

24-1648-CR(L)

25-542-cr(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*

BRIEF FOR DEFENDANT-APPELLANT

Michael K. Bachrach
LAW OFFICE OF MICHAEL K. BACHRACH
224 West 30th Street, Suite 302
New York, New York 10001
212-929-0592

Joshua L. Dratel
DRATEL & LEWIS
29 Broadway, Suite 1412
New York, New York 10006
212-732-0707

Steve Zissou
STEVE ZISSOU & ASSOCIATES
42-40 Bell Boulevard, Suite 302
Bayside, New York 11361
718-279-4500

Attorneys for Defendant-Appellant

Table of Contents

Table of Contents.....i

Table of Authorities.....iv

Statement of Subject Matter and Appellate Jurisdiction.....1

Statement of the Issues.....1

Preliminary Statement and Statement of the Case.....2

Statement of Facts.....4

A. *Procedural History*.....4

 1. *Hasbajrami’s Arrest, the Charges, and His Initial Plea of Guilty*.....4

 2. *The Government Confesses It Misled Hasbajrami and the Court*.....5

 3. *The Renewed Motion to Suppress and the District Court’s Opinion*.....6

 4. *Hasbajrami’s Initial Appeal*.....7

 5. *Proceedings Upon Remand and the District Court’s Opinion*.....8

POINT I

THE DISTRICT COURT ERRED IN APPLYING THE
“GOOD FAITH” EXCEPTION TO DENY THE MOTION
TO SUPPRESS IN THIS CASE WHICH SHOULD HAVE
BEEN GRANTED UNDER FISA AND/OR THE FOURTH AMENDMENT.....10

A. *Standard of Review*.....11

B. *Relevant History Regarding FISA and Section 702 Querying*.....11

C. *Section 702 Querying*.....14

D. <i>The “Good Faith” Exception Does Not Apply to FISA’s Statutory Suppression Provisions</i>	19
1. <i>The District Court’s Opinion</i>	19
2. <i>FISA’s Suppression Provision Incorporates Constitutional Violations</i> ..	20
E. <i>The “Good Faith” Exception Should Not Apply to the Circumstances Present Herein</i>	29
1. <i>The Principles Guiding Application of the “Good Faith” Exception</i>	29
2. <i>The Government’s Conduct in This Case Alone Should Deprive It of Resort to the “Good Faith” Exception</i>	31
3. <i>The Systemic, Historical Non-Compliance That Has Plagued Section 702’s Querying Process – Including During the Period at Issue Herein – Further Vitiates Any Claim of “Good Faith”</i>	35
a. <i>Section 702 Was Initiated as an Illegal Warrantless Program</i>	35
b. <i>The Extraordinary Scope of Section 702 Interception and Retention</i>	37
c. <i>Section 702’s Unremitting History of Non-Compliance</i>	40
i. <i>The 2011 FISC Opinion</i>	41
ii. <i>The 2014 PCLOB Report</i>	43
iii. <i>The 2017 FISC Opinion</i>	44
iv. <i>The 2018 FISC Opinion</i>	46
v. <i>The Government’s Appeal of the 2018 FISC Op.</i>	49
vi. <i>The 2019 FISC Opinion</i>	51

vii. <i>The 2020 FISC Opinion</i>	52
viii. <i>The 2022 FISC Opinion</i>	53
ix. <i>The 2023 PCLOB Report</i>	59
3. <i>FISA’s History of Non-Compliance Generally Warrants Rejection Of Application of the “Good Faith” Exception Here</i>	60
F. <i>Case Law Establishes That the “Good Faith” Exception Should Not Apply Here</i>	64
G. <i>The Balancing Performed as Part of the “Good Faith” Analysis Overwhelmingly Favors Suppression Here</i>	68
 POINT II	
 THE DISTRICT COURT ABUSED ITS DISCRETION IN DENYING SECURITY-CLEARED DEFENSE COUNSEL ACCESS TO THE CLASSIFIED MATERIALS THAT FORMED THE BASIS FOR THE DISTRICT COURT’S FINDING THAT “GOOD FAITH” APPLIED.....	
A. <i>Standard of Review</i>	72
B. <i>The District Court’s Opinion</i>	73
C. <i>FISA’s Provisions Require Disclosure In This Case</i>	74
1. <i>The District Court Misread the FISA Disclosure Provision</i>	74
2. <i>Disclosure Was “Necessary” In Relation to the District Court’s Decision Regarding “Good Faith”</i>	78
D. <i>Due Process Requires Disclosure</i>	79
E. <i>CIPA Provides a Well-Established Means of Disclosure</i>	80
Conclusion.....	83

Table of Authorities

Cases

<i>14 Penn Plaza LLC v. Pyett</i> , 556 U.S. 247 (2009).....	48
<i>Accord United States v. Ott</i> , 827 F.2d 473 (9th Cir.1987).....	22
<i>ACLU Foundation of Southern California v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991).....	21, 22
<i>ACLU v. Clapper</i> , 785 F.3d 787 (2d Cir. 2015).....	60
<i>Alderman v. United States</i> , 394 U.S. 65 (1969).....	23, 75, 76, 78
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	30
<i>Board of Education v. Rice</i> , A.C. 179 (1911).....	79
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018).....	66
[(<i>Case Name Redacted</i>), PR/TT No. [docket redacted] (FISC [date redacted]) (declassified Nov. 18, 2013).....	61
<i>Chandler v. Miller</i> , 520 U.S. 305 (1997).....	66
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000).....	66
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	5, 6
<i>Davis v. United States</i> , 564 U.S. 229 (2011).....	19, 31, 64, 68, 69
<i>Fazaga v. Fed. Bureau of Investigation</i> , 965 F.3d 1015 (9th Cir. 2020), rev’d and remanded on alternate grounds, 595 U.S. 344 (2022).....	22, 78
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978).....	22, 76, 78
<i>Green v. McElroy</i> , 360 U.S. 474 (1959).....	81

<i>Hennepin Cnty. v. Fed. Nat. Mortg. Ass’n</i> , 742 F.3d 818 (8th Cir. 2014).....	26
<i>Herring v. United States</i> , 555 U.S., 135 (2009).....	31, 67, 68
<i>Hudson v. Michigan</i> , 547 U.S. 586 (2006).....	69
<i>Illinois v. Krull</i> , 480 U.S. 340 (1987).....	68
<i>In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], No. BR 09-13, 2009 WL 9150896 (FISA Ct. Sept. 25, 2009)</i>	61
<i>In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], No. BR 09-06 (FISC June 22, 2009)</i>	61
<i>In re Carter Page, a U.S. Person, Docket Nos. 16-1182, 17-52, 17-375, 17-679 (FISA Ct.)</i>	61
<i>In re Directives [redacted]</i> , 551 F.3d 1004 (FISCR 2008).....	38
<i>In re DNI/AG 702(h) Certifications 2018, 941 F.3d 547 (Foreign Int. Surv. Ct. Rev. 2019)</i>	17, 49, 50, 51, 52
<i>In re 650 Fifth Ave. & Related Props</i> , 934 F.3d 147 (2d Cir. 2019).....	67
<i>In re Foreign Intelligence Surveillance Court (Redacted), 2011 WL 10945618 (FISC 2011)</i>	39, 41
<i>In re Foreign Intelligence Surveillance Court [Redacted], 402 F. Supp.3d 45 (Foreign Intel. Surv. Ct. 2018)</i>	16, 17, 18, 46, 47, 48, 49, 52
<i>In re Production of Tangible Things From [Redacted], No. BR 08-13, 2009 WL 9150913 (FISA Ct. March 2, 2009)</i>	61
<i>Joint Anti-Fascist Refugee Committee v. McGrath</i> , 341 U.S. 123 (1951).....	79

<i>Kungys v. United States</i> , 485 U.S. 759 (1998).....	25
<i>LeMay v. U.S. Postal Serv.</i> , 450 F.3d 797 (8th Cir. 2006).....	26
<i>Memorandum Opinion and Order [Redacted]</i> , (FISC April 21, 2022).....	53, 54, 55, 57, 58
<i>Norman v. United States</i> , 942 F.3d 1111 (Fed. Cir. 2019).....	26
<i>Prokop v. Lower Loup Nat. Res. Dist.</i> , 302 Neb. 10, 921 N.W.2d 375 (2019).....	26
<i>Redacted</i> , 402 F. Supp. 3d 45 (Foreign Intel. Surv. Ct. 2018).....	17
<i>[Redacted]</i> , <i>Mem. Op.</i> (FISC April 26, 2017).....	44, 45
<i>[Redacted]</i> , <i>Mem. Op.</i> , (FISC Dec. 6, 2019).....	51, 52
<i>[Redacted]</i> , <i>Mem. Op.</i> , (FISA Ct. Nov. 18, 2020).....	52
<i>Reynolds v. United States</i> , 345 U.S. 1 (1953).....	82
<i>Scott v. United States</i> , 436 U.S. 128 (1978).....	30
<i>TikToc Inc. v. Garland</i> , 145 S.Ct. 57 (2025).....	81
<i>United States v. Abuhamra</i> , 389 F.3d 309 (2d Cir. 2004).....	78, 79
<i>United States v. Abu-Jihaad</i> , 531 F. Supp.2d 299 (D. Conn. 2008), aff'd 630 F.3d 102 (2d Cir. 2010).....	22, 23, 73, 77
<i>United States v. Aref</i> , 553 F.3d 72 (2d Cir. 2008).....	72
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C.Cir.1982).....	22, 78
<i>United States v. Butler</i> , 297 U.S. 1 (1936).....	25
<i>United States v. Chambers</i> , 751 F. App'x 44 (2d Cir. 2018).....	66

<i>United States v. Daoud</i> , 755 F.3d 480 (7th Cir. 2014).....	75
<i>United States v. Davis</i> , 598 F.3d 1259, 1266 (11th Cir. 2010), aff'd, 564 U.S. 229 (2011).....	65
<i>United States v. DePalma</i> , 461 F.Supp. 800 (S.D.N.Y. 1978).....	30
<i>United States v. Duggan</i> , 743 F.2d 59 (2d Cir. 1984).....	77, 78
<i>United States v. Ganas</i> , 755 F.3d 125 (2d Cir. 2014), rev'd on other grounds, 824 F.3d 199 (2d Cir. 2016).....	29
<i>United States v. Giordano</i> , 416 U.S. 505 (1974).....	21
<i>United States v. Hasbajrami</i> , 945 F.3d 641(2d Cir. 2019).....	<i>passim</i>
<i>United States v. Hasbajrami</i> , 2014 WL 4954596 (E.D.N.Y. Oct. 2, 2014).....	6
<i>United States v. Hasbajrami</i> , No. 11 Cr. 623 (LDH), 2025 WL 447498 (E.D.N.Y. Feb. 10, 2025).....	<i>passim</i>
<i>United States v. Hasbajrami</i> , Nos. 15-2684, 17-2669 (2d Cir. Sept. 4, 2018).....	32, 33
<i>United States v. Hyde</i> , 574 F.2d 856 (5th Cir. 1978).....	30
<i>United States v. Karathanos</i> , 531 F.2d 26 (2d Cir. 1976).....	70
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	23, 28, 30, 31
<i>United States v. Lucky</i> , 569 F.3d 101 (2d Cir. 2009).....	11
<i>United States v. Lyles</i> , 910 F.3d 787 (4th Cir. 2018).....	30
<i>United States v. McGuinness</i> , 764 F. Supp. 888 (S.D.N.Y. 1991).....	28
<i>United States v. Moalin</i> , 973 F.3d 977 (9th Cir. 2020).....	60

<i>United States v. Moussaoui</i> , 333 F.3d 509 (4th Cir. 2003).....	80
<i>United States v. Moussaoui</i> , 365 F.3d 292 (4th Cir.), opinion amended on reh'g, 382 F.3d 453 (4th Cir. 2004).....	80
<i>United States v. Muhtorov</i> , 20 F.4th 558 (10th Cir. 2021).....	6, 47
<i>United States v. Ning Wen</i> , 477 F.3d 896 (7th Cir. 2007).....	23, 24
<i>United States v. Orozco</i> , 630 F. Supp. 1418 (S.D. Cal. 1986).....	28
<i>United States v. Ott</i> , 827 F.2d 473 (9th Cir. 1987).....	78
<i>United States v. Rice</i> , 478 F.3d 704 (6th Cir. 2007).....	27
<i>United States v. Rosa</i> , 626 F.3d 56 (2d Cir. 2010).....	66
<i>United States v. Varela</i> , 968 F.2d 259 (2d Cir. 1992).....	30
<i>United States v. Voustianiouk</i> , 685 F.3d 206 (2d Cir. 2012).....	29
<i>United States v. Wey</i> , 256 F. Supp.3d 355 (S.D.N.Y. 2017).....	66, 67
<i>United States v. Zubaydah</i> , 595 U.S. 195 (2022).....	80, 82
<i>Weeks v. United States</i> , 232 U.S. 383 (1914).....	30

Statutes

8 U.S.C. §3231.....	1
18 U.S.C. § 2.....	4
18 U.S.C. §2339A(a).....	4
18 U.S.C. §2518.....	27
18 U.S.C. §§2518(10)(a)(i)-(iii).....	27

28 U.S.C. §1291.....	1
50 U.S.C. §1806(e).....	21, 24, 25, 27, 28, 29
50 U.S.C. §1806(e)(1).....	20, 25
50 U.S.C. §1806(f).....	20, 21, 22, 25, 28, 29, 77
50 U.S.C. §1806(g).....	20, 21, 22, 23, 24, 25, 26, 28, 29, 74, 75, 78
50 U.S.C. §1861.....	60
50 U.S.C. §1881a	<i>passim</i> , 12
50 U.S.C. §1881a(a).....	14
50 U.S.C. §1881a(f).....	16, 17
50 U.S.C. §1881a(f)(B).....	18, 50
50 U.S.C. §1881a(f)(2).....	57
50 U.S.C. §1881a(f)(2)(A).....	18
50 U.S.C. §1881a(f)(3).....	18
50 U.S.C. §1881a(f)(3)(B).....	14, 15
FISA Amendments Act (2008).....	16, 37
FISA Amendments Reauthorization Act (2017).....	16, 17, 18
U.S. Const. amend. IV.....	<i>passim</i>
Federal Bureau of Investigations, Minimization Procedures (2016), §III.D.....	17
Foreign Intelligence Surveillance Act (1978).....	<i>passim</i>

Protect America Act (2007).....37

Other Authorities

David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions*, (3d ed. 2019).....12, 15, 16, 20, 21, 63, 74

David S. Kris, “Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond,” *Journal of Nat. Sec. L. & Policy* (2016).....16

Dept. of Justice, Archives, N. Katyal, *Confessions of Error: The Solicitor General's Mistakes During the Japanese-American Internment Cases* (May 20, 2011).....82

J. Weinstein, *The Role of Judges in a Government of, by, and for the People: Notes for the Fifty-Eighth Cardozo Lecture*, 30 *Cardozo L. Rev.* 1, 92 (2008).....82

Karen Greenberg, *Rogue Justice* (2016).....36

The Office of the Director of National Intelligence’s Office of Civil Liberties, Privacy, and Transparency *Annual Statistical Transparency Report Regarding the Intelligence Community’s Use of National Security Surveillance Authorities, Calendar Year 2020* (April 2021).....39, 57

The Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702* (2014).....15, 17, 39, 43, 47

The Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report* (January 29, 2015).....43, 44

The Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (September 28, 2023).....13, 14, 59

W. Weaver & R. Pallitto, *State Secrets and Executive Power*, 120 *Pol. Sci. Q.* 85 (2005).....82

Statement of Subject Matter and Appellate Jurisdiction

This appeal is from a final judgment of the United States District Court for the Eastern District of New York, which had jurisdiction pursuant to 18 U.S.C. §3231, denying Defendant-Appellant Agron Hasbajrami’s motion to suppress the fruits of electronic surveillance. The Memo and Order appealed from was filed February 10, 2025 (A. 40),¹ and a Notice of Appeal was timely filed March 6, 2025. A. 100.

