002) ("[T]he closer [the challenged]

procedures are to Title III procedures, the lesser are [the] constitutional concerns."). Indeed, courts have upheld the constitutionality of traditional FISA surveillance because it adopts the core safeguards associated with Title III surveillance. *See, e.g.*, *United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir. 1984); *In re Sealed Case*, 310 F.3d at 739-40.

But none of these core safeguards apply to queries of U.S. person communications under Section 702. First, Section 702 fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Katz*, 389 U.S. at 357. Under Section 702, the FISC's role consists principally of reviewing agency procedures. *See Hasbajrami I*, 945 F.3d at 652 ("In contrast to traditional domestic search warrants and FISA warrants . . . judicial review of Section 702 functions as a form of programmatic pre-clearance."). Decisions concerning whom to query are left to the discretion of executive branch employees, even as these decisions affect countless U.S. persons.

Second, Section 702 fails to condition the querying of U.S. person communications on the existence of probable cause of any kind. It permits the government to conduct searches without establishing to a court—and without even an executive branch determination—that the people whose information it is searching are foreign agents, engaged in criminal activity, or connected with terrorism.

And third, queries of U.S. person communications under Section 702 are not particularized. The requirement of particularity "is especially great in the case of eavesdropping," which inevitably results in the interception of unrelated, intimate conversations. *Berger*, 388 U.S. at 56. Unlike Title III, however, Section 702 does not require the government to identify to any court the email addresses, telephone lines, or places at which its queries will be directed, or "the particular conversations to be seized." *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). Instead, it permits the government to query and review the full contents of all the communications swept up in its massive collection.

Reasonableness may permit a degree of flexibility when it comes to the requirements above. *See In re Sealed Case*, 310 F.3d at 739-40. And indeed, the PCLOB and others have proposed procedures that stop short of a traditional warrant but would significantly strengthen querying protections for Americans. *See, e.g.*, President's Review Group, *Liberty and Security in a Changing World* 28-29, 145-50 (2013), https://perma.cc/4T8X-UJX6 (proposing modified probable-cause requirement); 2023 PCLOB Report at 12-13, 205-09, 216-24. But the complete absence of any individualized judicial review, any finding of probable cause, and any rules that would ensure particularity, permits agents to conduct fishing expeditions through Americans' private communications—exactly the kinds of searches that the Fourth Amendment prohibits.

B. The district court correctly balanced the degree of intrusion and the government's interest in concluding that the queries were not reasonable.

As this Court held in *Hasbajrami I*, "[t]o determine whether a search is reasonable under the Fourth Amendment, we examine the totality of the circumstances to balance, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." 945 F.3d at 666 (quoting *In re Terrorist Bombings*, 552 F.3d at 172). The totality of the circumstances includes the strength or weakness of any protections that constrain the government's intrusions on privacy. *See, e.g.*, *In re Directives*, 551 F.3d at 1012; [*Redacted*], 2011 WL 10945618, at *27-28. While the FBI has imposed tighter restrictions on querying in recent years in response to persistent violations, those rules "were not in place" in 2011. *Hasbajrami I*, 945 F.3d at 658. Given the extraordinarily lax standards that applied when Mr. Hasbajrami's communications were queried, the district court correctly held that the searches at issue represented a significant intrusion on privacy, one that outweighed the government's interests.

First, there is no question that Mr. Hasbajrami had a substantial privacy interest in his emails and electronic communications. *See id.* at 666; *United States v. Maher*, 120 F.4th 297, 307 (2d Cir. 2024); *United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016) (Gorsuch, J.) (noting that email is "a form of

communication capable of storing all sorts of private and personal details"). The FISC, too, has found that the privacy interests implicated by Section 702 queries are "substantial." [*Redacted*], 402 F. Supp. 3d at 87. As the FISC reasoned, the substantial degree of intrusion occurs precisely because the government acquires the "full contents" of vast numbers of communications, and queries allow FBI agents to sift through that trove of information for the communications of particular Americans. *Id.* at 75, 87-88.

