UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA,

- against - 11 Cr. 623 (JG)

AGRON HASBAJRAMI,

Defendant.

----------X

DEFENDANT'S POST-REMAND MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR SUPPRESSION AND ACCESS TO RELATED DISCOVERY

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

JOSHUA A. DRATEL, ESQ.
Dratel & Lewis
29 Broadway, Suite 1412
New York, New York 10001
(212) 732-0707
jdratel@dratellewis.com

STEVE ZISSOU, ESQ.
42-40 Bell Blvd., Suite 302
Bayside, New York 11361
(718) 279-4500
stevezissou@stevezissouesq.com

Attorneys for Defendant Agron Hasbajrami

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER

Introduction

This Memorandum of Law is submitted in support of defendant Agron Hasbajrami's motion to suppress certain electronically intercepted communications and evidence, and/or for discovery related to that motion. This Memo of Law is submitted in advance of the government's provision of information to the Court in order to preview the issues to be determined, and to emphasize the importance of disclosure and discovery to security-cleared defense counsel.

The basis for this submission, essentially a continuation of Mr. Hasbajrami's pretrial motions, is the Second Circuit's remand to the District Court for the purpose of determining, in the context of the electronic interception, retention, and searching of Mr. Hasbajrami's communications pursuant to the Foreign Intelligence Surveillance Act ("FISA"), "(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." *United States v. Hasbajrami*, 945 F.3d 641, 646-47 (2d Cir. 2019).

It is respectfully submitted that (b) and (c) cannot be answered without an answer to (a), which renders discovery necessary in order for the Court to make an informed, constitutionally grounded decision that includes an essential contribution from security-cleared defense counsel.

As discussed below, while (a) may well involve classified information, defense counsel possess the appropriate security clearance, and FISA itself provides two separate mechanisms, that would authorize and even require discovery to cleared defense counsel in this unique case – the first such remand in FISA's 43-year history. In its opinion, the Second Circuit explicitly conferred upon this Court the discretion to order such discovery. Indeed, it is respectfully submitted that the specific sections of FISA, and the Fifth Amendment's Due Process guarantee incorporated therein, require

it, and it can be accomplished seamlessly pursuant to the provisions of the Classified Information Procedures Act ("CIPA").

As detailed below, the revival of this case after Mr. Hasbajrami's initial plea of guilty was the result of the government's deliberate failure to disclose the specific nature of its FISA surveillance. Nor, once that misrepresentation was revealed, has the government been more forthcoming. As the Second Circuit's opinion notes repeatedly, as discussed below, the government would not even disclose *to the Court* certain information, or provide declarative answers to questions posed at oral argument. It is in that context of repeated non-disclosure that the remand occurred and discovery and disclosure here are necessary.

The government's failure of candor demonstrated here is simply an example and extension of the government's persistent history of non-compliance with FISA's procedural and substantive rules and limitations – which implicate the Fourth Amendment's search and seizure protections as well as the Fifth Amendment's Due Process guarantee – that have been catalogued repeatedly by a number of authorities: from periodic declassified opinions issued by the Foreign Intelligence Surveillance Court ("FISC"), to reports by the Department of Justice's Inspector General ("DoJ IG"), the National Security Agency's Inspector General ("NSA IG"), and Office of the Director of National Intelligence ("ODNI"), to Congressional complaints and investigations, to reports from the Privacy and Civil Liberties Oversight Board ("PCLOB").

Nor has oversight from those monitoring entities been sufficient to stem the tide of unremitting violations of both the rules governing the FISA process and the fundamental Fourth Amendment protections that apply even to collection of foreign intelligence of U.S. persons' communications.

Indeed, as discussed below, recent events indicate even that ineffective and limited supervisory mandate has been reduced. As a result, only the traditional federal courts – and in this case, *this* Court – are capable of enforcing those rules and preserving Fourth Amendment principles, but only with the meaningful participation of cleared defense counsel.

The pervasive violations chronicled in those opinions and reports issued during the past two decades – many of which are illuminating in the context of the Second Circuit's opinion in this case, and many of which have been issued since the Circuit's remand – depict a FISA system that has never functioned properly, particularly with respect to adherence to Fourth Amendment or even statutory standards, and especially with respect to the particular FISA program at issue in this case: so-called "Section 702" interception and querying authority.

As set forth below, those opinions and reports also provide examples of violations during the very period at issue in this case – 2011 – and reflect specific problems that exert a dispositive impact on the issues the Second Circuit directed be resolved:

(1) the Federal Bureau of Investigation's ("FBI") (and other law enforcement and intelligence agencies') continued and widespread overly permissive and improper access to Section 702 databases to pursue criminal investigations, including improper and indiscriminate use of "backdoor searches" and authority therefor that the FISC declared *un*reasonable in 2018 (and criticized for years before and since), inadequate internal controls within FBI and National Security Agency ("NSA") to control such backdoor searches, and an abject absence of required recordkeeping;

(2) the general unreliability of applications for FISA interceptions, perpetuated through renewal applications and subsequent querying, given the recent record and reporting,

buttressed by the historical record of non-compliance throughout FISA's history, including specific errors. violations, and abuses identified in the opinions and reports that likely replicate similar errors in the applications made with respect to Mr. Hasbajrami, *i.e.*, the failure to include complete or contradictory information and/or exculpatory information (either in initial applications or renewal requests, or as part of the querying process); and

(4) the government's misrepresentations and evasions in this case, coupled with the FBI's generally for years as documented in FISC opinions and elsewhere – to its own lawyers, by its lawyers to other lawyers in FBI and Department of Justice ("DoJ"), and to the FISC – and concealment that makes the Section 702 querying process (and FISA generally) completely untrustworthy to the extent that *ex parte* representations cannot be credited without scrutiny by an adverse party, *e.g.*, security-cleared defense counsel, and which demonstrate the weaknesses and susceptibility to error inherent in an *ex parte* process.

In addition, a recent decision issued since the Second Circuit's opinion herein establishes that Mr. Hasbajrami is entitled to notice of precisely what surveillance was conducted in the course of the investigation, and its relation to the evidence ultimately to be used against him. Thus far, the government has, through a series of prevarications, evasions, and equivocations, repeatedly denied Mr. Hasbajrami that notice to which he is entitled by statute, rule, and the Constitution.

It is inescapable – and the government has even acknowledged – that the disposition of Mr. Hasbajrami's motion to suppress will resolve this case categorically, as granting the motion will deprive the government of sufficient evidence to prosecute Mr. Hasbajrami, and require dismissal

of the case, and concurrent vacatur of his guilty plea.

This submission is lengthy, but the record of non-compliance and abuse specifically in this case and with respect to Section 702, and regarding FISA generally, is extensive and multifaceted – and even this catalogue is not exhaustive. Given the complexity and unique character of these issues – which have a decade of history in this case, and which generated an 89-page opinion from the Second Circuit – we respectfully request the Court's permission and indulgence to file this oversized brief, as only a comprehensive submission can provide the requisite showing for the Court.

Accordingly, it is respectfully submitted that the Court should order disclosure and discovery of the relevant materials to security-cleared defense counsel, and, ultimately, grant Mr. Hasbajrami's motion to suppress.

Statement of the Facts

Given the detail provided in the Second Circuit's opinion, *see United States v. Hasbajrami*, 945 F.3d at 645-49, and the Court's familiarity therewith (as demonstrated during the September 13, 2021, pretrial conference), this Statement of Facts will limit repetition of that discussion to contextual necessity, and instead address primarily matters *not* covered in the Second Circuit's discussion.

A. *Procedural History*

Agron Hasbajrami was arrested September 6, 2011, and ultimately 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).

As described in Mr. Hasbajrami's Revised Pre-Sentence Report, dated, February 6, 2013

("PSR"):

> An investigation by agents with the Federal Bureau of Investigation's Joint Terrorism Task Force ("JTTF") revealed that between April 2, 2011, and August 28, 2011, the defendant engaged in numerous email transactions with individual #1, utilizing different email accounts. Individual #1 (whose identity is known to the parties), is an individual the defendant believed was associated with a terrorism organization. During the course of their emails, the two arranged for the transfer of money from the defendant to individual #1, purportedly to support Islamic fundamentalist terrorism operations, and to arrange for the defendant's travel to the Federally Administered Tribal Areas ("FATA's") of Pakistan to join a jihadist fighting group. More specifically, the emails discussed and contained instructions and detailed descriptions of the smuggling route that the defendant was to take into the FATA, as well as contact instructions as to how the defendant would make contact with individual #1 once he arrived in the FATA, and how money should be sent to individual #1 from the United States, via a courier in Germany . . .

PSR, at ¶¶ 2-3 (footnote omitted). *See also Hasbajrami*, 945 F.3d at 645-47.

However, "[n]otwithstanding the emails discussed . . . above . . . there [was] information to suggest that Individual #1 was not in fact a terrorist, and that he solicited funds from the defendant for purposes unrelated to terrorism." PSR, at ¶ 3.

Nevertheless, Mr. Hasbajrami "was arrested by JTTF agents at John F. Kennedy International Airport in Jamaica, New York, on September 6, 2011, prior to boarding a flight bound for Istanbul, Turkey." *Id*. A contemporaneous "search of the defendant's luggage subsequent to his arrest revealed a tent, boots and cold-weather gear." *Id*. Also, "[t]he case agent advised that in a postarrest statement, the defendant admitted to the entirety of the offense." *Id*. *See also Hasbajrami*, 945 F.3d at 645, 647.

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

recounted, 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*, 945 F.3d at 648 (citation omitted).

Elaborating, the Circuit noted 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*, 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*, ___ F.3d ___, 2021 WL 5817486, at *77 n.2 (10th Cir. December 8, 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 Snowden leaks, recognizing that: [U]ntil the Snowden leaks in 2013, the American public was led to believe that the government did not query or use FAA-acquired surveillance against non-targeted U.S. persons"), *citing Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).