This Court has jurisdiction of the appeal pursuant to 28 U.S.C. §1291. This appeal returns to this Court after remand, and the District Court’s Judgment, following this Court’s opinion in *United States v. Hasbajrami*, 945 F.3d 641(2d Cir. 2019).

Statement of the Issues

I. Whether the District Court erred in applying the “good faith” exception in denying Hasbajrami’s motion to suppress evidence even though the District Court concluded the search at issue violated the Fourth Amendment; and

II. Whether the District Court abused its discretion in denying defense counsel – who possessed appropriate security clearance – access to classified materials essential to the District Court’s finding of “good faith.”

¹ “A.” refers to the Appendix filed as part of this appeal.

Preliminary Statement and Statement of the Case

This Opening Brief on Appeal is submitted on behalf of Defendant-Appellant Agron Hasbajrami, who is appealing from the District Court’s decision – upon remand from this Court following its opinion in *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (“*Hasbajrami I*”) – *not* to suppress evidence, and instead apply the “good faith” exception to the Fourth Amendment’s exclusionary rule, even though the District Court concluded that the search at issue was conducted in violation of the Fourth Amendment.

This case presents an issue of first impression with respect to the application of the “good faith” exception to querying under Section 702 that violates the Fourth Amendment.

As detailed below, there are several reasons why the good faith exception should not be available to the government: (1) the government *in this case* withheld critical information from Hasbajrami regarding the specific nature of the electronic surveillance, and was evasive and non-responsive *to this Court* during the prior appeal in this case, and to the District Court on remand; (2) the government’s implementation of the particular foreign intelligence electronic surveillance program, 50 U.S.C. §1881a, commonly referred to as Section 702, and particularly with respect to the querying of Section 702 databases that is at issue

herein, has been plagued from the outset, and continually for more than a decade, by significant non-compliance; and (3) the government’s continued failure to abide by the statutory provisions of the Foreign Intelligence Surveillance Act (“FISA”), of which Section 702 is a component, has also been rife with historical non-compliance.

In addition, the District Court erred in ruling that FISA’s suppression provisions, which are mandatory, do not incorporate Fourth Amendment challenges. As discussed below, the District Court’s decision is contrary to the plain language of the statute, case law, canons of construction, and even FISA’s legislative history.

The government’s invocation of the “good faith” doctrine is unavailing because it fails to address the government’s persistent violations of the Fourth Amendment and FISA in the context of Section 702 querying, which have uncorrected for decades with predictable results: they have continued unabated. Thus, the deterrent value of the exclusionary rule is at its zenith in this case.

In addition, closely related to the District Court’s application of the “good faith” exception – a fact-intensive inquiry – is its denial of Hasbajrami’s motion to permit his security-cleared attorneys’ access to the classified information and legal arguments upon which the District Court based its findings. As set forth below,

whether on statutory or constitutional grounds, denying security-cleared counsel access to those materials constituted error and precluded a complete and accurate assessment whether, indeed, the “good faith” exception applies in this case.

Accordingly, for all the reasons set forth below, it is respectfully submitted that the District Court’s denial of Hasbajrami’s motion to suppress on “good faith” grounds be reversed, or that the District Court’s decision denying security-cleared counsel access to the classified materials be reversed, and the matter remanded.

Statement of Facts

In light of the comprehensive explication of the facts provided by this Court in *Hasbajrami I*, 945 F.3d at 647-49, and the District Court, in its opinion below (“*Hasbajrami II*”), at A. 40-56, *United States v. Hasbajrami*, No. 11 Cr. 623 (LDH), 2025 WL 447498, at *4-5 (E.D.N.Y. Feb. 10, 2025), only those facts necessary and relevant to this appeal will be included herein.

A. *Procedural History*

1. *Hasbajrami’s Arrest, the Charges, and His Initial Plea of Guilty*

Agron Hasbajrami was arrested September 6, 2011, and has been in custody since that date. Ultimately, he was charged with three counts of provision and attempted provision of material support to terrorists, and one count of attempt to provide material support to terrorists, all in violation of 18 U.S.C. §§2339A(a), 2.

See Superseding Indictment, dated, January 26, 2012 (ECF # 20).

Hasbajrami pleaded guilty April 12, 2012, and was sentenced January 8, 2013, to 15 years' imprisonment (*see* Judgment, January 16, 2013 [ECF # 45]).

2. *The Government Confesses It Misled Hasbajrami and the Court*

As this Court recounted in *Hasbajrami I*, the government, in a February 24, 2014, letter to defense counsel, “stated that ‘based on a recent determination,’ it had concluded that the information obtained from FISA surveillance that the government had already disclosed ‘was itself also derived from other collection pursuant to Title VII of FISA [*i.e.*, Section 702] as to which you were aggrieved.’” *Hasbajrami I*, 945 F.3d at 648 (citation omitted).

This Court explained that “[t]he government’s provision of notice in this case was likely in response the Solicitor General’s assertion, at oral argument before the Supreme Court in *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013), that prosecutors would provide notice to defendants in cases where evidence was derived from Section 702 surveillance.” *Hasbajrami I*, 945 F.3d 648 n.3, *citing* Charlie Savage, “Door May Open Challenge to Secret Wiretaps,” *The New York Times*, October 17, 2013, at A3. *See also id.* (“[w]hile the government’s policy prior to *Clapper* was not to provide notice of Section 702 surveillance, it began reviewing cases and providing supplemental notice in 2013”); Charlie Savage,

“Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence,” *The New York Times*, October 26, 2013.

Upon learning that such notice was, in fact, not provided to defendants or their counsel, the Solicitor General instructed that such notice be provided *post hoc*. See also *United States v. Muhtorov*, 20 F.4th 558, 662, n.2 (10th Cir. 2021) (Lucero, J., *dissenting*) (“[t]he District Court pointed out, however, the confluence of the government’s belated §702 notice on October 25, 2013 and the 2013 [Edward] Snowden leaks, recognizing that: ‘until the Snowden leaks in 2013, the American public was led to believe that the government did not query or use [FISA Amendments Act]-acquired surveillance against non-targeted U.S. persons’”), *citing, Clapper*, 568 U.S. 398 (2013)).

3. *The Renewed Motion to Suppress and the District Court’s Opinion*

In response to the government’s belated disclosure, Hasbajrami moved to withdraw his guilty plea because, as Judge Gleeson concluded, “[w]hen the government provided FISA notice without [FISA Amendments Act] notice, Hasbajrami was misled about an important aspect of his case.” *United States v. Hasbajrami*, 2014 WL 4954596, *3 (E.D.N.Y. Oct. 2, 2014) (ECF # 85). See also *Hasbajrami I*, 945 F.3d at 648.

Judge Gleeson granted the motion, *id.*, and Hasbajrami reinstated his motion

to suppress. ECF # 92. Judge Gleeson denied that motion February 15, 2015, in a docket entry (and subsequently filed an Opinion March 8, 2106, ECF # 165) (including substitutions and redactions to reflect the government's unilateral decision that the material redacted would “expose government equities”).

Hasbajrami again pleaded guilty June 26, 2015 (ECF # 142), with the express reservation of his right to appeal his suppression motion. Hasbajrami was sentenced to 16 years’ imprisonment, *see* Judgment (ECF # 161; A. 34-38), and currently has a projected release date of September 9, 2025.

4. *Hasbajrami’s Initial Appeal*

Hasbajrami pursued in this Court his appeal from the District Court’s denial of his motion to suppress the fruits of the electronic surveillance, including evidence derived through the application of Section 702 surveillance. This Court issued an opinion in which it held (1) any inadvertent collection of Mr. Hasbajrami’s communications pursuant Section 702 was “harmless,” *Hasbajrami I*, 945 F.3d at 669; but that (2) “querying that stored data [consisting of the intercepted communications] does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable.” *Id.* at 670.

As a result, this Court remanded to the District Court for the purpose of

determining, “(a) what (if any) evidence relevant to Hasbajrami was obtained by the government by querying databases, (b) whether any such querying violated the Fourth Amendment and, if so, (c) whether any such violation tainted other lawfully-collected evidence.” *Id.* at 646-47.

5. *Proceedings Upon Remand and the District Court’s Opinion*

Upon remand, Hasbajrami moved to suppress, and for his security-cleared counsel to be permitted access to the classified materials (including legal briefs) relevant to the District Court’s ultimate determination whether the querying at issue violated FISA’s statutory provisions and/or the Fourth Amendment. *See* Defendant’s Post-Remand Memorandum of Law In Support of Motion for Suppression and Access to Related Discovery (“*Post-Remand Memo*”) (ECF # 191). The government’s response was substantially redacted with respect to the pertinent facts and arguments. *See* ECF # 196, at 6-8.

Hasbajrami filed a reply letter, ECF # 201, and supplemented his initial submission with two lengthy letters updating the District Court with respect to subsequent developments relevant to Section 702 specifically, and FISA generally, during the period his motion was pending. *See* ECF #s 205 & 206.

The District Court issued a Text Order May 1, 2024, denying suppression, advising that an opinion would be forthcoming. A. 39. That opinion was issued

January 21, 2025 (ECF # 219), but then revised to unredact certain portions (at Hasbajrami's request, *see* ECF # 220), and re-filed February 10, 2025 (ECF # 223; A. 40).

After extensive analysis, *see Hasbajrami II*, at A. 91, 2025 WL 447498 at *19, the District Court held that “the queries conducted as to Defendant were unreasonable under the Fourth Amendment.” A. 91; *Hasbajrami II*, 2025 WL 447498, at *19.

However, the District Court also denied suppression, “declin[ing] to impose the ‘harsh sanction’ of exclusion because the good faith exception applies.” *Id.* at 21; A. 92. The Court reached that conclusion because, “According to the Government, [Redacted] followed minimization procedures approved by the FISA Court and in place at the time when querying Section 702-acquired information as to Defendant. [Redacted].” *Id.*; A. 92-93.

In addition, “More importantly, the relevant queries here occurred in 2011, long before agents could have been expected to know that the querying required a warrant.” *Id.* The District Court also denied the motion to permit security-cleared defense counsel from having access to the relevant classified materials. *Id.* at 20; A. 93.

The District Court's denial of the motion to suppress based on the “good

faith” exception, as well as the denial of security-cleared counsel’s access to classified materials and briefing, are the subjects of this appeal.

POINT I

THE DISTRICT COURT ERRED IN APPLYING THE “GOOD FAITH” EXCEPTION TO DENY THE MOTION TO SUPPRESS IN THIS CASE WHICH SHOULD HAVE BEEN GRANTED UNDER FISA AND/OR THE FOURTH AMENDMENT

This appeal presents an issue of first impression: Whether the District Court erred in determining that the “good faith” exception applied to the government’s violations of FISA and the Fourth Amendment in its warrantless querying of the database(s) containing Hasbajrami’s electronic communications intercepted pursuant to Section 702.

The District Court’s error consists of two separate but related elements: (1) the “good faith” exception does not apply *at all* because FISA’s statutory provisions do not recognize the “good faith” exception when a violation occurs; and (2) the “good faith” exception should *not* apply to the Fourth Amendment violations that have been pervasive, repeated, systemic, and entirely unpunished with respect to this case, Section 702 historically, and FISA generally for decades.

Analysis of these two issues requires some recitation of the principles applicable to Section 702 querying specifically, and FISA generally, as well as to

some of their practical implications, but that exegesis will be abbreviated because, again, *Hasbajrami I*, 945 F.3d at 649-658, and *Hasbajrami II*, 2025 WL 447498, at 1-3 (A. 40-46), provide ample explanation of the history of FISA and Section 702, as well as to the mechanics of their implementation as instruments of foreign intelligence electronic surveillance.

A. *Standard of Review*

This Court reviews *de novo* a District Court’s decision regarding a motion to suppress evidence – including questions of law, and mixed questions of law and fact. *See United States v. Lucky*, 569 F.3d 101, 105-06 (2d Cir. 2009) (citing cases).

While the District Court claims that Hasbajrami did not move for suppression on the basis of statutory violations, *see Hasbajrami II*, 2025 WL 447498, at *21, in fact, Hasbajrami did move on that ground. *See Post-Remand Memo*, at 56 (asserting that the querying process “violated the Fourth Amendment and *the statute*”) (emphasis added).