Second, the government's rules in 2011 placed few meaningful constraints on agents' ability to conduct these intrusive searches of Mr. Hasbajrami and others. Despite the substantial privacy interests at stake, the FBI's policy was to encourage "maximal querying of Section 702 information," including in domestic criminal investigations unrelated to any foreign intelligence need. *Id.* at 78. The FBI's rules permitted agents to do so even at the earliest "assessment" stages of investigations, well before a full investigation had been opened. *See id.* at 80. The standards for conducting such queries were lax by design. As discussed, they simply required FBI agents to have a "reasonable basis to believe" that their queries were "likely" to return foreign intelligence information or evidence of a crime—a standard that imposed little practical constraint. *Id.* at 76; *see also* Background, *supra*. On top of that, the rules ensured little accountability. Not only were agents free to bypass obtaining a warrant, but 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.*

These permissive rules resulted in significant intrusions on Americans' privacy, including Mr. Hasbajrami's. Indeed, as the district court held with the benefit of the classified record, the Section 702 queries of Mr. Hasbajrami's communications involved far more than a minimal intrusion on privacy. *Hasbajrami II*, 2025 WL 447498, at *18 (citing "the volume of queries conducted, the length of time during which the queries occurred, and the type of communication subject to querying").[14]

This intrusiveness outweighs the degree to which the Section 702 queries here were needed "for the promotion of legitimate government interests." *Hasbajrami I*, 945 F.3d at 666. As the district court rightly recognized, this analysis does not simply weigh the government's general interest in Section 702 queries, but rather "whether the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search." *Hasbajrami II*, 2025 WL 447498, at *18 (quoting *Camara v. Mun. Ct. of City & Cnty. of San Francisco*, 387 U.S. 523,

[14] The FBI's lax rules also 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. [*Redacted*], 402 F. Supp. 3d at 76-78, 87.

533 (1967)). Thus, legitimate government interests—like "discovering potential links between foreign terrorist groups and persons within the United States," Gov't Br. at 19—are insufficient on their own to justify a search. Instead, the government must show why reasonable safeguards would have prevented it from realizing such interests. The government did not make that showing here based on the district court's review of the record—in part because the government presented little concrete justification for why its "dozens" of queries over many months were "uniquely 'time-sensitive' as to not require a warrant." *Hasbajrami II*, 2025 WL 447498, at *19.

The government has claimed that courts "would face a staggering burden" if agents had to seek judicial approval to query and review Americans' communications, Gov't Br. at 19, but that is wrong. First, the government ignores that stricter standards for U.S. person queries would require agents to have, for example, individualized suspicion of criminal activity or connection to a foreign power—meaning fewer searches in the first place. *See, e.g.*, *Mem. Op. & Order [Redacted]* at 22-23, (FISC Apr. 21, 2022), https://perma.cc/7SLA-Y5GU (noting the FBI's longstanding "pattern of broad, suspicionless queries"). Second, many of the safeguards that have been proposed are tailored to the querying context, in order to ensure that they are administrable. *See* 2023 PCLOB Report at 206 (recommending that the FISC approve U.S. person query terms subject to certain

conditions). In any event, the Court here need not determine precisely what safeguards are required today; it need only agree that the searches of Mr. Hasbajrami in 2011 were unreasonable.

Importantly, in analyzing reasonableness, the mere burden of obtaining court approval does not overcome the considerable privacy interests at stake. *See Johnson v. United States*, 333 U.S. l 0, 15 (1948) ("No reason is offered for not obtaining a search warrant except the inconvenience to the officers and some slight delay necessary to prepare papers and present the evidence to a magistrate. These are never very convincing reasons[.]"). While judicial review and other safeguards may require investigators to take additional steps to justify their searches, that is true of virtually all Fourth Amendment safeguards. Government convenience does not dictate whether a search is reasonable given the substantial privacy interests at stake.

Finally, stronger safeguards would not prevent the government from accessing the communications of U.S. persons under Section 702. *See supra* Section II.B (discussing exigent-circumstances exception and FISA's emergency provision). More broadly, the government itself has recognized that stronger querying protections are necessary and practicable. In the years since Mr. Hasbajrami was surveilled, the FISC, Congress, and the executive branch have all imposed new requirements on Section 702 queries given their intrusiveness and

widespread abuse. *See, e.g.*, [*Redacted*], 402 F. Supp. 3d at 86-88 (finding Section 702 querying rules constitutionally unreasonable); FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018) (requiring agencies to submit querying procedures to the FISC for annual approval); FBI Section 702 Querying Procedures (Mar. 1, 2024), https://bit.ly/4lRHTda.

The Court need not determine whether today's querying procedures are adequate to protect Americans (and amici believe they are not). But given the absence of even these protections in 2011, the Court can readily conclude that the searches of Mr. Hasbajrami were unreasonable under the Fourth Amendment.

CONCLUSION

For the foregoing reasons, the government's querying of Mr. Hasbajrami's communications violated the Fourth Amendment.

Dated: July 22, 2025

Respectfully submitted,

/s/ Patrick Toomey
Patrick Toomey
Ashley Gorski
Sara Robinson
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
ptoomey@aclu.org

Andrew Crocker
ELECTRONIC FRONTIER

FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 29(a)(4)(G), I certify as follows:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) because this brief contains 6,968 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

Dated: July 22, 2025

/s/ Patrick Toomey
Patrick Toomey