As a result, Mr. Hasbajrami moved to withdraw his guilty plea because, as Judge Gleeson concluded, "[w]hen the government provided FISA notice without FAA 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) (*see* ECF #85). *See also Hasbajrami*, 945 F.3d at 648. Judge Gleeson granted the motion, *id*., and Mr. 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"). Mr. Hasbajrami pleaded guilty June 26, 2015 (ECF # 142), with the express reservation of his right to pursue his motion to suppress on appeal.

B. ***The Structure and Parameters of Section 702 Surveillance***

As the Second Circuit's opinion explains, Section 702 was enacted as part of the 2008 FISA Amendments Act ("FAA"), building on the initial FISA constellation of surveillance authorities included in the original 1978 legislation, 50 U.S.C. §1801, *et seq*., and expanded through several post-9/11 amendments. *Hasbajrami*, 945 F.3d at 650.[1]

[1] As the Court pointed out, FISA was a reform designed to create *limitations* on the government's national security surveillance powers: "FISA was first enacted in response to revelations about the government's electronic surveillance of the domestic communications of United States citizens. *See* David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* §3:7 []; *Hasbajrami*, 945 F.3d at 650. *See also American Civil Liberties Union v. United States*, ___ U.S. ___, 142 S. Ct. 22 (2021) (Gorsuch, J., dissenting from denial of certiorari) ("[i]n response to allegations of wrongdoing by the Nation's intelligence agencies, in 1975 Congress convened a select committee chaired by Senator Frank Church to investigate. *See* S. Rep. No. 94-755, at v (1976). Ultimately, the Church committee issued a report concluding that the federal government had, over many decades, 'intentionally disregarded' legal limitations on its surveillance activities and 'infringed the constitutional rights of American citizens.' *Id*., at 137").

Thus, the Court continued, "'[t]raditional FISA' surveillance, as surveillance under the FISA has come to be known following the enactment of the FAA in 2008, governed surveillance inside the United States, in the context only of national security investigations rather than domestic criminal prosecutions." *Hasbajrami*, 945 F.3d at 650, *citing* David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* ("*Kris & Wilson*") §4:2.[2]

That "traditional FISA" "established procedures governing the collection of information derived from electronic surveillance, physical searches, 'pen/trap' surveillance, and tangible-things production orders, and the use of information so obtained." *Hasbajrami*, 945 F.3d at 650, *citing Kris & Wilson*, at §4:5. In turn,

> [i]n order to initiate traditional FISA surveillance, the government must submit an application to a court demonstrating that there is "probable cause to believe that 'the target of the electronic

---

[2] 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. 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.

Initially, such surveillance and interception, denominated the Terrorist Surveillance Program (hereinafter "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 113-16 (2016), at 113-16 (chronicling the transfer of the program's approval from DoJ to the White House because of DoJ's objections). After the TSP's existence was disclosed in December 2005 in *The New York Times*, "[u]timately, 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], and on a longer term basis by the FISA Amendments Act ('FAA') [P.L. 261]." *CRS Report: Overview*, at 10 (footnotes omitted).

> surveillance is a foreign power or agent of a foreign power,' and that each of the specific 'facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.'

Hasbajrami, 945 F.3d at 650, *citing Clapper*, 568 U.S. at 403, (*quoting* 50 U.S.C. §1805(a)(3)).

In addition, "FISA applications are reviewed by two specialized courts: the Foreign Intelligence Surveillance Court ('FISC') and the Foreign Intelligence Surveillance Court of Review ('FISCR'), both composed of Article III federal judges assigned to their role [on a rotating basis] by the Chief Justice of the United States." *Hasbajrami*, 945 F.3d at 650, *citing Kris & Wilson*, at §5:1.

Both the FISC and FISCR operate in *ex parte* fashion, with the government as the only party. *See In re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008). In 2015, the FISC assigned an "*amicus*" attorney to represent competing interests, but even under that framework, discussed **post**, at 118, *amicus* counsel is not in contact with the target of the surveillance (which remains unaware of the litigation) or afforded access to all information relevant to the litigation.

Like ordinary warrants, "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*, 945 F.3d at 650, *citing Kris & Wilson*, at §6:2. 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 electronic surveillance warrants, but even from "traditional FISA" applications and approvals. The following chart, initially created by the Federal Defenders Office in another case, demonstrates

how the FAA differs from other electronic surveillance statutes – traditional FISA and Title III wiretaps – in terms of what information must be presented to a neutral and detached judicial officer in order to obtain authorization to execute specific searches and seizures:

	Title III	Traditional FISA	§ 702
Required level of suspicion of an individual	Probable cause the individual is committing, has committed, or is about to commit a criminal offense. *See* 18 U.S.C. § 2518(3)(a).	Probable cause the individual is a foreign power (including terrorist organizations) or an agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2)(A).	None
Required level of suspicion regarding facility to be monitored	Probable cause communications concerning an offense will be obtained through interception. *See* 18 U.S.C. § 2518(3)(b).	Probable cause each targeted facility is being used, or is about to be used, by a foreign power or an agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2)(B).	None
Particularity regarding individual to be monitored	Specify the identity, if known, of the person committing the offense or whose communications are to be intercepted. *See* 18 U.S.C. § 2518(1)(b).	Specify the identity, if known, or a description of the specific target of the surveillance. *See* 50 U.S.C. § 1805(c)(1)(A).	None

Particularity regarding location to be monitored	Specify the nature and location of the communications facilities as to which, or the place where, interception will occur. *See* 18 U.S.C. § 2518(1)(b).	Specify the nature and location of each of the facilities or places at which the surveillance will be directed. *See* 50 U.S.C. § 1805(c)(1)(B).	None
Particularity regarding types of communications to be intercepted	Particular description of the type of communication sought to be intercepted. *See* 18 U.S.C. § 2518(1)(b).	Designate the type of foreign intelligence information being sought and the type of communications or activities to be subjected to the surveillance. *See* 50 U.S.C. § 1805(c)(1)(C).	None

As recognized by the PCLOB, Section 702 represented a momentous shift, as "[r]ather than approving or denying individual targeting requests, the FISA court authorizes the surveillance program as a whole . . . ." in advance of the calendar year in which the standards will be applied. PCLOB, PCLOB REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 106 (2014) ("*PCLOB Report*"), available at https://perma.cc/WD5R-5GKE. *See also United States v. Muhtorov*, 2021 WL 5817486, at *90 (Lucero, J., dissenting) ("the government submits certifications and targeting and minimization procedures to the FISC, without identifying non-U.S. persons who are to be targeted under §702 or U.S. persons whose communications may be incidentally collected, and the FISC reviews the government's submission only as to whether the proposed procedures are 'reasonably designed' to meet the statutory requirement"), *citing PCLOB*

Report, at 24-31.[3]

The scope of Section 702 surveillance, interception, and retention has been breathtaking. The *Congressional Research Service* has noted that

> [a]ccording to a partially declassified 2011 opinion from the FISC, NSA collected 250 million Internet communications per year under this program. Of these communications, 91% were acquired "directly from Internet Service Providers," referred to as "PRISM collection." The other 9% were acquired through what NSA calls "upstream collection," meaning acquisition while Internet traffic is in transit from one unspecified location to another.

Edward C. Liu, Andrew Nolan, Richard M. Thompson II, CONG. RESEARCH SERV., R43459, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES AND RECENT DEVELOPMENTS 10 (footnotes omitted) (April 1, 2014) (hereinafter *CRS Report: Overview*), available at https://bit.ly/3F2to0Z, *citing In re Foreign Intelligence Surveillance Court (Redacted)*, 2011 WL 10945618, at *9, 25 (FISA Ct. 2011) ("*2011 FISC Op.*"); *see also PCLOB Report*, at 116 ("current number [of internet communications intercepted pursuant to Section 702] is significantly higher [as of 2014]").

The OFFICE OF CIVIL LIBERTIES, PRIVACY, AND TRANSPARENCY, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL

---

[3] The PCLOB is an independent, bipartisan agency within the executive branch whose members are appointed by the President and confirmed by the Senate. PCLOB, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 2 (Jan. 23, 2014). The PCLOB conducted a public hearing March 19, 2014, at which the General Counsels of the Federal Bureau of Investigation, the National Security Agency, and the Director of National Intelligence, as well as the Deputy Assistant Attorney General for the Department of Justice's National Security Division, provided testimony about programs operated under Section 702 (50 U.S.C. §1881a). *See Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act Before The PCLOB* (2014) (transcript available at https://bit.ly/3dV1wA3).

SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2020 16 (April 2021) ("*ODNI 2020 Transparency Report*"), available at https://bit.ly/33AdOfb, issued by the Office of the Director of National Intelligence ("ODNI") (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.[4]

Similarly, the percentage annual increase from 2016 to 2017 was 21%. *See* ODNI, 2017 ODNI TRANSPARENCY REPORT (May 2018), available at https://bit.ly/3F5lSCp. Cumulatively, "[s]ince 2013, the first year for which numbers were disclosed, the number of targets has increased by 45%." Robyn Greene (policy counsel for the Open Technology Institute at New America Foundation), "The Intel Community's Annual Transparency Report Raises More Questions Than It Answers," *Just Security*, May 14, 2018 ("*Greene*"), available at https://bit.ly/3GMN897.

In addition, backdoor searches increased during that time frame as well. The *2017 ODNI Transparency Report* disclosed that in 2017, intelligence agencies *not* including FBI, *see 2020 Transparency Report*, at 17 n.*, "used 7,512 identifiers, like email addresses, that belonged to Americans to search through the contents of 702 information, though it's unclear how many communications were searched and how many times searches for Americans' communications contents were conducted." *Greene*.