B. *Relevant History Regarding FISA and Section 702 Querying*

Like ordinary warrants (and Title III warrants authorizing electronic surveillance), “traditional FISA” applications “must describe, among other things, whom the government wishes to search or surveil, the place or things to be

searched or surveilled, the sort of information the government expects to gather, and the existence and nature of any prior FISA applications targeting the individual.” *Hasbajrami I*, 945 F.3d at 650, *citing* David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions*, (3d ed. 2019) (“*Kris & Wilson*”), at §6:2.

Traditional FISA surveillance can be renewed in a manner similar to Title III renewals, but by FISA standards. Section 702, however, represents a radical departure not only from ordinary warrants, or Title III warrants, but even from “traditional” FISA applications and approvals.

Section 702 permits the Attorney General and Director of National Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the Foreign Intelligence Surveillance Court (“FISC”) the particular non-U.S. persons (or their electronic devices, or telephone numbers, or email addresses) who will be targeted. *See* 50 U.S.C. § 1881a(a).

The most recent report by the Privacy and Civil Liberties Oversight Board (“PCLOB,” constituted after the Edward Snowden disclosures in 2013), points out that “although Section 702 targets can only be non-U.S. persons, through

incidental collection the government acquires a substantial amount of U.S. persons' communications as well.” *The Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, September 28, 2023 (“2023 PCLOB Report”), at 178, available at <https://bit.ly/46acbD9>.

The intelligence community “uses the term ‘incidental’ because such collection is not accidental or inadvertent – rather, it is an anticipated collateral result of monitoring a target.” *Id.* (footnote omitted).

The 2023 PCLOB Report explained that “from a privacy and civil liberties perspective, incidental collection under Section 702 differs in at least two significant ways from incidental collection that occurs in the course of a criminal wiretap or the traditional FISA process.” *Id.* at 179 (footnote omitted): (1) “Section 702 allows the government to target a much broader range of people[]” because “collection is not limited to suspected terrorists or others engaged in nefarious activities[;]” and (2) “Section 702 targeting decisions lack the checks that are part of traditional FISA or criminal electronic surveillance[]” because, since only non-U.S. persons – “who lack recognized Fourth Amendment rights” – are formally targeted, “the statute does not require a judge to review and approve individual targets.” *Id.*

Nor is the scope of the problem subject to review. As the *2023 PCLOB Report* notes, “[t]here is currently no data or transparency identifying the magnitude of incidental collection of U.S. person information.” *Id.* Thus, while “[t]he term ‘incidental’ suggests that it is a small amount, . . . the government has not provided any actual metrics or estimates.” *Id.*

Indeed, “[s]ince the enactment of Section 702, the Intelligence Community has stated that it cannot provide metrics to show the magnitude of incidentally collected U.S. person information.” *Id.* at 179-80. While PCLOB recommended in its previous 2014 report that “NSA publish several metrics to ‘provide insight about the extent to which the NSA acquires and utilizes’ incidental collection of U.S. person information under Section 702, the NSA has asserted that it is ‘infeasible’ to provide a meaningful estimate of the volume of this collection.” *2023 PCLOB Report*, at 180 (footnote omitted) (citation omitted).

C. *Section 702 Querying*

A Section 702 “query” refers to “the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized” under 50 U.S.C. §1881a(a). 50 U.S.C.

§1881a(f)(3)(B).²

A query “term” or “identifier” is like a search term used in an Internet search – “the term could be, for example, an email address, a telephone number, a key word or phrase, or a specific identifier that an agency has assigned to an acquired communication.” PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702*, (2014), at 55 (“2014 PCLOB Report”), available at <https://perma.cc/WD5R-5GKE>.

As this Court explained in *Hasbajrami I*, data collected via Section 702 interceptions “is frequently reviewed through queries, which identify communications that have particular characteristics specified in the query, such as containing a particular name or having been sent to or from a particular e-mail address.” *Hasbajrami I*, 945 F.3d at 657, citing *2014 PCLOB Report*, at 127.

As this Court noted, “Colloquially, the parties (and those engaged in policy debates about the program) have referred to this querying capability as ‘backdoor searches.’” *Id.* at 657. The NSA, CIA, and FBI’s Section 702 minimization procedures permit the agencies to query unminimized Section 702 collection.

At the time of the querying at issue herein, approximately from February

² While this statutory definition was not in effect at the time of the querying at issue herein, it nevertheless serves as an accurate definition of the term within the Section 702 context. *See generally Kris & Wilson* at 689.

2011 to September 2011, the operative statute, the FISA Amendments Act (“FAA”), discussed **post**, at 37, did not contain a separate provision mandating the submission of “querying procedures.”

FISA now does contain such a provision, at 50 U.S.C. §1881a(f), which was added as part of the 2017 FISA Amendment Reauthorization Act, enacted in response to concerns regarding the FBI’s Section 702-acquired data query practices involving U.S. person identifiers. *See generally*, David S. Kris, “Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond,” *Journal of Nat. Sec. L. & Policy*, 2016, at 398; *see also Post-Remand Memo* (ECF # 191), at 56, n.35.

The FBI’s querying of immense Section 702 database(s) is pervasive and routine, and extends beyond national security investigations. As a 2018 opinion issued by the FISC explained, the “2016 FBI Minimization Procedures require FBI personnel, to the extent reasonably feasible, to design queries of Section 702 data to find and extract foreign-intelligence information or evidence of crime.” *In re Foreign Intelligence Surveillance Court [Redacted]*, 402 F. Supp.3d 45, 80 (FISC 2018) (“2018 FISC Op.”), *citing*, 2016 FBI Minimization Procedures, §III.D, at 11.

According to those same 2016 FBI Minimization Procedures, it has been “a routine and encouraged practice for the FBI to query” 702 information in

furtherance of authorized intelligence and law-enforcement activities, including when “making an initial decision to open an assessment.” *Redacted*, 402 F. Supp. 3d 45, 80 (Foreign Intel. Surv. Ct. 2018), *aff’d in part sub nom. In re DNI/AG 702(h) Certifications 2018*, 941 F.3d 547 (Foreign Int. Surv. Ct. Rev. 2019) (“*2018 FISC Op.*”), *citing*, 2016 FBI Minimization Procedures, §III.D, at 11 n.3. *See also 2018 FISC Op.*, 402 F. Supp.3d at 78 (FBI policy promotes “maximal querying of Section 702 information”).

At the time of the querying at issue herein, the FBI did not track the number of queries using U.S. persons identifiers. *2014 PCLOB Report* at 59. However, the PCLOB reported that “the number of such queries . . . is substantial for two reasons.” *Id.*

The first was that the FBI, at the time, stored traditional FISA and Section 702 information in the same database, thus commingling data collected via warrant, but also via warrantless electronic surveillance. The second was that the FBI routinely queried data, including Section 702-acquired information, in the course of criminal investigations and assessments unrelated to national security. *2014 PCLOB Report*, at 59.

The 2017 FISA Reauthorization Act, with the addition of the querying procedures for the FBI at §1881a(f), now explicitly prohibits “queries of

information acquired under subsection (a) that are solely designed to find and extract evidence of criminal activity.” 50 U.S.C. §1881a(f)(2)(A).

Also, §1881a(f)(3) added the requirement that FBI personnel “must obtain prior approval from a Federal Bureau of Investigation supervisor . . . or attorney who is authorized to access unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) for any query of such unminimized contents or noncontents made using a United States query term.” 50 U.S.C. § 1881a(f)(3). Additionally, §1881a(f)(B) added a requirement that the FBI maintain records documenting U.S. person queries made on Section 702-acquired data.

While the 2017 FISA Reauthorization Act became effective in January 2018, certain lawmakers retained reservations regarding querying authority and procedures. For example, Congressman Danny Heck, a member of the Permanent Select Committee on Intelligence, published an Additional View in that Committee’s Senate Report cautioning that the 2017 FISA Amendments Reauthorization Act did not

adequately address law enforcement’s practice of querying the Section 702 database, through use of an American’s identifying information, without first obtaining judicial approval. Although courts have approved such queries, they nevertheless are, in my view, inconsistent with values we hold dear in the United States. Though [the 2017 FISA Amendments Reauthorization Act] contains reforms intended to

address law enforcement uses of Section 702 data, these may not protect Americans' privacy interests in an adequate way.

Permanent Select Committee on Intelligence Report on FISA Amendments Reauthorization Act of 2017, December 19, 2017, available at <https://www.congress.gov/committee-report/115th-congress/house-report/475/1>.

D. *The “Good Faith” Exception Does Not Apply to FISA’s Statutory Suppression Provisions*

1. *The District Court’s Opinion*

The District Court incorrectly held that because the Government “followed the minimization procedures approved by the FISA Court and in place at the time when querying Section 702-acquired information as to Defendant” the “good faith” exception should apply. *Hasbajrami II*, 2025 WL 447498, at *20.

The District Court based its finding on the belief that “agents running those queries at the time had objectively reasonable good-faith belief that those queries did not require a warrant [based upon] reasonable reliance on [. . .] FISC-approved procedures.” *Id.*, quoting *Davis v. United States*, 564 U.S. 229, 238 (2011) (quotation marks omitted).

The District Court also held that its finding that the querying herein violated the Fourth Amendment was not covered by FISA’s statutory suppression provision. *See Hasbajrami II*, 2025 WL 447498, at *21.

2. *FISA's Suppression Provision Incorporates Constitutional Violations*

FISA's statutory suppression remedy, set forth in 50 U.S.C. §1806(g), provides that if the Court “determines that the surveillance was not lawfully authorized or conducted, it *shall* . . . suppress the evidence which was unlawfully obtained or derived” from such surveillance. (Emphasis added). *See also* 50 U.S.C. §1806(e)(1) (whether “the information was unlawfully acquired”); 50 U.S.C. §1806(f) (whether electronic surveillance “was lawfully authorized and conducted”).

Contrary to the District Court's analysis, that provision incorporates Fourth Amendment violations as well as any technical, statutory procedural defects. The leading treatise on FISA, co-authored by David S. Kris, who occupied positions of authority within the Department of Justice (“DoJ”) regarding FISA for years, *see also Hasbajrami I*, 945 F.3d at 650-54, (citing Mr. Kris's treatise), confirms that “[t]his ground for suppression plainly includes constitutional challenges to FISA itself.” *Kris & Wilson*, at 32:3, 295-296.³

³ *Kris & Wilson* elaborates:

FISA's first ground on which an aggrieved person may move for suppression – that ‘the information was not lawfully acquired’ . . . plainly includes constitutional challenges to FISA itself, as well as constitutional

Thus, once a court finds querying unlawful, §1806(g) mandates suppression and the “good faith” exception is unavailable. *See also United States v. Giordano*, 416 U.S. 505, 524 (1974) (suppression required by statute “does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights”).

Indeed, the courts and Congress, when it passed FISA in 1978, have interpreted the language of “unlawful” and “not lawfully authorized or conducted” contained in 50 U.S.C. §§1806(e), (f), and (g) to encompass violations of the FISA statute itself as well as the Constitution, and in particular the Fourth Amendment.

For example, in *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991), the Court explained that “[w]hen a district court conducts a §1806(f) review, its task is not simply to decide whether the surveillance complied with FISA.”

Rather, §1806(f) “requires the court to decide whether the surveillance was ‘lawfully authorized and conducted.’” *Id.* In that context, the Court continued,

violations in the application process, such as a failure to show probable cause, the intentional or reckless inclusion of materially false information in the application, and the use of FISA to investigate ordinary criminal conduct rather than to gather foreign intelligence information.

Kris & Wilson, 32:3, at 295-296.

“*The Constitution is law.*” *Id.* Thus, “Once the Attorney General invokes §1806(f), the respondents named in that proceeding therefore must present not only their statutory but also their constitutional claims for decision.” *Id.*

The Ninth Circuit, following *ACLU Foundation*, interpreted §1806(f) the same way, holding it applicable when aggrieved persons challenge “the legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law.” *Fazaga v. Fed. Bureau of Investigation*, 965 F.3d 1015, 1052 (9th Cir. 2020), *rev’d and remanded on alternate grounds*, 595 U.S. 344 (2022) (§1806(f) did not replace the state secrets privilege).

In fact, the Court in *ACLU Foundation* added that “[a]lthough there will be no adversary hearing, we have held that the procedure mandated by §1806(f) is an acceptable means of *adjudicating the constitutional rights* of persons who have been subjected to FISA surveillance.” *ACLU Foundation*, 952 F.2d at 465 (emphasis added), *citing United States v. Belfield*, 692 F.2d 141, 148-49 (D.C.Cir.1982). *Accord United States v. Ott*, 827 F.2d 473, 476-77 (9th Cir.1987).

Similarly, in *United States v. Abu-Jihaad*, 531 F. Supp.2d 299 (D. Conn. 2008), *aff’d* 630 F.3d 102 (2d Cir. 2010), the Court, in denying defendant a “[*Franks v. Delaware*, 438 U.S. 154 (1978)] hearing in connection with FISA surveillance,” cited §1806(g) as the potential answer, observing that FISA

“provid[es] that the suppression remedy is to be applied ‘in accordance with the requirements of law.’” 531 F. Supp.2d at 311.

Likewise, in discussing the phrase “in accordance with the requirements of the law,” Congress, in the House of Representatives Report No. 95-1283, Part I (1978) (“*House Report*”), at 93, cited *Alderman v. United States*, 394 U.S. 65 (1969), which involved a *constitutional* violation (even before FISA existed).

Here, the District Court relied upon *United States v. Ning Wen*, 477 F.3d 896 (7th Cir. 2007), for the proposition that suppression under §1806(g) was not required because “the statutory standards for an intercept order have been satisfied.” A. 93; *Hasbajrami II*, 2025 WL 447498, at *21, quoting *Ning Wen*, 477 F.3d at 897.

That not only ignores §1806(g)’s inclusion of constitutional defects within its purview, but also misapplies *Ning Wen*, which, as a threshold matter, is distinguishable because that case, which involved the “good faith” exception defined in *United States v. Leon*, 468 U.S. 897 (1984), did not involve Section 702, but instead “traditional” FISA, see *Hasbajrami I*, 945 F.3d at 644, which requires an individualized warrant based upon probable cause. *Ning Wen*, 477 F.3d at 897.

As a result, in *Ning Wen* the Court pointed out

FISA requires each intercept to be authorized by a warrant from a federal district judge . . . [t]his brings into

play the rule of [*Leon*] that the exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that “no reasonably well trained officer [would] rely on the warrant.”