---

[4] The 2020 total of 202,723 was, of course, affected substantially by the Covid-19 pandemic that generally reduced surveillance across all programs. *See* Charlie Savage, "National Security Surveillance Plummeted Amid Pandemic and Russia Inquiry Fallout," *The New York Times*, April 30, 2021, available at https://nyti.ms/3pVd0ZC (Benjamin T. Huebner, ODNI's chief civil liberties, privacy, and transparency officer said, "The pandemic was the single event with the biggest impact to human behavior worldwide since the Second World War. That means it also had an impact on our foreign intelligence targets"); Dustin Volz, "U.S. National Security Surveillance Dropped in 2020 as Pandemic Kept Suspects at Home," *The Wall Street Journal*, April 30, 2021, available at https://on.wsj.com/3yvsqrs.

That represented "a 42% increase over the number of Americans' identifiers used for warrantless searches in 2016, and a 61% increase since reporting started in 2015." *Id*. Those non-FBI backdoor searches of U.S persons' intercepted communications exceeded 9,000 in 2018 and 2019 before dropping to 7,218 in 2020 (an unusual year, *see* **ante**, at n. 4). *2020 ODNI Transparency Report*, at 17.[5]

In addition, the *CRS Report: Overview*, again citing the *2011 FISC Op*., relates that

> NSA also has two methods for collecting information about a specific target: "to/from" communications collection, in which the target is the sender or receiver of the Internet communications; and "about" communications collection, in which the target is only mentioned in communications between non-targets.

Id. (footnotes omitted), *citing 2011 FISC* Op., at *5.

Moreover, according to the *CRS Report: Overview*, "[t]he Obama Administration also acknowledged to the FISC that technical limitations in the 'upstream' collection result in the collection of some communications that are unrelated to the target or that may take place entirely between persons located in the United States." *Id*., at 10 (footnote omitted).[6]

---

[5] The *ODNI Transparency Reports* also suffer from undercounting. As a commentator has pointed out, the numbers in the *ODNI Transparency Reports* are "simply incompatible with the FISA Court's description of dozens of such queries from the past year, and seems to drastically misrepresent how common the phenomenon of Section 702-acquired information flowing into law enforcement queries can be." Jake Laperruque, "Key Takeaways From Latest FISA Court Opinion on Section 702 and FBIWarrantless Queries," *Just Security*, April 28, 2021 ("*Laperruque: Key Takeaways*"), at 4, available at https://bit.ly/3Fp845R. Thus, the *2020 FISA Op.* "makes clear that the ODNI's annual transparency report has not been accurately portraying the scale of FBI law enforcement queries yielding Section 702-acquired information." *Laperruque: Key Takeaways*, at 3. *See also id*., at 4 ("updated numbers failed to account for how broadly 'batch queries' could pull in U.S. persons' information").

[6] The *CRS Report: Overview*, also explains that

> [t]he PRISM and upstream collections differ from the telephony

Periodically the FISC has declassified – and published in redacted form – opinions it has issued with respect to Section 702. For example in 2011 the FISC issued a lengthy opinion assessing the legality of the government's practice of scanning U.S. persons' international communications for certain terms that the government believed were associated with its foreign-intelligence targets. *See 2011 FISC Op.*.

In 2018 the FISC issued an opinion addressing the government's querying of databases of international communications obtained without a warrant for information about Americans. *See In re Foreign Intelligence Surveillance Court [Redacted]*, 402 F.Supp. 3d 45 (FISA Ct. 2018), *aff'd in part sub nom. In re DNI/AG 702(h) Certifications 2018*, 941 F.3d 547 (FISA Ct. Rev. 2019) ("*2018 FISC Op.*"). In 2017, 2019, and 2020, the FISC issued opinions published the following year, respectively, cataloging additional violations committed in the operation of Section 702, but each time approved the program. *See also [Redacted]*, Mem. Op. (FISA Ct. Sept. 4, 2019) ("*2019 FISC Op.*"), available at bit.ly/2x3tRC9, and *[Redacted]*, Mem. Op. (FISA Ct. Nov. 18, 2020) ("*2020 FISC Op.*"); *[Redacted]*, available at https://bit.ly/3Fp1cW2; *[Redacted]*, Mem. Op. (FISA Ct. Apr. 26, 2017) ("*2017 FISC Op.*"), available at https://bit.ly/3qcjsf6.

In the conventional federal courts, the constitutionality of Section 702 interceptions has been upheld by three Circuits: the Second Circuit in this case, *Hasbajrami*, 945 F.3d at 662, the Ninth

---

> metadata program in two key respects. First, the PRISM and upstream collections acquire the contents of those communications. Second, as this program targets the "to/from" and "about" communications of foreigners who are abroad, the collection of Internet-based communications may be considered by some to be more discriminating than the bulk collection of telephony metadata.

CRS Report: Overview, at 10.

Circuit in *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016), and most recently the 10th Circuit in *United States v. Muhtorov*, ___ F.3d ___, 2021 WL 5817486, at *14.

However, whether particular queries, or the querying procedures themselves, satisfy the Fourth Amendment is an issue of first impression. *See also* Peter G. Machtiger, *Updating the Fourth Amendment Analysis of U.S. Person Communications Incidentally Collected Under FISA Section 702*, HARV. NAT'L SEC. J. ONLINE (Feb. 7, 2021) ("*Machtinger*"), available at https://bit.ly/3dYZYFa. ("[t]he *Hasbajrami* court considered the querying of previously collected Section 702 analysis separately, which is something other courts have not done").[7]

Among the important distinctions between Section 702 collection, retention, and querying of intercepted communications and conventional electronic surveillance pursuant to Title III, or even "traditional FISA," are the minimization requirements. In *2011 FISC Op.*, 2011 WL 10945618, at *5, Judge Bates noted that the FAA "requires that the minimization procedures 'meet the definition of minimization procedures under [50 U.S.C. §§]1801(h) or 1821(4) . . .'" *Id.*, *citing* 50 U.S.C. §1881a(e)(1).

Elaborating, Judge Bates pointed out that

> [m]ost notably, that definition requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons

[7] In *Muhtorov*, the Tenth Circuit expressly declined to address querying, making clear – while citing *this case* – that "[q]uerying might raise difficult Fourth Amendment questions that we need not address here." *Muhtorov*, 2021 WL 5817486, at *25, *citing Hasbajrami*, 945 F.3d at 672-73 (footnote omitted). *See also Muhtorov*, at *25 n.21 ("the dissent relies on the Second Circuit's discussion of querying, which is not pertinent to this case"), *citing Hasbajrami*, 945 F.3d at 670-73.

> consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

Id., *(quoting* 50 U.S.C. §§ 1801(h) & 1821(4)).

In *Muhtorov*, the Tenth Circuit, citing the Second Circuit's opinion herein, noted that "[i]n theory, minimization procedures should lead to deletion of incidentally collected communications that have no relevance to foreign intelligence." *Muhtorov*, 2021 WL 5817486, at *11, *citing Hasbajrami*, 945 F.3d at 655 (in the Section 702 context, "information is 'minimized' by non-retention").

However, the Court in *Muhtorov* conceded that "deletion rarely happens." *Id*., *citing PCLOB Report*, at 128-29. Rather, "those communications often remain in the agency's databases unreviewed until they are retrieved in response to a database query, or . . . deleted upon expiration of their retention period, without ever having been reviewed." *Id*., *citing PCLOB Report*, at 129.

In addition to the distinctions in the concept of "probable cause" – particularly the fact that individual targets of surveillance are not necessarily reviewed by the FISC prior to acquisition of their communications – between traditional FISA warrants and Section 702 (50 U.S.C. §1881a) surveillance and acquisition, the FISC's oversight role with respect to the latter is "narrowly circumscribed." *In re Proceedings Required by §702(I) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), available at https://bit.ly/3dXPo14.

The FISC is asked to opine on the lawfulness of an entire year's worth of mass surveillance prospectively without reviewing a single targeting decision and without knowing how any one of those searches affected U.S. persons. In turn, during the subsequent year, the application of Section

702 procedures to actual persons and facts is not performed by judges, but instead by low-level intelligence analysts. *See PCLOB Report*, at 42.

Instead, the FISC's role is essentially limited to reviewing the targeting and minimization procedures that the government proposes to use to target and acquire communications prospectively. *See CRS Report: Overview*, at 11 (footnote omitted). The FISC must also find that the minimization procedures are reasonably designed to minimize the retention, and prohibit the dissemination, of information that is about a U.S. person or that could identify a U.S. person. *Id*. (footnote omitted), *citing* 50 U.S.C. §1881a(e).[8] However, the minimization procedures may allow for the retention and dissemination of information, including U.S. person information, that is evidence of a crime. *Id*.

C. *"Backdoor" Searches of the Section 702 Database(s)*

The minimization procedures also improperly permit the government's retention of these U.S. person communications for later searching – the so-called "backdoor searches" – through which the government subsequently queries its repository of FAA-collected communications specifically for information about U.S. citizens and residents – like Mr. Hasbajrami – including for evidence of criminal activity. *See PCLOB Report*, at 59; 2011 Minimization Procedures §3(b)(6).[9]

---

[8] FISA defines a "United States person" to include "citizens, aliens lawfully admitted for permanent residence, and United States corporations." *Muhtorov*, 2021 WL 5817486, at *6 n.4, *citing* 50 U.S.C. §1801(i).

[9] Warrantless backdoor searches were once prohibited by the government's minimization procedures, but the prohibition was lifted in the October 3, 2011, *2011 FISC Op.* *See* Ellen Nakashima, "Obama Administration Had Restrictions on NSA Reversed in 2011," *The Washington Post*, Sept. 7, 2013, available at http://wapo.st/1hP9FWm (the FISC "in 2008 imposed a wholesale ban on such searches at the government's request, said Alex Joel, civil liberties protection officer at the Office of the Director of National Intelligence (ODNI). The government included this restriction 'to remain consistent with NSA policies and procedures that NSA applied to other authorized collection activities,' he said. But in 2011, to more rapidly and effectively identify relevant foreign intelligence communications, 'we did ask the court' to lift

As the Second Circuit explained in its opinion in this case, "[d]ata 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*, 945 F.3d at 657, *citing PCLOB Report*, at 127. As the Court noted, "[c]olloquially, the parties (and those engaged in policy debates about the program) have referred to this querying capability as 'backdoor searches.'" *Id*., *citing PCLOB Report*, at 87.

The FBI's querying of immense Section 702 database(s) is pervasive and routine, and extends beyond national security investigations. As the *2018 FISC Op*. 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." *2018 FISC Op*., 402 F. Supp.3d at 80, *citing* 2016 FBI Minimization Procedures, §III.D, at 11.

According to those same minimization procedures, it is "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." *2018 FISC Op*., 402 F. Supp.3d, *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").

The *2018 FISC Op.* quoted a Supplemental FBI Declaration that asserted that "'[d]atabase

---

the ban, ODNI general counsel Robert S. Litt said in an interview. 'We wanted to be able to do it,' he said, referring to the searching of Americans' communications without a warrant").

In the present case, Mr. Hasbajrami's communications were purportedly intercepted during the period of April 2, 2011, through August 28, 2011, *see Hasbajrami*, 945 F.3d at 658. The government has yet to reveal whether the backdoor searches that were conducted in this case occurred during the time that such were categorically prohibited by the government's minimization procedures. If such was the case, it would present an additional ground for suppression.

queries are a critical tool,' and in one system during fiscal year 2017, FBI ran approximately 3.1 million queries 'against raw FISA-acquired information . . ., including section 702-acquired information.'" *2018 FISC Op.*, at 74-75. A "significant percentage" of those queries likely involved U.S. persons. *Id*., at 75.

Indeed, "[i]n 2017, NCTC [National Counterterrorism Center], the CIA, and NSA collectively used approximately 7500 terms associated with U.S. persons to query content information acquired under Section 702." *Muhtorov*, 2021 WL 5817486, at *87 n.29 (Lucero, J., *dissenting*), *citing 2018 FISC Op*., at 75. As a result, through Section 702, the government obtains the "full contents" of a wide range of electronic communications, and can sift through a vast storehouse for those by specific U.S. persons. *2018 FISC Op.*, 402 F. Supp.3d at 88.

In fact, during a 2015 FISC hearing (later declassified) before Judge Hogan, a government lawyer (whose name is redacted from the transcript) informed the Court that "[b]ecause these systems are queried on such a routine basis, these federated systems in some ways *are FBI's Google of its lawfully acquired information*." *In re [Redacted]*, (FISC) (TFH), Transcript of Proceedings Held Before the Honorable Thomas F. Hogan, October 20, 2015, at 34 (emphasis added), available at https://bit.ly/33tCztf. Indeed, the lawyer confirmed, "[t]hey are quite routine." *Id*.

The *2018 FISC Op*. also discussed "'categorical batch queries' (as opposed to queries conducted on the basis of individualized assessments)." *2018 FISC Op*., 402 F. Supp.3d at 53. Those "batch queries" were quite problematic, as the FISC noted that "many, though not all, recent misapplications of the querying standard by the FBI involved categorical batch queries." *Id*., at 83. Also, the "batch queries" process evaded supervisory control, and threatened to do so in the future: "More significantly, the Court is doubtful that in practice FBI personnel will consistently channel

categorical batch queries into §IV.A.3's approval process before they examine content information retrieved by those queries." *Id*.

Monitoring of the querying process during the relevant time period was also materially impaired, if not rendered ineffectual altogether, by FBI's refusal to require adequate and transparent records of queries of U.S. persons. Not only were the reasons for backdoor searches of U.S. persons' communications not recorded, but agents were not compelled to distinguish (in writing) backdoor searches of U.S. persons from those conducted on foreigners' communications. *2018 FISC Op*., 402 F. Supp.3d at 52-53, 67-68, 73-91. *See also id*., at 68-73 (describing limitations of FBI systems). Indeed, even after Congress in 2018 required the FBI to record the number of its U.S.-person queries in 2018, the agency failed to do so. *Id*.

In that environment, the queries of U.S. persons' communications circumvented Fourth Amendment protections by converting sweeping warrantless surveillance directed nominally at foreigners into a turbo-charged vehicle for investigating U.S. persons for ordinary criminal conduct. In fact, the President's Review Group recommended prohibiting the practice of backdoor searches, concluding that the practice violates the "full protection of [Americans'] privacy," *see* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 149, 145-50 (Dec. 12, 2013), available at https://bit.ly/3yWugSI ("*PRG Report*"). Also, in June 2014, the House of Representatives voted to prohibit such searches. *See* Charlie Savage, "House Votes to Curb NSA Scrutiny of Americans' Communications," *The New York Times*, June 20, 2014, available at http://nyti.ms/1vh2zti.

D. ***The Ambiguous State of the Factual Record Regarding Backdoor Searches Herein***

Here, as the Second Circuit 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*, 945 F.3d at 660. As a result, the 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 FISA court'bs issuance of Title I and Title III warrants with respect to Hasbajrami.' Order, *United States v. Hasbajrami*, Nos. 15-2684, 17-2669 (2d Cir. Sept. 4, 2018), ECF No. 203." *Id*. *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 fluid and elusive. At oral argument, the government, rather than directly answer the 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.[10]

But that is not the same as saying there was *no* backdoor search of Mr. Hasbajrami, and it may well obscure a number of factual scenarios – namely, when government agents used a backdoor

[10] During oral argument, at 50:50 the government was extremely cagey in its responses, avoiding answering directly the 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 record, which precipitated the Circuit's post-argument Order.

search but, in the government's narrow, unilateral view, its ultimate criminal case did not "arise" from that search. The government did not even purport to address how its queries of Mr. Hasbajrami's emails may have informed its other investigative efforts.[11]

Indeed, the Government's filing leaves open many possible scenarios in which the Government's evidence was derived from a backdoor search of Mr. Hasbajrami. For instance, the backdoor searches of Mr. Hasbajrami's communications could have contributed to investigative efforts wholly apart from the Title I and III FISA orders, including the government's Rule 41, Fed.R.Crim.P., warrants, orders (or warrants) pursuant to 18 U.S.C. §2703 (Stored Communications Act), grand jury subpoenas, and use of informants, all of which were avenues that spanned many months.[12]

Moreover, the government may be conflating the legal question of whether its criminal case

---

[11] *Muhtorov* is easily distinguished in this regard, as the Court therein, in concluding that the defendant was *not* subject to any Section 702 database querying, limited its analysis to "whether the collection of his communications violated the Fourth Amendment." *Muhtorov*, 2021 WL 5817486, at *12 (footnote omitted). *See also id*., at *13 ("[t]here is nothing in the record to support that evidence derived from queries was used to support the traditional FISA applications") (footnote omitted); *id*., at *14 ("Mr. Muhtorov's as-applied challenge thus begins and ends with whether the incidental collection of his Section 702 communications was constitutional").

[12] The dissent in *Muhtorov* structured the "derivative evidence" question(s) as follows:

> [W]as the decision to seek traditional FISA authority influenced by any querying of §702 databases by the FBI using identifiers associated with [the defendant]? Or by information collected in other intelligence surveillance programs? And if it was the result of querying of §702 databases, was the specific querying conducted reasonable under the Fourth Amendment under the facts of this case?

Muhtorov, 2021 WL 5817486, at *86 (Lucero, J., *dissenting*).

was "derived from" a backdoor search with the factual question of whether one occurred at all. The Circuit rejected the government's conclusory claim, requiring through its remand a far more detailed examination of how the FBI's investigation proceeded. Considering the government's previous extended concealment of the Section 702 interceptions altogether, *see* **ante**, at 8, the remand is abundantly prudent.

The government also made a new set of assertions at oral argument about whether its exploitation of Mr. Hasbajrami's emails occurred in "real-time." Oral Argument at 58:52. Those claims, too, are 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), with respect to its review of *Mr. 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."

If not in real-time, that review would more than likely be through a subsequent backdoor search. Indeed, the District Court's opinion made clear that the government obtained warrantless access to "many" of Mr. Hasbajrami's emails pursuant to Section 702 prior to any showing of probable cause, Dist. Ct. Op. at 24 (ECF #165), and those appear to include "historical emails" sent over "the months leading up to the initiation of the government's investigation," Government's Brief on Appeal (2d Cir. ECF # 130) ("Gov't Br."), at 5.

The government also pointed to its Brief, but that provided little concrete information about how and when FBI agents first encountered Mr. Hasbajrami's emails in their Section 702 databases, how long those emails had already been retained, or how long the FBI continued reviewing Mr.

Hasbajrami's emails without a warrant before seeking individual FISA orders. *See* Gov't Br., at 5-7.

The government has presented inconsistent timetables, but each nevertheless compels the conclusion that Mr. Hasbajrami was the subject of backdoor searches. For example, the initial Indictment (ECF # 1), alleges a time frame of "between June 1, 2010 and September 6, 2011[.]" *Id*., at 1. In its September 2011 motion to remand Mr. Hasbajrami the government alleged money transfers by Mr. Hasbajrami "[b]eginning in 2010," at 3, and/or Western Union transfers from December 2010 through February 2011. *See* Government's September 9, 2011, Memorandum of Law in Support of the Government's Motion for a Permanent Order of Detention, at 3, 4-5 (ECF # 3).