Ning Wen, 477 F.3d at 897.

That process – each intercept authorized by a warrant based on probable cause issued by a federal judge – is materially distinct from Section 702, which does not require an individualized warrant containing probable cause. *See Hasbajrami I*, 945 F.3d, at 650; *Hasbajrami II*, 2025 WL 447498, at *1 (A. 40).

Also, in *Ning Wen* the Court did not find *any* violation – either of FISA’s provisions or the Fourth Amendment. Consequently, the Court in *Ning Wen* was not distinguishing between constitutional and statutory remedies but simply holding that because neither the FISA statute nor the Fourth Amendment had been violated, suppression was not warranted under §1806(g). Thus, *Ning Wen* is inapposite.

Moreover, the binary construction of §1806(e) – mandating suppression if “(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval” – further establishes that FISA suppression encompasses constitutional violations as well as those confined

to statutory procedures.

Therefore, the District Court’s interpretation of “lawful” within §§1806(e), (f), and (g) as addressing *only* procedural flaws is inconsistent with the statutory text, which offers both (1) the inclusive “information was unlawfully acquired,” and (2) the specific “not made in conformity with an order of authorization or approval.” 50 U.S.C. § 1806(e). Non-compliance with FISC-approved procedures would fit within the second category.

The District Court’s interpretation – that both subsections pertain solely to conduct that did not comport with those procedures – would render §1806(e)(1) entirely superfluous. That view is foreclosed by the firmly established principle of statutory interpretation that every provision is to be given effect (*verba cum effectu sunt accipienda*). See *Kungys v. United States*, 485 U.S. 759, 778 (1998) (it is a “cardinal rule of statutory interpretation that no provision should be construed to be entirely redundant”); *United States v. Butler*, 297 U.S. 1, 65 (1936) (“These words cannot be meaningless, else they would not have been used”).

Moreover, §1806(f)’s language that statutory suppression under FISA applies to motions made “pursuant to any other statute or rule of the United States[,]” naturally includes the Fourth Amendment. See also James Kent, *Commentaries on American Law* 433 (1826) (“Several acts *in pari materia*, and

relating to the same subject, are to be taken together, and compared in the construction of them, because they are considered as having one object in view, and as acting upon one system”).

Nor does §1806(g)’s mandate, by using the term “shall,” afford a district court discretion. *See* Black’s Law Dictionary, (12th ed. 2024) (“shall” means “Has a duty to; more broadly, is required to. . . . This is the mandatory sense that drafters typically intend and that courts typically uphold”).

That meaning conforms with that applied repeatedly in the courts. *See, e.g., Norman v. United States*, 942 F.3d 1111, 1117 (Fed. Cir. 2019) (“use of the word ‘shall’ means what follows is mandatory, not discretionary”); *see also Hennepin Cnty. v. Fed. Nat. Mortg. Ass’n*, 742 F.3d 818, 822 (8th Cir. 2014); *LeMay v. U.S. Postal Serv.*, 450 F.3d 797, 799 (8th Cir. 2006); *Prokop v. Lower Loup Nat. Res. Dist.*, 302 Neb. 10, 27-28, 921 N.W.2d 375, 391 (2019) (“in statutory interpretation, ‘shall,’ as a general rule, is considered mandatory and inconsistent with the idea of discretion”).

Thus, once the District Court here concluded the querying was *not* conducted lawfully, §1806(g) required suppression.

The structure of Title III also provides an apt analogy to the circumstances herein regarding the immunity of a statutory remedy from the “good faith”

exception. The suppression mechanism therein, at 18 U.S.C. §2518, has generally been insulated from the “good faith” exception.

In fact, that language of 50 U.S.C. 1806(e) parallels that in Title III – which directs suppression if “the communication was unlawfully intercepted” and if “the interception was not made in conformity with the order of authorization or approval.” 18 U.S.C. §§2518(10)(a)(i)-(iii).

Applying that standard, in *United States v. Rice*, 478 F.3d 704 (6th Cir. 2007), the Sixth Circuit eschewed the “good faith” exception based on the existence of Title III’s statutory suppression mechanism, which is nearly identical to that of FISA, noting “[t]he language and legislative history of Title III strongly militate against engrafting the good-faith exception into Title III warrants.” *Id.* at 712.

The Court in *Rice* cited “the language in Title III[,]” which “provides that exclusion is the exclusive remedy for an illegally obtained warrant.” The Court added that “[i]n contrast to the law governing probable cause under the Fourth Amendment, the law governing electronic surveillance via wiretap is codified in a comprehensive statutory scheme providing explicit requirements, procedures, and protections.” *Id.*

That is precisely the case with FISA – a “comprehensive statutory scheme

with explicit” provisions – as well. Also, in *United States v. McGuinness*, 764 F. Supp. 888 (S.D.N.Y. 1991), the Court rejected the government’s argument that the Court should apply *Leon* to a Title III wiretap case, noting that “[i]t is doubtful, [] whether the *Leon* exception applies to wiretaps, since the exclusionary rule for wiretaps is explicitly commanded by statute, 18 U.S.C. §2518(10)(a), while the exclusionary rule for ordinary searches is a judicial gloss on the Fourth Amendment’s general prohibition of unreasonable searches.” *McGuinness*, 764 F. Supp. at 897 n.2.

Similarly in *United States v. Orozco*, 630 F. Supp. 1418, 1522 (S.D. Cal. 1986) (footnote omitted), the District Court reasoned that “[a]lthough courts have suppressed seizures of wire and oral communications by applying traditional fourth amendment and exclusionary rule analysis, Congress has chosen to supplement the judicially fashioned exclusionary rule with a statutory remedy for unreasonable electronic surveillance.”

The Court in *Orozco* added that, “Congress has not in the wake of the *Leon* decision attempted to modify this remedy. Nor does the *Leon* decision suggest that the Supreme Court would attempt to create an exception to a statutorily-imposed remedy.” *Id.* Again, Congress’s inaction after *Leon* applies to FISA and §§1806(e), (f) & (g) with equal force.

Accordingly, the statutory language (and canons of construction), as well as the courts that have addressed the issue, and the leading treatise on FISA, all concur that §1806(g), in conjunction with §§1806(e) & (f), includes constitutional violations within its suppression mandate, and that District Court was required to order suppression once it concluded the querying in this case was unlawful.

E. *The “Good Faith” Exception Should Not Apply to the Circumstances Present Herein*

Even assuming the “good faith” exception did apply herein, it would not rescue the querying in this case. As discussed below, the “good faith” exception should be rejected in this case for a number of reasons that can be divided among three categories: (1) the government’s conduct in this case; (2) the persistent and serious non-compliance that has infected the Section 702 program throughout its existence; and (3) the extensive history of material non-compliance with respect to implementation of FISA generally.

1. *The Principles Guiding Application of the “Good Faith” Exception*

As this Court has explained, “It is the Government’s burden – not [the defendant’s] – to demonstrate the objective reasonableness of the officers’ good faith reliance” on binding appellate precedent. *United States v. Ganius*, 755 F.3d 125, 140 (2d Cir. 2014), *rev’d on other grounds*, 824 F.3d 199 (2d Cir. 2016) (*en banc*), *citing United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012).

In assessing the applicability of the “good faith” exception, a court must conduct an objective inquiry. In *United States v. Lyles*, 910 F.3d 787 (4th Cir. 2018) the Fourth Circuit, in refusing to find “good faith,” stated “*Leon’s* standard is ultimately an ‘objective’ one” disclaiming any intent to “impugn[] the subjective good faith of the officer who ran the warrant application through [multiple layers of] review . . .” *Id.* at 797.

The rationale for the exclusionary rule has varied since the doctrine was established in *Weeks v. United States*, 232 U.S. 383 (1914), and today courts often formulate the exclusionary rule as a balancing test: “The deterrence theory of the exclusionary rule, which now holds sway, requires us, before suppressing evidence in a particular proceeding, to balance the deterrent effect of applying the exclusionary rule against the cost to society of excluding relevant information.” *United States v. Varela*, 968 F.2d 259, 260 (2d Cir. 1992).⁴

⁴ In the context of broad electronic searches, the Supreme Court has expressly held that a court must consider even those aspects of the intrusion that do not lead to evidence at trial. *See Scott v. United States*, 436 U.S. 128, 142-43 (1978), (weighing, as part of its Fourth Amendment analysis, the government’s interception of seven phone calls between the defendant and her mother – notwithstanding that “none of these conversations turned out to be material to the investigation at hand”). *See also Berger v. New York*, 388 U.S. 41, 55, 58-60 (1967); *United States v. Hyde*, 574 F.2d 856, 870 (5th Cir. 1978) (analyzing interception of privileged communications that did not produce evidence of conspiracy); *United States v. DePalma*, 461 F.Supp. 800, 822 (S.D.N.Y. 1978) (same).

Also, “The basic insight of the *Leon* line of cases is that the deterrence benefits of exclusion by exclusion ‘var[y] with the culpability of the law enforcement conduct’ at issue.” *Davis*, 564 U.S. at 238, quoting *Herring v. United States*, 555 U.S., 135, 143 (2009).

In *Herring*, the Court also reiterated that the “good faith” analysis should include an evaluation of the totality of institutional conduct, and not be confined simply to the narrow circumstances of the specific search or seizure at issue:

As laid out in our cases, the exclusionary rule serves to deter *deliberate, reckless, or grossly negligent conduct*, or in some circumstances *recurring or systemic negligence*.

Herring, 555 U.S. at 144 (emphasis added).

2. *The Government’s Conduct in This Case Alone Should Deprive It of Resort to the “Good Faith” Exception*

Here, the government cannot satisfy its burden. Indeed, the government’s claims of “good faith” ignore Judge Gleeson’s blunt characterization of the government’s misrepresentations in this very case that required Hasbajrami’s initial guilty plea to be vacated. *See ante*, at 5-6.

Judge Gleeson elaborated that there existed “a DOJ policy that transcended this case” and was designed deliberately to fail to provide notice of warrantless Section 702 surveillance. Order, October 2, 2014 (ECF #85), at 6. That defines

bad faith, as the only plausible rationale for such concealment was to prevent courts from adjudicating challenges by defendants to Section 702 surveillance because DOJ itself had serious doubts about the constitutionality of the indiscriminate querying process. Nor did the government's excuse persuade Judge Gleeson, either.

Further proof is that here the government stood silently while Hasbajrami entered a guilty plea that was neither knowing nor intelligent, and, rather than acknowledge Section 702's role in this case, watched him be sentenced to 15 years' imprisonment as a result.

Even during the initial appeal in this case, as this Court pointed out more than once, "At oral argument, the government was unable to represent whether or not identifiers related to Hasbajrami had been used in querying previously-acquired Section 702 surveillance databases." *Hasbajrami I*, 945 F.3d at 660.

As a result, this Court "ordered the government to 'identify[] the record evidence that supports the proposed factual inference that it conducted no queries or backdoor searches of Section 702 material with regard to Hasbajrami before or leading to the FISC's issuance of Title I and Title III warrants with respect to Hasbajrami.'" *Id.*, quoting Order, *United States v. Hasbajrami*, Nos. 15-2684, 17-2669 (2d Cir. Sept. 4, 2018) (ECF # 203); see also *id.* at 646 ("no information

about any queries conducted as to Hasbajrami was provided to the district court, and the information provided to us on this subject is too sparse to reach a conclusion as to the reasonableness of any such queries conducted as to Hasbajrami”).

Indeed, the government’s position has been elusive. At oral argument before this Court, the government, rather than directly answer this Court’s question about queries in this case, instead – and in a departure from its prior briefing – claimed for the first time that this is “not a criminal case” that “arose from” a backdoor search. Oral Argument at 45:20, *United States v. Hasbajrami*, Docket Nos. 15-2684, 17-2669 (2d Cir. Aug. 27, 2018), available at <https://bit.ly/3ywLeGK>.⁵

The government also made a new set of assertions at oral argument regarding whether its exploitation of Hasbajrami’s emails occurred in “real-time.” Oral Argument at 58:52. Those claims, too, were rife with ambiguity. While the government asserted, at 59:00, “[t]his case involved very, very focused attention by the U.S. government in real time or close to real time on the *communications of foreign persons* who were involved in international terrorism” (emphasis added),

⁵ During oral argument, at 50:50 the government was extremely cagey in its responses, avoiding answering directly this Court’s questions regarding backdoor searches, and instead repeating either that (a) the “criminal case” was not the product of a backdoor search; and/or (b) the record did not disclose whether there was a backdoor search. The government conceded ambiguity with respect to the

with respect to its review of *Hasbajrami's* communications, the government equivocated, “perhaps it’s not fair to ask you to draw the inference that it was real-time or close to real-time.”

Nor did even this Court’s post-argument September 4, 2018, Order noted above yield a definitive answer from the government about backdoor searches of Hasbajrami’s communications. In fact, this Court’s dissatisfaction with the nature and extent of the government’s (even *ex parte*) disclosures was a refrain throughout *Hasbajrami I*:

Because the district court was not even aware whether such querying had occurred, and *because even we have not been advised as to what was done, for what reasons, and with what results*, we remand to the district court to determine the facts, consistent with the considerations stated above, and to decide in the first instance, based on its factual findings, whether there was a constitutional violation in this particular case, and what (if any) evidence would need to be suppressed if there was indeed a violation.

Hasbajrami I, 945 F.3d at 673 (emphasis added).

The government’s resistance to providing a complete account continued upon remand, as the District Court observed:

The Government describes dozens of queries run against an unknown number of communications collected from Defendant. [Redacted] Unfortunately that is the extent of

record, which precipitated this Court’s post-argument Order (ECF # 203).

the information provided by the Government with respect to the querying in this case. The Government largely fails to identify specific query terms, specific results of querying, or the underlying contents of the underlying communications subject to querying [Redacted][.]

A. 87; *Hasbajrami II*, 2025 WL 447498, at *18.

As a result, the government “merely provided [Redacted] that purport to reconstruct the record without any supporting evidence” and “[t]he Government’s opposition is rife with similarly vague and unsupported notions.” *Id.*

The District Court recognized the irony of the “sparse record” the government provided, considering a lack of information on appeal generated this Court’s remand in the first place. *Id.* (quotation marks omitted). Thus, sharing this Court’s frustration, the District Court stated, “again [the Court was] left with an incomplete record, from which the Government asks this Court to infer that the querying here was ‘reasonable.’” *Id.*

3. *The Systemic, Historical Non-Compliance That Has Plagued Section 702’s Querying Process – Including During the Period at Issue Herein – Further Vitiates Any Claim of “Good Faith”*

a. *Section 702 Was Initiated as an Illegal Warrantless Program*

Even Section 702’s origin story is antithetical to any concept of “good faith.” Commenced secretly as a warrantless surveillance program that was both expansive and technologically advanced, it collected electronic communications by

both U.S. persons and non-U.S. persons.

Initially, the surveillance and interception, denominated the Terrorist Surveillance Program (“TSP”), was performed without any legislative or court authorization. *See* James Risen & Eric Lichtblau, “Bush Let U.S. Spy on Callers Without Courts,” *The New York Times*, Dec. 16, 2005, available at <https://nyti.ms/3yyKr8c>. *See also* Karen Greenberg, *ROGUE JUSTICE* (2016), at 113-16 (chronicling the transfer of the program’s approval from DoJ to the White House because of DoJ’s objections).

Thus, “in 2001, the NSA [] began acquiring Internet-based communications of overseas targets without the use of a traditional law enforcement warrant or an electronic surveillance order under Title I of FISA.” Edward C. Liu, Andrew Nolan, Richard M. Thompson II, CONG. RESEARCH SERV., R43459, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES AND RECENT DEVELOPMENTS 9 (footnote omitted) (April 1, 2014), available at <https://bit.ly/3F2to0Z> (hereinafter “*CRS Report: Overview*”), *citing*, Dec. 20, 2013, Unclassified Declaration of Frances J. Flesch, National Security Agency, in *Schubert v. Obama*, 07 Civ. 693 (JSW) (N.D.Cal.), at ¶ 32, available at <https://bit.ly/327AQJJ>.

After the TSP’s existence was disclosed in December 2005 in *The New York*

Times, “[u]ltimately, new statutory authority for this type of acquisition was provided, at first, temporarily under the Protect America Act (‘PAA’) of 2007 [P.L. 110-55; 110-55; 121 Stat. 552 (2007)], and on a longer term basis by the [FAA, P.L. 110-261; 122 Stat. 2436 (2008)].” *CRS Report: Overview*, at 10 (footnotes omitted).

Following the FAA’s passage, PAA collection activities transitioned to the newly-minted Section 702 of FISA. While the FAA was enacted in 2008, for seven years prior to its passage NSA had been conducting (at least) the very same electronic surveillance and interception ultimately authorized by the FAA.

b. *The Extraordinary Scope of Section 702 Interception and Retention*

After passage and implementation of the PAA and subsequently the FAA, the Government began using the new, warrantless surveillance regime instead of “traditional” FISA surveillance, predicated on Court-determined probable cause. That change was reflected in the data: a 40% decrease in the total number of “traditional” FISA electronic surveillance applications. *Compare* 2007 ANNUAL FISA REPORT (2,371 Title I FISA applications in 2007), available at <http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf> *with* 2009 ANNUAL FISA REPORT (1,329 Title I FISA applications in 2009), available at <http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf>.

The extent to which Section 702 has swallowed the rest of FISA (and particularly “traditional” FISA, is even more apparent from the more recent data:

In 2021, the most recent year for which data is available, there were more than 230,000 foreign targets of Section 702 warrantless surveillance. By contrast, the government obtained FISA court orders to eavesdrop on about 300 Americans or noncitizens on domestic soil.

Charlie Savage, “Security Agencies and Congress Brace for Fight Over Expiring Surveillance Law,” *The New York Times*, February 27, 2023, available at <https://nyti.ms/3myME26>. See also Elizabeth Goitein, “The Year of Section 702 Reform, Part I: Backdoor Searches,” *Just Security*, February 13, 2023, at 1, available at bit.ly/3AeQqRD (“a series of recent government reports and FISA Court opinions have demonstrated that Section 702 has become a go-to domestic spying tool for the FBI, and that FBI agents are routinely violating statutory and court-ordered limits on accessing Americans' data ‘incidentally’ collected under Section 702”).

The result, of course, has been a dramatic reduction in judicial oversight of foreign intelligence electronic surveillance of both non-U.S. persons *and* U.S. persons “incidentally” intercepted via the Section 702 program. Yet, in *In re Directives [redacted]*, 551 F.3d 1004 (FISCR 2008), the Foreign Intelligence Court of Review (“FISCR”), had reported that the “[g]overnment assures us that it

does not maintain a database of incidentally collected information from non-targeted United States persons.” *Id.* at 1015.

The monumental scope of the Section 702 collection, both at the time of the querying in question here, and in the intervening years continuing through today, is staggering. In a 2011 FISC opinion, Judge Bates wrote that the NSA had informed him that it collected, “more than 250 million Internet communications” per year via the FAA. *In re Foreign Intelligence Surveillance Court (Redacted)*, 2011 WL 10945618, at *30-31 (FISC 2011) (“2011 FISC Op.”). *See also Hasbajrami I*, 945 F.3d at 671 (“the vast technological capabilities of the Section 702 program, estimated by the PCLOB as totaling nearly 250 million e-mails annually by 2011 and likely larger numbers since then”), *citing 2011 FISC Op.*, 2011 WL 10945618, at *9, 25; *2014 PCLOB Report*, at 116 (“current number [of internet communications intercepted pursuant to Section 702] is significantly higher [as of 2014]”).

The Office of the Director of National Intelligence’s Office of Civil Liberties, Privacy, and Transparency *Annual Statistical Transparency Report Regarding the Intelligence Community’s Use of National Security Surveillance Authorities, Calendar Year 2020*, at 16 (April 2021) (“ODNI 2020 Transparency Report”), available at <https://bit.ly/33AdOfb> (and mandated by the USA

FREEDOM Act of 2015), disclosed that the number of Section 702 “targets” totaled 164,770 in 2018, and increased essentially 25% in 2019 to 204,968.

ODNI’s 2020 Transparency Report, while noting that “the frequency with which FBI uses U.S. person query terms is greater than other agencies[,]” also documents an astounding increase in the number of estimated FBI queries of U.S. persons’ “unminimized Section 702-acquired contents and noncontents for foreign intelligence information and/or evidence of a crime” in 2021: from fewer than 1,324,057 from December 2019 through November 2020 to 3,394,053 from December 2020 through November 2021. *Id.*, at 21.

c. *Section 702’s Unremitting History of Non-Compliance*

Application of the “good faith” exception here would also be wholly inappropriate in light of the unremitting non-compliance that has characterized implementation of Section 702 and its querying process for as long as relevant data and information have been available.⁶

⁶ Except for one opinion, FISC decisions were not publicly available until after Edward Snowden’s disclosures in 2013 regarding clandestine electronic surveillance programs. Afterward, in part to explain the nature of the FISC’s role in those programs, and in part as a commitment to more transparency, the FISC began declassifying certain earlier opinions, and going forward published a declassified version of its annual opinions regarding the Section 702 program renewals. *See* <https://www.fisc.uscourts.gov/docket/declassified-opinions>. FISC opinions are not published publicly contemporaneously, but instead are subject to a lengthy declassification process. Thus, FISC opinions are usually made public at

The catalogue below represents just a fraction of the actual record of misuse of FISA-acquired data, both because this motion is limited by space constraints, and because the public record itself is limited to what has been released by the government and FISC, through its declassified decisions, and reports by entities such as the PCLOB (since 2014) and the Office of the Director of National Intelligence (“ODNI”).

i. *The 2011 FISC Opinion*

The persistent problems with Section 702 were recognized in the earliest published FISC opinion regarding the program in 2011 – the time period of the querying in this case. *See 2011 FISC Op.*, 2011 WL 10945618, at *9, 25.

In the *2011 FISC Op.*, Judge Bates, Chief Judge of the FISC at the time, excoriated NSA for exceeding its acquisition authority and making repeated misrepresentations to the FISC regarding NSA’s activities. As described in the *CRS Report: Overview*, Judge Bates was evaluating “the targeting and minimization procedures proposed by the government to address new information regarding the scope of upstream collection.” *CRS Report: Overview*, at 13 (footnotes omitted).

The *CRS Report: Overview* continued that “[s]pecifically, the government

least a year after they are issued in classified form (to the government).

had recently discovered that its upstream collection activities had acquired unrelated international communications as well as wholly domestic communications due to technological limitations.” *Id.* (footnotes omitted). In response, Judge Bates “found the proposed minimization procedures to be deficient on statutory and constitutional grounds.” *Id.* (footnotes omitted).

According to the *CRS Report: Overview*,

With respect to the statutory requirements, the FISC noted that the government’s proposed minimization procedures were focused “almost exclusively” on information that an analyst wished to use and not on the larger set of information that had been acquired. Consequently, communications that were known to be unrelated to a target, including those that were potentially wholly domestic, could be retained for up to five years so long as the government was not seeking to use that information.

Id. (footnote omitted).

The *CRS Report: Overview* noted that Judge Bates concluded that “this had the effect of maximizing the retention of such information, and was not consistent with FISA’s mandate to minimize the retention of U.S. person information.” *Id.* (footnote omitted). In his opinion, Judge Bates also noted the pervasive nature of the violations.

For example, Judge Bates stated “The court is troubled that the government’s revelations regarding NSA’s acquisition of Internet transactions

mark *the third instance in less than three years* in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.” *Id.*, at *5, n.14 (emphasis added).

Judge Bates further noted that the government’s submissions in that proceeding made it clear that the NSA had been acquiring Internet transactions even before the FISC’s first approval thereof. *Id.* at *17 n.45.

ii. *The 2014 PCLOB Report*

Operating parallel to the FISC, the PCLOB, established after Edward Snowden’s disclosures, *see ante*, at n. 6, issued its first report in 2014. The *2014 PCLOB Report* found that “certain aspects of the Section 702 program push the entire program close to the line of constitutional reasonableness,” including “the use of queries to search the information collected under the program for the communications of specific U.S. persons.” *2014 PCLOB Report*, at 88.

In 2015, the PCLOB released an additional set of recommendations which identified key deficiencies in the use of Section 702-acquired data by both FBI and NSA. PCLOB, *Recommendations Assessment Report*, January 29, 2015, (“*2015 PCLOB Recommendations*”), available at <https://bit.ly/4eO87eb>.

The PCLOB found that there existed a significant gap between the “actual practice” of the FBI in querying Section 702-acquired data, and the minimization

procedures that the FBI used to undertake queries. The PCLOB wrote:

Even though FBI analysts and agents who solely work on non-foreign intelligence crimes are not required to conduct queries of databases containing Section 702 data, they are permitted to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI's minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices.

2015 PCLOB Recommendations, at 18.⁷

Although the PCLOB noted that the FBI planned to implement the recommendations, it would take nearly a decade of continued abuse of the Section 702 program, and law enforcement resistance to both the PCLOB and FISC, as discussed **post**, at 44-60, as well as a statutory change in Section 702, before the FBI implemented the changes.

iii. *The 2017 FISC Opinion*

Indeed, despite Judge Bates's iteration of the defects in the Section 702 program's acquisition and minimization protocols, the FISC's annual opinions

⁷ As the PCLOB noted in its *2015 PCLOB Recommendations*, "The FBI's minimization procedures should be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations." *2015 PCLOB Recommendations*, at 18.

authorizing renewal/revision of Section 702 protocols have been compelled to recite a litany of continuing material violations specifically in the context of Section 702 database querying.

For example, in its 2017 opinion, the FISC observed that “NSA examined all queries using identifiers for ‘U.S. persons targeted pursuant to Sections 704 and 705(b) using the [redacted] tool in [redacted] . . . from November 1, 2015 to May 1, 2016[,]” and “[b]ased on that examination, ‘NSA estimates that approximately eighty-five percent of those queries, representing [redacted] queries conducted by approximately [redacted] targeted offices, were not compliant with the applicable minimization procedures.’ [Redacted], Mem. Op. (FISC April 26, 2017) (“2017 FISC Op.”), available at <https://bit.ly/3qcjsf6> (citations omitted) (footnote omitted).

In addition, the 2017 FISC Op. reported that at an October 26, 2016, hearing “the Court ascribed the government’s failure to disclose [certain internal] reviews at the October 4, 2016 hearing to an institutional ‘lack of candor’ on NSA’s part and emphasized that ‘this is a very serious Fourth Amendment issue.’ October 26, 2016 Transcript at 5-6.” 2017 FISC Op. at 19-20.

As a result, “The Court found that, in light of the recent revelations, it did not have sufficient information to assess whether the proposed minimization

procedures accompanying the Initial 2016 Certifications would comply with statutory and Fourth Amendment requirements, as implemented.” *Id.*

iv. *The 2018 FISC Opinion*

The following year, the FISC’s 2018 opinion documented that “the FBI has conducted tens of thousands of unjustified queries of Section 702 data.” In fact, the FISC reiterated that (as cited earlier in its opinion), “the FBI has conducted tens of thousands of unjustified queries of Section 702 data[,]” and “[b]ased on the information available – e.g., queries for [redacted] and for persons with access to FBI facilities – it appears that many subjects of those queries were U.S. persons.” *2018 FISC Op.*, 402 F. Supp.3d at 87.

While the FISC found it “difficult on the record before [it] to assess to what extent U.S.-person information was returned and examined as a result of those queries[,]” at the very least “*the reported querying practices present a serious risk of unwarranted intrusion into the private communications of a large number of U.S. persons.*” *Id.* (emphasis added).

The *2018 FISC Op.* further explained that a single search could have expansively abusive results: “In a number of cases, a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including U.S. persons.” *Id.* at 76. The opinion also expressed serious

reservations that the intentionally unauthorized queries “do not present the same level of concern as those that evidence misunderstanding of the querying standard.” *Id.* at 78.

In addition, due to the FBI’s failure to adhere to the statutory standard for documentation, for use in audits of the agency’s use of the program, the FISC was not even able to identify with confidence the level of non-compliance. *Id.* See also *Muhtorov*, 20 F.4th 558 at 677 (10th Cir. 2021) (Lucero, J., *dissenting*) (noting the “FBI’s documented history of widespread U.S. person querying and of non-compliance with its record-keeping responsibilities under its own minimization procedures”), *citing 2014 PCLOB Report*, at 59.