Since the government also reported that the surveillance was between April and September of 2011, *see* **ante**, at 6, 19 n.9, the earlier commencement strongly suggests a backdoor search that produced information from essentially a year earlier than April 2011. Indeed, there still remains the question whether the government gleaned information about Mr. Hasbajrami *exclusively* from querying and not merely from identifying Mr. Hasbajrami through incidental interceptions of other targets. Regardless, at no point has the government claimed that the evidence it obtained against Mr. Hasbajrami could have been discovered through an independent source wholly independent of the poisonous tree. *See* **post**, at 43-45.

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

> 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, 945 F.3d at 673 (emphasis added).[13]

E. *The Issues Identified by the Second Circuit for Resolution by This Court*

In the factual context set forth above, the Second Circuit's opinion identified a number of issues to be resolved upon remand. As a threshold matter, the Court recognized multiple times that

> What kinds of querying, subject to what limitations, under what procedures, are reasonable within the meaning of the Fourth Amendment, and when (if ever) such querying of one or more databases, maintained by an agency of the United States for information about a United States person, might require a warrant, *are difficult and sensitive questions*.

Hasbajrami, 945 F.3d at 672-73 (emphasis added). *See also id*., at 646 ("querying databases of stored information derived from Section 702-acquired surveillance also raises novel and difficult questions"); *id*., at 670 ("the storage and querying of information raises challenging constitutional questions, to which there are few dear answers in the case law"), *citing cf. In re Directives*, 551 F.3d at 1015; *Hasbajrami*, 945 F.3d at 670 (querying stored §702 data has "important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable").

---

[13] In contrast, again, *Muhtorov* is readily distinguishable, as the Court therein pointed out that "[t]he government affirmatively represents that "'the Section 702-derived evidence at issue was not obtained or derived from queries using terms associated with Muhtorov.' Aplee. Br. at 45." *Muhtorov*, 2021 WL 5817486, at *13. Thus, "'[t]he record therefore shows that the Section 702 information submitted to the FISC was not based on queries using terms associated with Muhtorov.'" Redacted Aplee. Suppl. Br. at 10-11." *Id.*

The Court did not "purport to answer them here, or even to canvass all of the considerations that may prove relevant or the various types of querying that may raise distinct problems." *Hasbajrami*, 945 F.3d at 673. Rather, the Court explained that "[q]uerying, depending on the particulars of a given case (such as what databases are queried, for what purpose, and under what circumstances), could violate the Fourth Amendment, and thus require the suppression of evidence[,]" and concluded that as an initial determination "a district court must ensure that any such querying was reasonable." *Id*., at 646.

As the Second Circuit emphasized,

> there is still an open issue as to what queries of Section 702-acquired information occurred in this case, whether any such queries were reasonable and, if unreasonable, whether the queried information tainted the application before the FISC or in some other way would lead to the suppression of any evidence.

Hasbajrami, 945 F.3d at 673.

The Circuit also dispensed with several of the government's arguments. For example,

> in its post-argument briefing, the government argues that even if it did query Section 702 databases, that action ultimately could not matter because the 80 communications collected as a result of incidental collection would provide an independent source sufficient to support the FISC's probable cause determination. Gov't Supplemental Classified Br. at 9 (arguing that "this Court's analysis should be limited to alleged 'searches' where a causal link can be drawn between the search and the acquisition of the evidence that Hasbajrami seeks to suppress.").

Hasbajrami, 945 F.3d at 673-74.

Yet the Second Circuit rejected the government's "independent source" rationale, declaring that it could not "do so on the sparse record presented" because the Circuit did "not know what databases were queried by whom, for what reasons, what (if any) information was uncovered by such

queries, or what (if any) use was made of any information uncovered." *Hasbajrami*, 945 F.3d at 672. *See also id*., at 674 ("[w]e cannot apply the independent source doctrine on the record currently before us").

Thus while "[t]he government has represented that no information derived from any such queries was presented to the FISC to obtain the FISA warrant," it had "not addressed whether any such information contributed to the investigation in other ways. [Redacted]" *Id*. *See also* **ante**, at 24 (providing examples of such uses). Ultimately, the Circuit articulated, "[w]hat is unclear is just how much Section 702-acquired information would remain, after further fact-finding at the district court." *Id*., at 675.

Consequently, as the Second Circuit concluded, "[g]iven these considerations, the district court here must conduct an inquiry into whether any querying of databases of Section 702-acquired information using terms related to Hasbajrami was lawful under the Fourth Amendment." *Id*. The Second Circuit could not, "and should not, go further, pending development of a more complete record by the district court on remand, and an assessment by the district court as to whether whatever was done was consistent with the Fourth Amendment and whether, if there was any illegality, any evidence should have been suppressed in response to Hasbajrami's motion." *Id*., (footnote omitted).[14]

---

[14] Likewise, the Second Circuit left it "to the district court to determine, in the first instance, whether any exceptions to the exclusionary rule, such as a good faith exception, might apply in this case." *Hasbajrami*, 945 F.3d at 676 (footnote omitted). Similarly, the Second Circuit delegated to this Court the initial determination whether, "if any evidence should have been suppressed, [] the failure to suppress that evidence was harmless, and if it was not what remedy is appropriate." *Id*., at 676-77. Mr. Hasbajrami defers analysis of those issues pending the government's assertion that any particular Fourth Amendment exception (and/or harmless error) applies, although it is noted that *the good faith exception is not available for illegal FISA surveillance*. *See* 50 U.S.C. §1806(g).

The Second Circuit also endowed this Court with maximum flexibility in conducting its fact-finding review and legal analysis: "[o]n remand, the district court should undertake whatever proceedings are necessary, consistent with the considerations stated above." *Hasbajrami*, 945 F.3d at 677.

F. *Disclosure to Security-Cleared Defense Counsel*

That discretion expressly included disclosure of the underlying factual material (and certain legal arguments) to security-cleared defense counsel:

> To the extent that any decisions must be made about what information is to be presented to appropriately-cleared defense counsel, such decisions too are best left to the district court after it becomes clear what the inquiry about querying will involve. *Cf.* [*United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010)] (noting that, under FISA, disclosure is exception and *ex parte*, in camera review is the rule, and that the review of materials that are "relatively straightforward and not complex" may not necessarily require adversarial testing).

Hasbajrami, 945 F.3d at 677 (footnote omitted).

As a result, the Second Circuit denied "without prejudice to renewal before the district court on remand" Mr. Hasbajrami's motion for disclosure (to security-cleared counsel) of certain classified materials, including redacted portions of Judge Gleeson's opinion, the government's Rule 28(j) letter in the Circuit, and redacted portions of the Circuit's opinion "consistent with the requirements of CIPA and FISA." *Hasbajraim*, 945 F.3d at 677 n. 24. Therefore, "the district court remains free to consider[]" the motion "in the first instance[.]" *Id.*[15]

[15] The government's Rule 28(j), Fed.R.App.P. letter, dated December 21, 2018, to which the Circuit referred, was filed by the government *ex parte,* thereby raising the very distinct prospect that the government filed a supplementary authority, perhaps even a FISC opinion – indeed, the *2018 FISC Op.* was issued October 18, 2018, in classified form but not declassified until well afterwards – without providing security-cleared defense counsel access to legal

ARGUMENT

POINT I

THE COURT SHOULD ORDER THE GOVERNMENT TO DISCLOSE TO SECURITY-CLEARED DEFENSE COUNSEL THE MATERIALS THE GOVERNMENT PROVIDES TO THE COURT IN CONNECTION WITH THE PROCEEDINGS ON REMAND, AND ULTIMATELY GRANT MR. HASBAJRAMI'S MOTION TO SUPPRESS

In remanding, the Second Circuit expressly concluded that Section 702 queries targeting information regarding U.S. persons constituted Fourth Amendment events independent of the initial incidental interception of the underlying communications. *See Hasbajrami*, 945 F.3d at 670 (government's querying of a U.S. person's communications intercepted pursuant to Section 702 constitutes a "separate Fourth Amendment event" that must independently satisfy constitutional requirements).

That conclusion was imperative: when government law enforcement or intelligence personnel query the retained intercepted communications of a U.S. person pursuant to Section 702, the authority for the initial interception is quite attenuated. Indeed, at that juncture, not only has the target of the surveillance ostensibly changed, but the nature and degree of the intrusion on protected communications has also been transformed.

As the Supreme Court has recognized in a variety of contexts – including digital searches – a search that relies on an exception to the warrant requirement is strictly limited by its original justification. *See, e.g., Terry v. Ohio*, 392 U.S. 1, 19 (1968); *Riley v. California*, 573 U.S. 373, 400-401 (2014); *see also Hasbajrami*, 945 F. 3d at 670-71 (reviewing cases). Authority to intrude

---

arguments the government was making to the Circuit. *See* ECF # 230 (government's December 21, 2018, letter providing public notice of filing).

further requires new and independent approval. *See Riley*, 573 U.S. at 404.

Thus, the Second Circuit assigned to this Court the task of determining whether the government's queries in its investigation of Mr. Hasbajrami violated the Fourth Amendment, and therefore require suppression of all evidence derived from those queries. As set forth below, that evaluation requires not only identification of relevant Fourth Amendment principles, but also analysis of the scope and mechanisms of the querying system with respect to Section 702 databases.

A. *Applicable Fourth Amendment Principles and Jurisprudence*

Here, while the Second Circuit upheld the constitutionality of *initial* warrantless surveillance/collection pursuant to Section 702 (*i.e.*, the "incidental" interception aspect of surveillance program itself), it did not decide whether *later* backdoor searches would still require a warrant, or be reasonable under the Fourth Amendment.

1. *The Warrant Requirement Applies to Section 702 Backdoor Queries*

The first insuperable obstacle to the constitutional validity of any querying in this case is that such queries were conducted without a warrant. As the Second Circuit intimated, and other cases have held in analogous circumstances, querying in the Section 702 context requires a warrant. As a result, the warrantless querying in this case violated the Fourth Amendment.