That deliberate lack of transparency rendered the FISC unable to identify whether the FBI was conducting U.S. person queries, or non-U.S. person queries, a difference critical to any Fourth Amendment inquiry.

The *2018 FISC Op.* disclosed further purposeful defects in documentation that shield FBI’s querying practices – and their Fourth Amendment implications – from FISC and Congressional examination. For instance,

[t]he querying procedures did not require FBI personnel to document the basis for finding that each United States-person query satisfied the relevant standard – *i.e.*, that queries be reasonably designed to return foreign-intelligence information or evidence of a crime.

2018 FISC Op., at 52.

The *2018 FISC Op.* further admonished the FBI for its hesitancy to adopt more stringent procedures consistent with FISA's requirements, finding, "Regardless of how persuasive the FBI's considerations may be, the Court is not free to substitute its understanding of sound policy – or, for that matter, the understanding of the Director of the FBI – for the clear command of the statute." *Id.*, at 72, citing *14 Penn Plaza LLC v. Pyett*, 556 U.S. 247, 270 (2009) ("[a]bsent a constitutional barrier, 'it is not for us to substitute our view of . . . policy for the legislation which has been passed by Congress'") (other citations omitted).

The *2018 FISC Op.* also highlighted other deficient aspects of the FBI's use of Section 702-acquired data, finding that querying did not require any documentation regarding individual suspicion, require any higher-level approval, institute any restrictions on the use of the resulting information returned from the queries, or institute any requirement that irrelevant information be promptly destroyed. *See 2018 FISC Op.*, at 73-80.

As the *2018 FISC Op.* recognized, "Without such documentation and in view of reported instances of non-compliance with that standard, the procedures seemed unreasonable under FISA's definition of 'minimization procedures' and possibly the Fourth Amendment." *Id.* at 52.

In reaching this determination about the insufficiency of the FBI's procedures, the FISC explained

Because the FBI procedures, as implemented, have involved a large number of unjustified queries conducted to retrieve information about U.S. persons, they are not reasonably designed, in light of the purpose and technique of Section 702 acquisitions, to minimize the retention and prohibit the dissemination of private U.S. person information.

Id. at 82.

Ultimately, the FISC concluded that FBI's permissive rules for searching through U.S. persons' communications rendered the querying protocols unreasonable under the statute and the Fourth Amendment. *See 2018 FISC Op.*, at 86-88. The *2018 FISC Op.* also concluded that "[t]here are demonstrated risks of *serious error and abuse*, and the Court has found the government's procedures do not sufficiently guard against that risk." *Id.*, at 88 (emphasis added).

v. *The Government's Appeal of the 2018 FISC Op.*

The government appealed the FISC's 2018 decision(s), and in 2019, the FISCR released an opinion, *In Re: DNI/AG 702(h) Certifications 2018*, 941 F.3d 547 (Foreign Int. Surv. Ct. Rev. 2019) ("*2019 FISCR Op.*"), that addressed (1) whether the FBI would be required to keep a record of each United States person query term, and (2) whether the FBI's proposed 2018 querying and minimization

procedures complied with the requirements of FISA and the Fourth Amendment. *Id.*, at 549.

The FISCR affirmed the FISC’s 2018 decisions in part, finding that the FBI’s proposed procedures did *not* comply with Section 702(f)(1)(B) because they did not “include a procedure whereby FBI personnel document . . . whether a particular query term related to a United States person,” and declining to address the second, more general issue, until the FBI submitted revised procedures. *2019 FISCR Op.*, 941 F.3d at 549.

The FISCR opinion detailed the FBI’s blatant disregard for the statutory changes made to FISA in the 2017 FISA Amendments Reauthorization Act, namely Section 702(f)(1)(B), which requires that “a record [be] kept of each United States person query term” (codified at 50 U.S.C. §1881a(f)(1)(B)), and of which the FISC became aware because the FBI submitted querying procedures to the FISC that appeared to ignore this statutory requirement “adhering to its prior practice of keeping a record of all query terms used to query Section 702 information without differentiating between query terms that related to a United States person and those that do not.” *Id.* at 16.

The FISCR also detailed in its opinion how, after the FISC rejected the FBI’s procedures and requested resubmission, the FBI resubmitted amended

certifications but left that key portion – relating to documenting U.S. person query terms – *unchanged*. *Id.* at 555.

As a result, the FISCR again rejected the procedures because U.S. person queries were not separately documented, and, although the FBI’s proposed procedures were consistent with applicable requirements, “the FBI had not implemented similar existing procedures consistently with those requirements—and, presumably, that it could be expected to implement the proposed procedures in a *similarly deficient manner*.” *Id.* at 20 (emphasis added). Yet, as the FISCR pointed out, rather than “implement the corrective measure the FISC proposed,” the FBI had appealed. *Id.* at 21.

vi. *The 2019 FISC Opinion*

The FISC opinion for 2019 included another example of the FBI’s refusal to admit error, and instead to make transparently spurious arguments to the FISC. A query had enabled access to “unminimized Section 702 information using the identifiers for approximately 16,000 persons.” *[Redacted]*, *Mem. Op.*, (FISC Dec. 6, 2019) (“*2019 FISC Op.*”), available at <https://bit.ly/44u2w9j>.

As the *2019 FISC Op.* continued, “[b]ased on the facts reported, the FBI’s position that the queries for all 16,000 persons were reasonably likely to retrieve foreign-intelligence information or evidence of a crime is unsupportable.” *Id.*; *see*

also id. at 68 (“[t]here is no relevant distinction between [Redacted] queries and other broad, suspicionless queries previously identified by the government and the Court as violations of the querying standard”), *citing*, *2018 FISC Op.*, 402 F.Supp.3d at 75-77.

The *2019 FISC Op.*, like its predecessors, also described how the FBI frequently violated its own rules and protocols with respect to Section 702, and how the FBI’s systems were designed in ways that continued to multiply, rather than diminish, the intrusions on U.S. persons’ communications. *Id.* at 67-70, 81.

vii. *The 2020 FISC Opinion*

In 2020, the FISC delivered another opinion, which listed specific instances of FISA violations, including 69 improper queries by a terrorism task-force officer, [Redacted], *Mem. Op.*, (FISA Ct. Nov. 18, 2020) (“*2020 FISC Op.*”), at 40, available at <https://bit.ly/3Fp1cW2>, as well as “[o]ther reported violations [that] apparently resulted from the failure of FBI personnel to opt out of querying raw FISA-acquired information[,]” *id.*, “as well as conducting overly broad queries.” *Id.*, at 41.

In addition, the Court found “that the FBI’s failure to properly apply its querying standard . . . was more pervasive than was previously believed,” although it noted that most of those queries “occurred prior to the implementation of the

FBI's system changes and training" regarding the documentation requirement. *Id.* at 39, 41.

viii. *The 2022 FISC Opinion*

The FISC released its April 21, 2022, opinion in May 2023. *See Memorandum Opinion and Order [Redacted]*, (FISC April 21, 2022) ("*2022 FISC Op.*"), available at <https://bit.ly/40QZ5XO>. That opinion addressed the ongoing non-compliance issues that afflict the FBI's implementation of the Section 702 program. *See id.*, at 7 ("compliance issues have continued to surface").

For instance, the FISC noted "The FBI Querying Procedures include new provisions adopted to address a pattern of broad, suspicionless queries that are not reasonably likely to retrieve foreign intelligence information or evidence of crime." *Id.* at 22-23.

The FISC further found that FBI agents "ran a batch query of unminimized FISA information in June 2020, using identifiers of 133 individuals arrested "in connection with civil unrest and protests between approximately May 30, and June 18, 2020." *Id.* at 27.

The civil unrest and protests referred to were the Black Lives Matter and Defund The Police protest movements. *See generally* Mathis Ebbinghaus, Nathan Bailey, Jacob Rubel, *The Effect of the 2020 Black Lives Matter Protests on Police*

Budgets: How “Defund the Police” Sparked Political Backlash, Social Problems, 2024, available at <https://academic.oup.com/socpro/advance-article/doi/10.1093/socpro/spae004/7630127>.

The DoJ’s National Security Division (“NSD”) subsequently notified the FISC that it had later “assessed that the queries were not reasonably likely to retrieve foreign intelligence information or evidence of a crime.” *2022 FISC Op.*, at 27 (citation omitted).

Notwithstanding that conclusion rendered by the DoJ lawyers assigned the responsibility of administering FISA, including Section 702, the FBI “maintained that there was a ‘reasonable basis to believe these queries would return foreign intelligence because [redacted] information, not relied upon by the person who ran the queries, that suggested that [redacted] of a foreign power [redacted] a message on behalf of [redacted] organization ‘protesting’ U.S. [redacted] violence against African-Americans to various U.S. persons.” *Id.*

In that same *2022 FISC Op.*, the FISC noted that since it had issued a Querying Violations Order, “the government has reported additional, significant violations of the querying standard, including several relating to the January 6, 2021 breach of the U.S. Capitol.” *Id.* at 28.

For example, one analyst

ran 13 queries of individuals suspected of involvement in the January 6, 2021 Capitol breach. The analyst said she ran the queries to determine whether these individuals had foreign ties, and indicated she had run “thousands of names within in the FBI systems in relation to the Capitol breach investigations.”

Id.

Regarding these queries, too, NSD “concluded the queries were not reasonably likely to retrieve foreign intelligence information or evidence of a crime.” *Id.*; *see also id.*, at 29 (NSD “assessed” that “360 queries in connection with domestic drug and gang investigations, domestic terrorism investigations, and the Capito] breach. [REDACTED]” that “provided no information to support a reasonable basis to believe foreign intelligence information or evidence of a crime would likely be returned[,] . . . did not meet the querying standard”) (citation omitted).

In addition, an analyst “conducted a batch query for over 19,000 donors to a congressional campaign. The analyst who ran the query advised that the campaign was a target of foreign influence, but NSD determined that only eight identifiers used in the query had sufficient ties to foreign influence activities to comply with the querying standard.” *Id.* at 29.

According to the *2022 FISC Op.*, in May 2021 the FBI’s Office of Internal Auditing (“OIA”) conducted an enterprise-wide audit and uncovered further

querying violations. OIA's audit looked at more than 2,000 queries between April 1, 2020, and March 31, 2021. NSD, in reviewing the OIA's findings, concluded that 286 queries were non-compliant. *Id.* at 30.

These queries included persons associated with the above-mentioned civil unrest and protests of 2020 as well as the January 6, 2021 Capitol breach. *Id.* at 31. Based on this audit and NSD's subsequent analysis, "the government reported in excess of 278,000 non-compliant FBI queries of raw FISA-acquired information." *Id.*

Included among them were "467 queries of the names and identifiers of cleared defense contractors [redacted][.]" *Id.* at 32. Again, "NSD determined these queries were not reasonably likely to return foreign intelligence information or evidence of a crime because there was no specific information indicating that the named companies were being targeted by foreign adversaries." *Id.* at 32.

In its 2022 opinion, the FISC found "Across the FBI, the government has reported queries of raw FISA-acquired information as 'part of routine baseline checks to determine whether there was any information regarding the subject [of the query] in FBI holdings,' without a specific factual basis to believe the query was reasonably likely to return foreign intelligence information or evidence of a crime." *Id.* at 33.

Further, the FISC found instances of violations of Section 702(f)(2), which requires that the FBI obtain a court order before accessing the content of communications when the query is “solely designed to find and extract evidence of criminal activity.” *Id.* at 33; 50 U.S.C. §1881a(f)(2).

In one instance, “the FBI queried unminimized Section 702-acquired information using the name of someone then believed to have been present at the breaching of the Capitol and who was the subject of an open predicated criminal investigation relating to that event.” *2022 FISC Op.*, at 33.

Regarding those violations, ODNI’s 2020 Transparency Report identified “four instances in which . . . a FISC order was required pursuant to section 702(f)(2) but not obtained prior to reviewing the results of a query that was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security.” *ODNI 2020 Transparency Report*, at 22.⁸

Nor did the FBI even seek or obtain any such orders. *Id.* Thus, even as late

⁸ See also Elizabeth Goitein, “ODNI’s 2019 Statistical Transparency Report: The FBI Violates FISA . . . Again,” *Just Security*, May 11, 2020, available at <https://bit.ly/3sh2OxH> (“[t]he news that the FBI violated the warrant requirement is just the latest in a remarkable series of revelations. . . . These incidents follow a decade in which the government failed (for several years) to report the collection of purely domestic communications under Section 702, and then failed (for several more years) to comply with the procedures that the [FISC]

as 2021, FBI had a zero percent compliance record *even when it knew the law required it to seek an order from the FISC before conducting a query.*

In response to this pervasive non-compliance the FISC recommended “revising the FBI’s querying procedures” yet again, as well as “modifying its systems, providing revised and expanded guidance on the querying standard, augmenting training, and increasing auditing and oversight efforts.” *2022 FISC Op.*, at 34.

The FISC also recognized that written procedures are not the problem. Rather, “[t]he real concerns have always centered on the querying provisions as likely to be implemented by the FBI, in view of the repeated querying violations.” *Id.* at 36. However, as before, the FISC approved renewal of the Section 702 program.

Thus, in defiance of procedures and protocols, FISC directives, and statutory requirements, the FBI has continued to query unabated without regard for Fourth Amendment considerations it knows full-well apply. Nothing could be further from “good faith.”

imposed to remedy the resulting Fourth Amendment violation”).

ix. *The 2023 PCLOB Report*

As noted **ante**, at 13-14, the PCLOB issued a report in 2023 dedicated to Section 702. Regarding FBI policies developed to address the enduring non-compliance set forth above, the *2023 PCLOB Report* concluded “These new policies are welcome, but are not sufficient to address the threats posed by U.S. person queries.” *Id.* at 190. *See also id.* at 191 (“FBI’s new procedures for approval of Sensitive Queries represent an important step toward directly addressing these threats to protected expressive activity. However, these procedures are not sufficient to fully safeguard First Amendment activities”); *id.* at 190-91 (descriptions and statistics regarding non-compliance incidents occurring in 2021).