In discussing Section 702 querying, the Circuit observed that "[t]he Supreme Court has expressed increasing concern about the interaction between Fourth Amendment precedent and evolving government technological capabilities. *Riley* rested in part on the fact that '[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals.' 573 U.S. at 386 []." *Hasbajrami*, 945 F.3d at 671.

Therefore, because of the scope and layers of information accessible in the digital environment, "[a] search of the information on a cell phone [therefore] bears little resemblance to the type of physical search considered" in past cases." *Id*. [second brackets in original], *also citing United States v. Ganias*, 824 F.3d 199, 217-18 (2d Cir. 2016) (*en banc*) (noting privacy implications of expansive technology and data storage).[16]

The Second Circuit added that in *Carpenter v. United States*, ___ U.S. ___, 138 S. Ct. 2206 (2018), in which the Supreme Court held that a warrant (rather than merely a Court order pursuant to 18 U.S.C. §2703(d) obtained under a standard less than probable cause) was required to gain access to databases containing cell-site location information ("CSLI"), "the Court concluded that a warrant (or a valid substitute) was required to acquire cell-site records, even though they were stored by a third party and under traditional Fourth Amendment doctrine a cellphone user would not have an expectation of privacy in such information[.]" *Hasbajrami*, 945 F.3d at 671.[17]

---

[16] As the dissent in *Muhtorov* reasoned, "If anything, the Fourth Amendment questions posed by §702 are even greater than those addressed in *Riley* because §702 communications may legally be seized without any showing of probable cause, reasonable suspicion, or even any suspicion of criminal activity." *Muhtorov*, 2021 WL 5817486, at *88 (Lucero, J., dissenting).

[17] As *Machtinger* points out, warrantless querying of Section 702 databases has been the subject of controversy and criticism even inside government:

> Both Executive Branch and congressional personnel have flagged the lack of a warrant requirement for incidentally collected U.S. person communication as a cause for concern. President Obama's Review Group on Intelligence and Communications Technologies recommended that "it should take either a law enforcement or FISA judicial order to query the database. . . . [T]here should at least be a judge involved before there is access to the contents of U.S. person communications."[] One draft bill in Congress would have "[r]estrict[ed] law enforcement from using information obtained or derived from warrantless surveillance except when investigating the most serious crimes, like murder."[] The

In *Carpenter*, the Supreme Court explained that it "decline[d] to grant the state unrestricted access to a wireless carrier's database of physical location information[] because,

> [i]n light of the deeply revealing nature of [this information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.

Carpenter, 138 S. Ct. at 2223.[18]

Accordingly, "[t]he Government's acquisition of the cell-site records here was a search under that Amendment." *Id*. *See also Hasbajrami*, 945 F.3d at 671-72 (quoting the entire passage). Thus, the Court in *Carpenter* rejected any exception for *post hoc* searches of databases in which the resident information was obtained absent any Fourth Amendment violation.

Critically, in *Carpenter* the Court distinguished certain government conduct that mirrors the issues presented here. For instance, the Court did *not* "consider other *collection* techniques

---

> *Hasbajrami* case provides the opportunity for the judiciary to address the issues as a matter of constitutionality.

Machtinger, at 2. Indeed, debate regarding the parameters of Section 702 querying, and the prerequisites for such searches, complicated and ultimately stalled Congressional action with respect to renewal of certain FISA authorities. *See, e.g.*, Charlie Savage, "Surveillance and Privacy Debate Reaches Pivotal Moment in Congress," *The New York Times*, Jan. 10, 2018, available at https://nyti.ms/3E5Axw6 ("[a] yearslong debate over National Security Agency surveillance and protections for Americans' privacy rights will reach a climactic moment on Thursday as the House of Representatives takes up legislation to extend a program of warrantless spying on internet and phone networks that traces back to the Sept. 11 attacks"); Faiza Patel, "The 702 Reform Debate Is Just Heating Up," *Just Security*, May 16, 2016, available at https://bit.ly/3sbF4uw (a recent "hearing exposed key differences between those who believe that Section 702 should be narrowed . . . and those who believe that Section 702 should be reauthorized in essentially its current form").

[18] *Carpenter* has been characterized as "one of this generation's most important Fourth Amendment opinions." Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J. FORUM 943, 943 (Apr. 1, 2019) (other citations omitted).

involving foreign affairs or national security," but instead focused on the querying, extracting, and reviewing of CSLI held in third-party storage sites. *Carpenter*, 138 S. Ct. at 2220 (emphasis added).[19]

The Court in *Carpenter* concluded that access to "[t]he location information obtained from Carpenter's wireless carriers was the product of a search." *Id*., at 2217. As it recognized, just as with Section 702 databases – which are searched for purposes of ordinary criminal investigations, *see* **post**, at 51 – "[w]ith just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense," *id.*, at 2217-18, thereby discovering "cell phone location information [that] is detailed, encyclopedic, and effortlessly compiled." *Id.*, at 2216.[20]

In *Carpenter*, the Supreme Court recognized that reasoning applied to emails as well by citing *United States v. Warshak*, an opinion in which the Sixth Circuit noted: "[b]y obtaining access to someone's email, government agents gain the ability to peer deeply into his activities[.]" *Id.,*

---

[19] The mere fact that Section 702 initially targets the communications of non-U.S. persons has never before been sufficient reason to jettison the warrant requirement that protects U.S. persons' electronic communications – neither in criminal investigations nor foreign intelligence investigations. *See* Orin Kerr, "The Surprisingly Weak Reasoning of Mohamud," *Lawfare*, Dec. 23, 2016, available at https://bit.ly/2PfkPWx. This Court should not embrace such a novel exception here, which would license a sweeping end-run around U.S. persons' Fourth Amendment rights. As with other types of electronic searches, it is reasonable and practicable to require the Government to obtain an individualized court order when it seeks to retain and use communications that it knows are protected by the Fourth Amendment.

[20] In *Carpenter*, the Court reasoned that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 138 S. Ct. at 2214 (*quoting Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010). *See also Muhtorov*, 2021 WL 5817486, at *84 (Lucero, J., dissenting) ("I would not blind myself to the constitutional implications raised by a 'vast body of information' that may be 'simply stored in a database, available for review by request from domestic law enforcement agencies solely on the speculative possibility that evidence of interest to agents investigating a particular individual might be found there'"), *citing Hasbajrami*, 945 F.3d at 670.[21]

The Court in *Carpenter* was concerned – again quite pertinent here – that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable . . ." and enabling the government to "travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers . . ." *Id.*, at 2218. As the Court declared, under such circumstances, "the Government's obligation is a familiar one – get a warrant." *Id.*, at 2221.[22]

Accordingly, querying a Section 702 database requires a warrant.[23]

---

[21] *See also Carpenter*, 138 S. Ct. at 2222, (*quoting Warshak*, 631 F.3d at 283-88 ("[i]f the third-party doctrine does not apply to the 'modern-day equivalents of an individual's own 'papers' or 'effects,' then the clear implication is that the documents should receive full Fourth Amendment protection")).

[22] In *Carpenter*, the Court recognized that exigent circumstances, such as "the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence . . . [along with] bomb threats, active shootings, and child abductions," may allow law enforcement to circumvent the warrant requirement for CSLI queries. *Id.*, at 2223. *See also Riley*, 573 U.S. at 73, *citing Missouri v. McNeely*, 569 U.S. 141, 149 (2013) (providing two examples of exigent circumstances as "a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone). However, in *Carpenter*, the FBI's investigation of nine armed robberies and its urgency to identify all of the accomplices was not exigent. *Carpenter*, 138 S. Ct. at 2212. Here, notably, the government has not at any point suggested its warrantless querying was motivated by any exigency.

[23] One commentator, in analyzing the Second Circuit's opinion herein, suggests that "*Carpenter* provides a window into how the Supreme Court thinks about the constitutional

2. *The Querying Procedures As a Whole Should Be Examined to Determine if They Satisfy Fourth Amendment Standards*

The querying procedure itself – as a precursor to examination of the specific querying in this case – should also be evaluated for Fourth Amendment reasonableness as a threshold issue. That approach conforms with how the FISC approves querying: not on a fact-specific or case-by-case basis, but based on the querying procedures themselves for the upcoming year. Thus, even though each query is a separate Fourth Amendment event, the querying framework itself must pass constitutional muster.

As the FISC has repeatedly acknowledged, the querying rules are an important element of the constitutional analysis. *See, e.g., 2017 FISC Op.*, at 15-18 (describing prohibition on U.S.-person queries of Upstream information). *See also 2020 FISC Op.*, at 6 ("the [targeting, querying, and minimization] procedures as a whole must be consistent with statutory and constitutional requirements").

The procedures regulating access to Section 702 databases raise fundamental Fourth Amendment questions. As the Second Circuit cautioned herein,

> If such a vast body of information is simply stored in a database, available for review by request from domestic law enforcement agencies solely on the speculative possibility that evidence of interest to agents investigating a particular individual might be found there, the program begins to look more like a dragnet, and a query more like a general warrant, and less like an individual officer going to the

---

implications of bulk data collection." *See Machtinger*, at 2. While "[i]gnoring *Carpenter* in deciding *Hasbajrami* might make sense under a narrow reading of *Carpenter*, which focuses solely on CSLI, [] *dicta* from *Carpenter* about applying the Fourth Amendment in the era of modern technology may support a more robust constitutional analysis of incidental collection under Section 702." *Id.* (footnote omitted). Thus, "[w]hile *Carpenter*'s *dicta* are non-binding, they may provide insight into how the Supreme Court might address other forms of bulk data collection, like the collection in *Hasbajrami*, in the future." *Id.*

> evidence locker to check a previously-acquired piece of evidence against some newfound insight.

Hasbajrami, 945 F.3d at 671. *See also Machtinger*, at 14 ("the court expressed some concern about the breadth, comprehensive reach, and automatic nature of Section 702," and "seemed to seriously consider that querying should receive greater Fourth Amendment protection than it currently does") (footnotes omitted); *Muhtorov*, 2021 WL 5817486, at *84 (Lucero, J., dissenting) (noting "the thorny constitutional issues that querying presents").

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).

Acutely conscious of these basic constitutional tenets, the Court "ha[s] recognized only limited circumstances in which the usual rule does not apply." *Edmond*, 531 U.S. at 37. In accordance with that principle, the Supreme Court has consistently determined that government programs that authorize its agents to conduct *seizures* – such as those attendant to vehicle checkpoints – without "the appropriate quantum of particularized suspicion," must pass Fourth Amendment muster. *Id*., at 34-5. *See also Muhtorov*, 2021 WL 5817486, at *88 n.32 (Lucero, J., dissenting) ("[a]s the court held in *Riley*, mere seizure does not authorize search of contents").

In addition, "[w]hile reasonableness under the Fourth Amendment is predominantly an objective inquiry, [the Court's] special needs and administrative search cases demonstrate that purpose is often relevant when suspicionless intrusions pursuant to a general scheme are at issue." *Edmond*, 531 U.S. at 47 ("a checkpoint program whose primary purpose was to detect evidence of

ordinary criminal wrongdoing" is not sufficient to justify suspicionless seizures of private citizens). *Cf. Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 450 (1990) (curbing drunk driving was a pressing enough state interest to justify the brief "suspicionless seizures" that occur at checkpoints); *United States v. Martinez-Fuerte*, 428 U.S. 543, 545 (1976) ("[i]nterdicting the flow of illegal entrants from Mexico poses formidable law enforcement problems," thus justifying a brief seizure at a permanent checkpoint to ascertain immigration status).

In determining whether such programs are designed consistent with the Fourth Amendment, "the Court examine[s] the government interests advanced to justify such routine intrusions 'upon the constitutionally protected interests of the private citizen,'" to determine whether "under the circumstances the government interests outweighed those of the private citizen." *Martinez-Fuerte*, 428 U.S. at 561, *citing Camara v. Municipal Court*, 387 U.S. 523 (1967).

However, in checkpoint cases, the Court emphasized that it examines government programs or actions involving *searches*[24] with a much more stringent standard than that of the *seizures* discussed above. *See Martinez-Fuerte*, 428 U.S. at 561 ("the [use of the balancing test] is appropriate here, where we deal neither with searches nor with the sanctity of private dwellings, ordinarily afforded the most stringent Fourth Amendment protection"). Indeed, the Court has "held that checkpoint searches are constitutional only if justified by consent or probable cause to search." *Id*., *citing United States v. Ortiz*, 422 U.S. 891 (1975).

---

[24] "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter*, 138 S. Ct. at 2213, *citing Smith v. Maryland*, 442 U.S. 735, 740 (1979).

Here, the immense breadth of the Government's collection under Section 702, described **ante**, at 8-19, coupled with its ability to query the resulting databases for the emails of U.S. persons like Mr. Hasbajrami, is the initial subject for review. *Compare In re Directives*, 551 F.3d at 1015 ("Government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons").

Accordingly, the Section 702 querying program as a whole – again, an issue of first impression outside the *ex parte* context of the FISC – is ripe for review to determine whether or not it violates the Fourth Amendment.

3. *Even if the Warrant Requirement Does Not Apply, Section 702 Backdoor Queries Must Satisfy the Fourth Amendment's "Reasonableness" Requirement*

Even if, assuming *arguendo*, a warrant is not required to conduct a Section 702 query, such a search must still be reasonable under Fourth Amendment jurisprudence. As the Circuit explained in its opinion, "[f]or today we need only reiterate that 'the ultimate touchstone of the Fourth Amendment is reasonableness.'" *Hasbajrami*, 945 F.3d at 672, (*quoting Riley*, 573 U.S. at 381, and *cf*. *Abu-Jihaad*, 630 F.3d at 121-22).

It is well settled that the reasonableness of electronic surveillance is evaluated under "the totality of the circumstances" – which includes the breadth and volume of the information/communications intercepted, as well as the rules dictating how those sensitive communications may be acquired, retained, and used. *See, e.g., In re Directives*, 551 F.3d at 1012; *2011 FISC Op.*, at *27-28. In FISC proceedings, the government has conceded that the querying rules bear directly on reasonableness. *See [Redacted]*, Mem. Op. at 40 (FISA Ct. Nov. 6, 2015), available at bit/ly/3487WWE. *See also Muhtorov*, 2021 WL 5817486, at *24.

The reasonableness standard is well-defined for electronic surveillance: courts consider the adequacy of procedures regulating the government's intrusions into privacy, including the strength or weakness of the applicable minimization protocols. *See, e.g., Berger v. New York*, 388 U.S. 41, 58 (1967); *In re Sealed Case*, 310 F.3d 717, 737-41 (FISA Ct. Rev. 2002); *United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir. 1984) (analyzing "the procedures fashioned in FISA"); *2018 FISC Op.*, 402 F. Supp. 3d at 75 (explaining that "the rules for U.S.-person queries are especially important for minimization of Section 702 information").

Also, because electronic surveillance presents "inherent dangers" of overbreadth, *see Berger*, 388 U.S. at 60, the lawfulness of particular surveillance depends on the safeguards attendant to the acquisition, retention, and use of the private information the government intercepts. *See In re Directives*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *2011 FISC Op.*, at *27-28. The querying rules go to the heart of this analysis because, as the Circuit and the FISC have recognized, they pose a considerable threat to the privacy of U.S. persons' electronic communications. *See Hasbajrami*, 945 F.3d at 672 ("[t]reating querying as a Fourth Amendment event and requiring the query itself to be reasonable provides a backstop to protect the privacy interests of United States persons and ensure that they are not being improperly targeted"); *2018 FISC Op.*, 402 F. Supp. 3d at 87 ("[t]he Court regards *the privacy interests at stake as substantial*") (emphasis added).

Indeed, 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." *2018 FISC Op*. 402 F. Supp.3d at 87.

Similar to the *Carpenter* Court's concern about the sheer amount of CSLI being stored and queried,[25] the Second Circuit herein noted "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." *Hasbajrami*, 945 F.3d at 671.

The requisite evaluation entails an objective analysis that examines the breadth of the search and the restrictions on how the government may exploit the resulting information; it is not controlled by *post hoc* claims regarding which of the intercepted communications the government ultimately intends to rely on at trial. *See Berger*, 388 U.S. at 60 (examining defects in the statutory procedures).

4. *Suppression Necessarily Encompasses the "Fruit of the Poisonous Tree"*

The "fruit of the poisonous tree" doctrine requires suppression whenever the tainted search or seizure played a direct or indirect role in developing an investigation and evidence. The Second Circuit made application of that principle quite clear in this case in various parts of its opinion.

---

[25] The Court in *Carpenter* repeatedly highlighted the sheer number of people, devices, and discreet communications collected, stored, and potentially queried over a significant period of time – a factor relevant to the massive scale of communications collected in the national security realm. *See, e.g.,* 138 S. Ct. at 2218 ("[c]ritically, because location information is continually logged for all of the 400 million devices in the United States – not just those belonging to persons who might happen to come under investigation – this newfound tracking capacity runs against everyone"); *id*., at 2219 ("[t]he Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years").

As the Circuit recognized, the government's argument on appeal – that it could restrict the analysis to whether any of the specific information gleaned from backdoor searches itself constituted projected trial evidence – did not correctly state the standard. *See Hasbajrami*, 945 F.3d at 672-74. *See also* **ante**, at 26.

Rather, evaluating broad electronic searches, like wiretaps, courts consider even those aspects of the intrusion – from acquisition, to retention, to use – that do not yield evidence as tainting the fruits that are used as evidence. That is not a piecemeal exercise that depends on tracing each defect in the surveillance to the government's evidence at trial. *Id*. *See also United States v. Suggs*, 998 F.3d 1125, 1142 (10th Cir. 2021) ("this so-called 'fruit of the poisonous tree' doctrine does not demand a particularly tight causal chain between the illegal search and the discovery of the evidence sought to be suppressed").

In fact, as the Second Circuit has directed here, the Supreme Court has expressly held that, when evaluating broad electronic searches, a court must consider even those aspects of the intrusion that do *not* lead to evidence at trial. In *Scott v. United States*, 436 U.S. 128 (1978), the Supreme Court weighed, 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." *Scott*, 436 U.S. at 142-43. *See also, e.g.*, *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).

Similarly, in *Berger*, once the Supreme Court observed that the petitioner "clearly ha[d] standing to challenge" the wiretap statute at issue because he was "indisputably affected by it[,]"

Berger, 388 U.S. at 55, the Court examined numerous defects in the statutory wiretap procedures without regard to whether those particular flaws directly affected the government's evidence at trial. *See id*. at 55, 58-60.

The "fruit of the poisonous tree" doctrine compels an exhaustive review of the sources of the government's information and ultimate evidence. *See, e.g., Wong Sun v. United States,* 371 U.S. 471, 486-88 (1963) (articulating "fruit of the poisonous tree" doctrine, under which court must examine whether evidence was "come at by the exploitation" of an unlawful search); *Murray v. United States*, 487 U.S. 533, 536-37 (1988) (describing right to seek suppression of evidence "derived" from an unlawful search).[26]

As the Supreme Court instructed in *Alderman v. United States*, 394 U.S. 165 (1969), in the context of electronic surveillance, the examination is particularly fact-intensive. *Id*., at 168, 180-85. That scrutiny should be even more exacting here given the government's consistently penurious interpretation of what it means for evidence to be "derived" from its electronic surveillance. *See, e.g*., Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?" *Just Security*, December 11, 2015, available at https://bit.ly/32eUu70.