Reviewing the history of FBI querying of Section 702 databases, the *2023 PCLOB Report* lamented, “The behavior indicates that FBI has treated Section 702 databases essentially as a *search engine for routine use.*” *Id.*, at 191 (emphasis added). Also, “FBI’s routine use of queries to search a specialized foreign intelligence database is especially problematic due to the fact that FBI uses the database for pre-assessment and assessment actions.” *Id.* at 192.

The *2023 PCLOB Report* cautioned that “[i]n the Board’s view, such routine querying of 702 information based on even an uncorroborated tip demonstrates

another key privacy threat posed by U.S. person queries.” *Id.*

In addition, “Further compounding the issue, these noncompliant searches are only able to be uncovered through manual auditing of the FISA databases at local field offices[,]” *id.* at 191-92, leading to the inescapable conclusion that the improper querying is even more widespread than reported.

3. *FISA’s History of Non-Compliance Generally Warrants Rejection of Application of the “Good Faith” Exception Here*

The history of government – whether DoJ or FBI or NSA – non-compliance with even the relaxed strictures imposed by FISA coupled with misrepresentations to the FISC, is too voluminous and multifaceted to present herein. Even the sources listed below represent only a fraction of the abuses that have continually invaded the privacy of U.S. persons in manners that exceed either or both statutory and constitutional authority. *See, e.g., ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (addressing an entirely different FISA program); *United States v. Moalin*, 973 F.3d 977, 984, 996 (9th Cir. 2020) (same program – the Section 215 [50 U.S.C. §1861] bulk telephony metadata collection program – violated the statute and may have violated the Fourth Amendment, but violations were harmless).

In addition to the 2011, 2017, 2018, 2019, 2020, and 2022 FISC opinions digested *ante*, at 40-60, other FISC opinions declassified since 2013 include other examples of the government’s persistent and diverse noncompliance

with FISC orders and restrictions, and lack of candor in its communications with the FISC:

- June 25, 2020, *Order in In re Carter Page, a U.S. Person*, Docket Nos. 16-1182, 17-52, 17-375, 17-679 (FISA Ct.), Opinion and Order Regarding Use and Disclosure of Information, available at <https://www.clearinghouse.net/chDocs/public/NS-DC-0127-0009.pdf>
- *[(Case Name Redacted), PR/TT No. [docket redacted]* (FISC [date redacted]) (declassified Nov. 18, 2013), available at <https://bit.ly/33EBsr3>);
- *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], No. BR 09-06* (FISC June 22, 2009) available at <https://bit.ly/3m5enUH>);
- *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], No. BR 09-13*, 2009 WL 9150896, at *2 (FISA Ct. Sept. 25, 2009); and
- *In re Production of Tangible Things From [Redacted], No. BR 08-13*, 2009 WL 9150913 (FISA Ct. March 2, 2009).⁹

In addition, the DoJ Inspector General (“DoJ IG”) has issued several reports

⁹ The FISC’s findings in these cases is discussed in more detail in

(digested more fully in Hasbajrami's *Post-Remand Memo*, at 61-74) detailing the FBI's and DoJ's repeated and systemic failures to abide by FISA's provisions:

- Office of the Inspector General, Department of Justice, Oversight and Review Division 20-012, *Review of Four Fisa Applications and Other Aspects of the Fbi's Crossfire Hurricane Investigations* (December 9, 2019), available at bit.ly/2sOu8H4;
- *Management Advisory Memorandum for the Director of the Federal Bureau of Investigation Regarding the Execution of Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons*, DoJ IG, March 30, 2020, available at <https://bit.ly/3mtppmU>;
- DoJ IG, *Audit of the Federal Bureau of Investigation's Execution of its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.s. Persons*, Report 21-129 (September 2021), available at <https://oig.justice.gov/sites/default/files/reports/21-129.pdf>;
- Office of the Inspector General, National Security Agency/Central Security Service, *Special Study of NSA Controls to Comply with*

Hasbajrami's *Post-Remand Memo*, at 74-82.

Signals Intelligence Retention Requirements – Unclassified Summary

(December 12, 2019), available at <https://bit.ly/3oWYPUJ>; and

- DoJ IG, *Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act*, March 8, 2006, available at <https://bit.ly/33q2J00>.

In response to a FISC Order after the DoJ IG’s 2019 report, FBI Director Christopher Wray replied with a detailed proposal for correcting the FBI’S non-compliance with FISA. *See* FBI’s (Unclassified) January 10, 2020 Response to the Court’s Order Dated December 17, 2019 (“FBI Response”), available at <https://bit.ly/3plwFDh>.

Not satisfied, the FISC appointed as its “amicus attorney” the estimable FISA veteran David S. Kris to evaluate the adequacy of those corrective measures. In a January 15, 2020, letter to FISC Chief Judge James E. Boasberg, Kris reported that “that the FBI’s proposed Corrective Actions are insufficient and must be expanded and improved in order to provide the required assurance to the Court.” *See* January 15, 2020, Letter from David S. Kris, at 2, available at <https://bit.ly/3sd7410>.

Kris also reiterated that while “the government must adhere to a strict duty of candor and accuracy before the Court. . . . Nor can there be any dispute that the government has profoundly failed to meet that duty.” *Id.* at 4. Kris added that

“[t]he FBI’s recent failures, however, are egregious enough to warrant serious consideration of significant reform.” *Id.*, at 8.

F. *Case Law Establishes That the “Good Faith” Exception Should Not Apply Here*

This unbroken record demonstrates that the FBI and NSA have had ample opportunity to correct FISA’s, and Section 702’s, serious and recurring problems through supervision and internal review. Not only have they abjectly failed to do so, but they have resisted any substantive reform, instead instituting a series of fig-leaf procedural protections that are routinely ignored.

Consequently, the lack of “good faith” is profound and manifest. Rather than “good faith,” the government’s conduct has demonstrated a pattern of systemic defiance.

As the Supreme Court has instructed, the “good faith” exception is applicable only when government personnel conduct a search “in objectively reasonable reliance on binding judicial precedent.” *Davis v. United States*, 564 U.S. 229, 247 (2011). Here, citing *Davis*, the District Court applied the “good faith” exception because the “agents here conducted queries ‘in reasonable reliance on binding precedent’ at the time, there in the form of FISC-approved procedures.” *Hasbajrami II*, 2025 WL 447498, at *20, *citing Davis*, 564 U.S. at 240.

However, as the Eleventh Circuit initially explained in *Davis*, binding

judicial “precedent on a given point must be unequivocal.” *United States v. Davis*, 598 F.3d 1259, 1266 (11th Cir. 2010), *aff’d*, 564 U.S. 229 (2011).

Here, such “unequivocal” and “binding” precedent simply did not exist at the time the querying in this case was performed. The government cannot point to any statute or court opinion that expressly authorized warrantless querying of the Section 702 databases (as opposed to instituting generalized minimization protocols).

The District Court relied on the minimization procedures, which included querying, that had been approved by the FISC. A. 61-63; *Hasbajrami II*, 2025 WL 447498, at *8. The publicly available procedures in closest proximity to the querying in this case were promulgated in 2008. *See* Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act, Effective November 1, 2008 (declassified April 13, 2017), available at <https://bit.ly/3U8Anyu>.

Yet the standard in those procedures was *reasonableness*, and did not carve out any exceptions to the Fourth Amendment, or alter the typical Fourth Amendment analysis. *Id.* at 16. Thus, those procedures do not provide safe harbor as unequivocal binding precedent that would override traditional Fourth Amendment principles.

The default rule is that warrantless searches on U.S. persons are *not* permitted, and nothing provided the agents herein authority to depart from that standard. As the Supreme Court has explained in the context of programmatic stops, such as traffic checkpoints, “[a] search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.” *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000), *citing Chandler v. Miller*, 520 U.S. 305, 308 (1997).

Thus, this case is entirely *unlike* those that found “good faith” after the Supreme Court’s decision in *Carpenter v. United States*, 585 U.S. 296 (2018), *see, e.g., United States v. Chambers*, 751 F. App’x 44 (2d Cir. 2018). In *Carpenter* agents relied on a *statute*, 18 U.S.C. §2703(d), and individualized *court orders* obtained pursuant to that statute. Neither predicate is present here.

In *United States v. Wey*, 256 F. Supp.3d 355 (S.D.N.Y. 2017), in holding the “good faith” exception did not apply, the District Court relied on this Court’s opinion in *United States v. Rosa*, 626 F.3d 56, 65 (2d Cir. 2010), in ruling that government agents had conducted an “overseizure” of items that were outside of the scope of the warrant as issued. *Wey*, 256 F. Supp.3d at 403.

Wey is instructive here because of the District Court’s conclusion that “more troubling than . . . the initial seizure . . . are the efforts of the Government and its

Hearing witnesses to leverage the inappropriately expansive terms of the Warrants into strained explanations of why these materials were in fact properly seized.” *Wey*, 256 F. Supp.3d at 404.

That tracks the government’s attempts herein to leverage the validity of the initial Section 702 collection into a justification for the “inappropriately expansive” subsequent querying. Here, as in *Wey*, those efforts should not be rewarded.

Similarly in *In re 650 Fifth Ave. & Related Props*, 934 F.3d 147 (2d Cir. 2019), this Court declined to apply the “good faith” exception even though the District Court had overlooked the defects in the warrant because “the agents on site here knew what they were looking for and, importantly, why[.]” *Id.* at 163 (quoting *In re 650 Fifth Ave.*, No. 08 Civ. 10934 (KBF), 2017 WL 2062983, at *23 n.34).

There, as here, reliance on the discretion of the querying FBI agents within the boundaries of an essentially generalized order, in the form of approved procedures, does not qualify for application of the “good faith” exception.

In addition, *Herring*’s instruction that “good faith” does not apply to “deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence” is entirely applicable here. *Herring*, 555 U.S. at

144. Indeed, in *Herring* the Court explained that “an error that arises from nonrecurring and attenuated negligence is thus far removed from the core concerns that led [the Court] to adopt the rule in the first place.” *Id.*

Here, the persistent, pervasive, and overwhelming volume of non-compliance – deliberate, opaque, and resistant to reform and direction provided by the FISC and Congress – clearly establishes at the very least the “deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence” identified in *Herring*, which precludes application of the “good faith” exception. As a result, as in *Illinois v. Krull*, 480 U.S. 340 (1987), reasonable government officials “should have known that the [querying] was unconstitutional.” *Id.*, at 355.

G. *The Balancing Performed as Part of the “Good Faith” Analysis Overwhelmingly Favors Suppression Here*

Given the recurring and systemic non-compliance with respect querying of Section 702 databases, the balancing attendant to an evaluation of the impact of the “good faith” exception is decidedly in favor of suppression.

While the District Court cites *Davis* for the proposition that in cases such as this the “deterrence rationale of the exclusionary rule loses much of its force,” A. 92; *Hasbajrami II*, 2025 WL 447498 at *20, citing *Davis* 564 U.S. at 238, (internal quotation marks omitted), the quantum of potential deterrence here, is

indisputably greater by several orders of magnitude than that in *Davis*, in which police officers relied on contemporaneous Fourth Amendment jurisprudence, *New York v. Belton*, 453 U.S. 454, 458-459 (1981), to conduct a search of an automobile, only to have that rule changed two years later in *Arizona v. Gant*, 556 U.S. 332 (2009).

In *Davis*, the advantage of deterrence was marginal: there was no record of “recurring or systemic negligence,” it was not stated or implied that methods by which the police department was conducting automobile searches were repeatedly questioned by the courts, or that police officers were ignoring orders, directives, policy memos, or procedures.

Instead, by all accounts, the officers in that case were nothing less than the type of “[r]esponsible law enforcement officers [who] will take care to learn ‘what is required of them’ under Fourth Amendment precedent and will conform their conduct to these rules.” *Davis*, 564 U.S. at 241, quoting *Hudson v. Michigan*, 547 U.S. 586, 599 (2006).

While in *Davis*, “[a]bout all that exclusion would deter in this case is conscientious police work[,]” *id.*, here significant deterrence, affecting the rights of innumerable U.S. persons whose communications in Section 702 databases is queried, can be achieved. Here, it is not “conscientious police work,” that is the

target of deterrence, but rather a history and culture of impunity.

In *United States v. Karathanos*, 531 F.2d 26, 33 (2d Cir. 1976), this Court determined that suppression would have the salutary effect of making magistrates or state officials authorizing search warrants “aware that their decision to issue a search warrant is a matter of importance not only in regard to the constitutional rights of the person to be searched, but also in regard to the success of any subsequent criminal prosecution[.]”

Here, suppression, rather than application of the “good faith” exception, will make FBI and NSA personnel acutely aware that querying is “a matter of importance” not only to Hasbajrami – who has already served all but two months of his sentence – but to the principles of the Fourth Amendment at large. It would internalize compliance within the FBI and restore accountability.

Indeed, this case presents the paradigmatic example of the situation of which Justice Potter Stewart warned: “If the courts admit illegally obtained evidence . . . there would be little reason for police officers to err on the side of caution where constitutional principles are unsettled.” Potter Stewart, *The Road to Mapp v. Ohio and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1402 (1983).

Otherwise, impunity – and the inevitable accompanying Fourth Amendment

violations – will continue to reign unchecked. This appeal presents the opportunity to right a wrong committed during the investigation of this case while also correcting persistent contraventions of the Fourth Amendment, as well as the FISC’s directives and Congress’s intent.

POINT II

THE DISTRICT COURT ABUSED ITS DISCRETION IN DENYING SECURITY-CLEARED DEFENSE COUNSEL ACCESS TO THE CLASSIFIED MATERIALS THAT FORMED THE BASIS FOR THE DISTRICT COURT’S FINDING THAT “GOOD FAITH” APPLIED

The District Court erred in denying security-cleared defense counsel access to the classified materials, which included classified briefing, the government provided *ex parte* that contributed to the District Court’s decision to apply the “good faith” exception.

The government’s resort to – and the District Court’s application of – the “good faith” doctrine only reinforces the need for disclosure to security-cleared defense counsel. “Good faith,” while a legal doctrine, nevertheless requires examination of *facts*, even if the standard is objective.

It is illogical and unfair if the only party able to review, analyze, and argue the facts is *the very party whose “good faith” is at issue*. That is not just an *ex parte* proceeding, but something even more fundamentally antithetical to justice

and accuracy in judicial determinations.

As set forth below, the District Court (1) misapplied the relevant statutory provisions; (2) failed to appreciate sufficiently that an *ex parte* presentation under the circumstances of this case denied Hasbajrami his right to Due Process guaranteed by the Fifth Amendment; and (3) failed to recognize that the Classified Information Procedures Act (“CIPA”) provided a readily available avenue to provide Hasbajrami the requested materials.

A. *Standard of Review*

The proper standard of review is *de novo* because the District Court’s decision to deny security-cleared defense counsel access to evidence derived from improper querying was based on an erroneous application of the law, namely, 50 U.S.C. § 1806(f).

The District Court’s subsequent decision to deny disclosure under CIPA should likewise be reviewed under the *de novo* standard, “because the Court already found disclosure to be inappropriate under FISA,” *Hasbajrami II*, 2025 WL 447498 at *22, which is a question of law since CIPA is a procedural statute which merely “clarifies district courts’ power under [Rule 16(d)],” *United States v. Aref*, 553 F.3d 72, 78 (2d Cir. 2008).

B. *The District Court's Opinion*

The District Court denied disclosure because, “Having reviewed the supplemental record on remand, the Court agrees with the Government that such evidence is ‘relatively straightfoward’ and ‘not complex.’” A. 95; *Hasbajrami II*, 2025 WL 447498, at *21, citing *United v. Abu Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010).

The District Court also concurred with the government that “the record on remand is significantly less voluminous and complex than the general Section 702 materials that Judge Gleeson was able to review without ordering disclosure,” A. 95; *Hasbajrami II*, 2025 WL 447498, at *21 (concluding that the “record, while lacking does not require Defendant’s review”); *id.*, at *18 (observing that the materials provided by the government were “sparse”), quoting, *Hasbajrami I*, 945 F.3d at 673.

However, the District Court did not attempt to reconcile the relevance and importance of that conclusion with its earlier observation that the government had failed to provide the queries themselves, the results of the queries, or “any supporting evidence” to justify the government’s assertions. A. 87; 2025 WL 447498, at 18. *See also ante*, at 34-35.

C. *FISA’s Provisions Require Disclosure In This Case*

FISA includes two sections that authorize disclosure “under appropriate security procedures and protective orders” – either because “such disclosure is necessary to make an accurate determination of the legality of the surveillance[,]” 50 U.S.C. §1806(f), or “to the extent that due process requires discovery or disclosure.” 50 U.S.C §1806(g).

Also, §1806(g) requires in addition to suppression, that the Court “otherwise *grant the motion of the aggrieved person,*” 50 U.S.C § 1806(g) (emphasis added), which logically includes motions to compel discovery of relevant materials after a search is determined to be unlawful.

1. *The District Court Misread the FISA Disclosure Provision*

In denying disclosure, the District Court failed to recognize the fundamental distinction FISA draws between the underlying FISA applications, orders, and materials and the evidence obtained from the surveillance. As *Kris & Wilson* point out:

Sections 1806(f), 1825(g), and 1845(f) distinguish between, on the one hand, “applications or orders or other materials relating to” a search or surveillance, and “evidence or information obtained or derived from electronic surveillance,” on the other.

Kris & Wilson at 31:7, p. 288.

Kris & Wilson also point out the House Report stated that “the provision that became Section 1806(g) ‘alters existing law and is a limitation on existing discovery practice’ refers only to FISA applications, orders, and related material.” *Id.*

As §1806(g)’s legislative history further demonstrates, Congress “sought to incorporate the Supreme Court’s holding in *Alderman v. United States*, 394 U.S. 165 (1969), that when a court grants a motion to suppress under FISA, it must require the government to ‘surrender to the defendant all the information illegally acquired in order for the defendant to make an intelligent motion on the question of taint.’” *Kris & Wilson*, 32:7, page 305, quoting *House Report* at 93 (which cites *Alderman* for the rule that “once a defendant claiming evidence against him was the fruit of unconstitutional electronic surveillance has established the illegality of such surveillance . . . he must be given those materials illegally acquired in the Government’s files to assist him in establishing the existence of ‘taint’”); *see also Alderman*, 394 U.S. at 181.¹⁰

In practical terms, the “question of taint” is no different than evaluating

¹⁰ The posture of this case, in which it was not the FISA applications, but instead the subsequent querying, that comprise the documentation essential to deciding whether “good faith” applies, distinguishes it dispositively from *United States v. Daoud*, 755 F.3d. 480 (7th Cir. 2014), in which only the FISA application materials were at issue.

whether the government acted in “good faith” here. The Court in *Alderman* explained the necessity of disclosure, and the concept underlying the procedural remedy created in 50 U.S.C. §1806(g), in language entirely applicable here:

Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide *the scrutiny which the Fourth Amendment exclusionary rule demands*.

Alderman, 394 U.S. at 184 (emphasis added); *see also id.* (“In our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate”).

Franks v. Delaware, 438 U.S. 154 (1978), also offers a persuasive analog. The Court rested its decision in significant part on the inherent inadequacies of the *ex parte* nature of the procedure for issuing a search warrant, and the contrasting enhanced value of adversarial proceedings during subsequent review.

The Court recognized that “the hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct.” *Franks*, 438 U.S. at 169. While the “pre-search proceeding is necessarily *ex parte*,” that only amplifies the need for disclosure in post-search proceedings because

[t]he usual reliance of our legal system on adversary proceedings itself should be an indication that an *ex parte* inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations.

Id.

FISA's legislative history further confirms that Congress envisioned disclosure in the unprecedented circumstances present here. Congress sought to “strik[e] a reasonable balance” between “mandatory disclosure” and “an entirely *in camera* proceeding *which might adversely affect the defendant's ability to defend himself.*” S. Rep. No. 701, 95th Cong., 2d Sess. at 64, reprinted in 1978 U.S.C.C.A.N. 4033 (“*Senate Report*”) (emphasis added).

Thus, in concluding the record “does not *require* Defendant's review,” the District Court erred, as its reliance on the language of 50 U.S.C. §1806(f), and *Abu-Jihaad*, which addressed only whether FISA applications and orders should be disclosed, not the evidence derived therefrom nor the legal briefs submitted thereafter to justify the warrantless search when subject to *post hoc* judicial review, was misplaced.. A. 95; *Hasbajrami II*, 2025 WL 447498 at *21.

2. *Disclosure Was “Necessary” In Relation to the District Court’s Decision Regarding “Good Faith”*

In the alternative, even if this Court decides to apply the “necessary” standard, either to the evidence obtained by improper querying, or to the queries themselves and all materials related to their execution, disclosure is still required under that standard.

In *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984), relying on FISA’s legislative history, this Court identified factors that would justify disclosure, explaining that the need for disclosure

might arise if the judge’s initial review revealed potential irregularities such as possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order[.]

Duggan, 743 F.2d at 79; *see also United States v. Belfield*, 692 F.2d at 147 (quoting S. Rep. No. 701, 95th Cong., 2d Sess. 64 (1979)); *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (same).

Here, the circumstances match those this Court described in *Duggan* and by the D.C. Circuit in *Belfield* (reflecting the legislative history), and the government’s non-compliance clearly rises to level requiring disclosure of the querying materials relevant to whether the government acted in “good faith.” *See*

also *Fazaga v. Fed. Bureau of Investigation*, 595 U.S. 344 (2022) (analyzing issue pursuant to the state secrets privilege).

D. *Due Process Requires Disclosure*

Moreover, 50 U.S.C. §1806(g) requires disclosure in order to afford Hasbajrami the Due Process that the Fifth Amendment guarantees. In addition to the considerations articulated in *Alderman, Franks*, and *Duggan* (as well as FISA’s legislative history), discussed *ante*, at 72-77, in *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004), this Court reemphasized the importance of open, adversary proceedings, declaring:

Particularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other.

Abuhamra, 389 F.3d at 322-23, *citing Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 171 n.17 (1951) (Frankfurter, J., *concurring*) (*citing Board of Education v. Rice*, A.C. 179, 182 (1911) (noting the “the duty lying upon every one who decides anything” is to “act in good faith and fairly listen to both sides, for that is a duty lying upon every one who decides anything” to “always giv[e] a fair opportunity to those who are parties in the controversy [to] correct[] or contradict[] any relevant statement prejudicial to their view”)

Those same principles the Supreme Court and this Court have found compelling in those cases mandate rejection of *ex parte* procedures in the peculiar context of this case. Denying an adversary access to the facts (and *post hoc* legal arguments) constitutes an advantage as powerful and insurmountable as exists in litigation.

Also, the transparency issues that have historically plagued Section 702 and FISA – including, as recognized by this Court and the District Court, *in this case* – only amplify the need for disclosure here to security-cleared defense counsel, as it remains apparent that an insular approach only encourages, even enables, impunity with respect to the violations of civil liberties that attend such secrecy.

E. *CIPA Provides a Well-Established Means of Disclosure*

Additionally, the classified nature of the materials does not foreclose access by security-cleared defense counsel. This Court clearly envisioned that disclosure can be arranged “consistent with the requirements of CIPA and FISA.” *Hasbajrami I*, 945 F.3d at 677 n.24. *See also United States v. Moussaoui*, 365 F.3d 292, 308 n.12 (4th Cir.), *opinion amended on reh’g*, 382 F.3d 453 (4th Cir. 2004) (applying principles and provisions of CIPA to circumstances involving classified information and materials even though the statute did not technically cover the specific situation); *United States v. Moussaoui*, 333 F.3d 509, 513-15

(4th Cir. 2003).

In *United States v. Zubaydah*, 595 U.S. 195, 255 (2022) (Gorsuch, J., joined by Sotomayor, J., *dissenting*), Justices Gorsuch and Sotomayor, in dissent, cited CIPA as a means of regulating disclosure of classified information even in a *civil* case. *Id.*, at 255 (Gorsuch, J., joined by Sotomayor, J., *dissenting*).

Indeed, Justice Gorsuch even more recently stressed, “Efforts to inject secret evidence into judicial proceedings presents obvious constitutional concerns.” *TikToc Inc. v. Garland*, 145 S.Ct. 57, 74 (2025) (Gorsuch, J., *concurring*). “Usually, ‘the evidence used to prove the Government’s case must be disclosed to the individual [or at least, as in the present situation, his security-cleared defense counsel] so that he has an opportunity to show that it is untrue.’” *Id.*, *quoting*, *Green v. McElroy*, 360 U.S. 474, 496 (1959).

CIPA was designed to regulate the use of classified material in federal criminal prosecutions, and to create a system through which defense counsel would gain access to classified information and materials pertinent to the case. That purpose coincides precisely with disclosure of the materials security-cleared counsel seeks here.

In that context, the history of Section 702 violations summarized *ante*, at 40-60, is specifically relevant to whether disclosure to security-cleared counsel is

necessary and appropriate in this case. Ultimately, in light of the historical record of repeated, unpunished, and unremedied violations of Section 702 program specifically (and FISA generally), and the backdoor querying process in particular (since its inception), it is respectfully submitted that an accurate determination whether the government acted in “good faith” cannot be reached without the substantive participation of security-cleared defense counsel in evaluating the facts at issue.¹¹

Accordingly, it is respectfully submitted that the Court should compel disclosure to security-cleared counsel the information and materials necessary to the determination whether the “good faith” exception applies (including those the District Court noted were *not* produced at all, *see ante*, at 34-35).

¹¹ In *Zubaydah*, Justices Gorsuch and Sotomayor, examined the historical record in much the same manner as the *Post-Remand Memo* did herein, contextualizing past instances in which subsequent disclosures decades later revealed that the government, in invoking the state secrets doctrine, had not been candid to the courts. Concluding that “[m]ore recent history reveals that executive officials can sometimes be tempted to misuse claims of national security to shroud major abuses and even ordinary negligence from public view[.]” 595 U.S. at 250, they discussed several historical examples, *id.*, at 252, including the initial state secrets case, *Reynolds v. United States*, 345 U.S. 1 (1953), which was predicated on a lie. *Zubaydah*, 595 U.S. at 251-52, *citing*, Dept. of Justice, Archives, N. Katyal, *Confessions of Error: The Solicitor General's Mistakes During the Japanese-American Internment Cases* (May 20, 2011); J. Weinstein, *The Role of Judges in a Government of, by, and for the People: Notes for the Fifty-Eighth Cardozo Lecture*, 30 *Cardozo L. Rev.* 1, 92 (2008); W. Weaver & R. Pallitto, *State Secrets and Executive Power*, 120 *Pol. Sci. Q.* 85, 101, 107-112 (2005).

Conclusion

Accordingly, it is respectfully submitted that the District Court's decision denying Hasbajrami's motion to suppress should be reversed, and/or the District Court's denying security-cleared defense counsel access to the classified materials relevant to its determination of the motion to suppress should be reversed, and Indictment dismissed, or the matter remanded for further proceedings.

Dated: July 15, 2025
New York, New York

Respectfully submitted,

/S/

MICHAEL K. BACHRACH
Law Office of Michael K. Bachrach
224 West 30th Street, Suite 302
New York, NY 10001
(212) 929-0592
michael@mbachlaw.com

JOSHUA L. DRATEL
Dratel & Lewis
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707
jdratel@dratellewis.com

STEVE ZISSOU
Steve Zissou & Associates
42-40 Bell Blvd., Suite 302
Bayside, NY 11361

– On the Brief –

Joshua L. Dratel
Michael K. Bachrach
Jacob C. Eisenmann (*pending admission*)

*Attorneys for Defendant-Appellant
Agron Hasbajrami*

CERTIFICATE OF COMPLIANCE WITH F.R.A.P. 32(a)

I hereby certify that:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7) because this brief contains 16,428 words, excluding the parts of the brief exempted under Fed. R. Civ. P. 32(a)(7)(B)(iii), pursuant to motion for leave to file an oversized brief filed with this Court on July 14, 2025.
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportional typeface using WordPerfect in 14 point font Times New Roman style.

Dated: July 15, 2025

\s\ Joshua L. Dratel
Joshua L. Dratel
DRATEL & LEWIS
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707
jdratel@dratellewis.com