Nor has the government even publicly provided its definition of "derived," which accords it unwarranted flexibility in avoiding disclosure and, ultimately, suppression. The government's resistance to transparency further reinforces the indispensability of adversarial participation and litigation in the process, as detailed **post**, at 82-103.

---

[26] As detailed **post**, at 82-96, an informed decision with respect to this issue is not arrived at *ex parte*. *See Alderman v. United States*, 394 U.S. 165, 168, 180-85. (1969).

Also, limiting Fourth Amendment analysis to whether the intrusion into privacy produced trial evidence would essentially turn the prohibition against general warrants on its head, as innocuous or non-pertinent communications would not be relevant to the determination – yet it is the collection, retention, and use of those very communications that is protected most.[27]

That approach is appropriate because searches of electronic/digital information and communications are often expansive, enabling the government to seize large amounts of private information that is unrelated to the government's investigation. *See Ganias*, 824 F.3d 217-18. While the *en banc* Court in *Ganias* relied on the "good faith" exception in reversing the panel's opinion, it cautioned,

> [W]e offer no opinion on the existence of a Fourth Amendment violation in this case, we make some observations bearing on the reasonableness of the agents' actions, both to illustrate the complexity of the questions in this significant Fourth Amendment context and to highlight the importance of careful consideration of the technological contours of digital search and seizure for future cases.

Ganias, 824 F.3d at 209.

In that context, the *en banc* Court in *Ganias* elaborated that it wanted to "highlight the complexity of the relevant questions for future cases and to underscore the importance, in answering such questions, of engaging with the technological specifics." *Id*., at 217 (footnote omitted). *See also id*., at 220 (noting that a full record is required to adjudicate the "complex and rapidly evolving technological issues, and the significant privacy concerns, relevant to its consideration") (footnote omitted). *See also* Andrew Guthrie Ferguson, Professor of Law, UDC David A. Clarke School of

---

[27] The Ninth Circuit in *Mohamud* did not examine this question; nor was it ever briefed. *Mohamud*, 843 F.3d at 438. Also, as noted **ante**, at n.13, the Court in *Muhtorov* expressly declined any issue related to querying.

Law (Reporter), *The Fourth Amendment in the Digital Age*, National Association of Criminal Defense Lawyers Symposium, available at https://bit.ly/3ISspCJ; Peter A. Crusco, "Email Account Seizures and Retention of Large Digital Records," *New York Law Journal*, June 28, 2016, available at https://bit.ly/3oXWOaY ("[t]he issue of voluminous digital searches calls into question the particularity doctrine of the Fourth Amendment").

B. ***The Querying System In 2011 and the Querying In This Case Were Likely Unreasonable***

The querying system that permits backdoor searches has transformed Section 702 into a systematic tool for untrammeled, and heretofore unreviewable warrantless review of the private electronic communications of U.S. persons like Mr. Hasbajrami, and investigations of those persons for any manner of potential offenses. Whether in its structure, or specifically as applied to Mr. Hasbajrami, the Section 702 querying is unreasonable by Fourth Amendment standards.

Certainly the public record compels a presumption that during the time period at issue herein – 2010-2011 – the government was *not* in compliance with FAA or FISA in a number of critical and relevant aspects. In August 2013 the government began releasing declassified versions of a series of FISC opinions, continuing through 2021, that have catalogued the abuses and transgressions – exceeding the authority granted by the FISC – the government committed in the course of implementing Section 702 programs and surveillance/acquisition.

Most recently, FISC opinions in 2018 and 2020 provided an illuminating window into the mechanics of Section 702 querying, and its unreasonableness under the Fourth Amendment. In the *2018 FISC Op.*, for example, the FISC reaffirmed that "[t]he government is not at liberty to do whatever it wishes with those U.S.-person communications, notwithstanding that they are 'incidental

collections occurring as a result of' authorized acquisitions." *2018 FISC Op.*, 402 F. Supp.3d at 87, (*quoting In re Directives*, 551 F.3d at 1015).

As the FISC pointed out, "[t]he FISCR in *In re Directives* relied on the government's assurance 'that it does not maintain a database of incidentally collected information from non-targeted United States persons' when it held on the facts of that case that 'incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.'" *Id.*

Yet that is not necessarily the case any longer (if it ever was an accurate representation). As the FISC recognized, "while the FBI may not maintain a separate database of U.S.-person communications acquired under Section 702, it routinely queries raw Section 702 data in order to identify and examine communications of particular U.S. persons." *Id.*[28]

In turn, the FISC reasoned, "[w]hether those querying practices adequately protect the privacy of those U.S. persons, or instead unjustifiably invade U.S. persons' privacy, bears on the analysis of reasonableness under the Fourth Amendment." *Id.*, *citing In re Certified Question*, 858 F.3d 591, 609 (FISA Ct. Rev. 2016) (*per curiam*) (examining intra-FBI restrictions on access to information acquired pursuant to a FISA pen register/trap-and-trace authorization as part of assessment of Fourth Amendment reasonableness).

1. *The Routine and Extraordinarily Expansive Scope of Section 702 Querying*

Section 702 querying is not treated as an extraordinary procedure. Rather, it is the default. As the FISC reported, the "FBI encourages its personnel to make maximal use of queries – provided

[28] The FISC added that "[t]he large number of U.S.-person queries run by the FBI makes its querying practices significant, despite its receiving only a small percentage of the total information acquired under Section 702." *2018 FISC Op.*, 402 F. Supp.3d at 75.

they are compliant with the FBI's minimization procedures and other applicable law – in order to perform their work." *2018 FISC Op*., at 80.

Querying is also implemented as a *first* resort at the start of the investigative process: "it is '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.'" *Id*., (*quoting* 2016 FBI Minimization Procedures §III.D at 11 n.3). *See also id*., (*quoting* a Supplemental FBI Declaration (submitting to the FISC), at 6 ("FBI uses queries, among other reasons, 'to quickly determine whether a new tip or lead . . . warrants opening an investigation, is related to an existing investigation,' or requires no further action")).

The standard is *not* probable cause, but instead far more elastic: "there must be 'a reasonable basis to expect [it] will return foreign intelligence information or evidence of crime.'" *2018 FISC Op*., at 76. Nor did the querying rules impose any accountability. As discussed **post**, at 53-54, the FBI did not even require agents to memorialize the bases for targeting a U.S. person through a backdoor search. *2018 FISC Op*., at 52-53, 79.

The absence of such a fundamental requirement made effective oversight difficult, if not impossible. *Id*. As a result, without any articulable demonstration of suspicion, an FBI agent could enter in the datebase(s) a U.S. person's name, email address, or telephone number, and retrieve whatever trove of communications Section 702 has vacuumed into its collection during the prior five years. Queries thus represented a free pass for accessing protected communications that, otherwise, would be inaccessible without a warrant or probable cause.

Other aspects of Section 702 queries distinguish them from any traditional review of electronic interceptions. For instance, the majority of Section 702 interceptions are not manually

reviewed, in real-time or otherwise. *See PCLOB Report* 128-129 ("NSA analysts do not review all or even most communications").

As the Second Circuit and the FISC have pointed out, that is not surprising considering the billions of communications stored for years; therefore, many communications would never be examined by an agent absent a backdoor search. *See Hasbajrami*, 945 F.3d at 671; *2018 FISC Op*., at 75. *See also United States v. Jones*, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., *concurring*) (28-day long GPS monitoring of defendant's movements was, for Fourth Amendment purposes, qualitatively different than ordinary visual surveillance); *id*., at 429-30 (Alito, J., concurring).[29]

Also, a Section 702 query is comprehensive. While an agent might review a small subset of communications in the course of pursuing a foreign target, a backdoor search is a deliberate effort to retrieve *all* of a U.S. person's communications resident in the Section 702 databases. *See Hasbajrami*, 945 F.3d at 672 ("querying is problematic because it may make it easier to target wide-ranging information about a given United States person"). *See also Muhtorov*, 2021 WL 5817486, at 88 n.31 (Lucero, J., dissenting) ("[t]he 250,000,000+ communications that are collected annually under §702, however, are not documented in real time. Instead, they are stored, often without processing, in vast lakes of data, and their contents are most often obtained through querying"), *citing PCLOB Report*, at 59, 116.

In that context, in applying Section 702 programmatic electronic surveillance, the government targets not only individuals, "but also groups, entities, associations, corporations, or

[29] The formal ground for the principal ruling in *Jones* was that a trespass had occurred. However, even the plurality opinion acknowledged that "[i]t may be that achieving the same [tracking] result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." *Jones*, 565 U.S. at 412.

foreign powers." *PCLOB Report*, at 20-21. Thus, an entire foreign government can constitute a single target. *Id.* Moreover, for each targeted individual or group, the government may monitor any and all "selectors" – phone numbers, email addresses, IP addresses, or other identifiers – that it believes are associated with the target. *See* Charlie Savage, et al., "Hunting for Hackers, NSA Secretly Expands Internet Spying at U.S. Border," *The New York Times*, June 4, 2015, available at nyti.ms/2RfT9Us.[30]

Some of the selectors may be used by hundreds of different people, and because the threshold for targeting is so low, the number of surveillance targets ballooned to more than 200,000 annually by 2019. *See* **ante**, at 14. Every single communication between a U.S. person and one of these individuals or groups is collected and stored in the government's databases, and accessible via querying.

2. *The History of Non-Compliance and Abuse of Section 702 Querying Authority*

The history of government – whether DoJ or FBI or NSA – non-compliance with even the relaxed strictures imposed by FISA is too voluminous and multifaceted to present herein. Even the comprehensive review below represents only a fraction of the abuses that have continually invaded the privacy of U.S. persons in manners that exceed either or both statutory or 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

[30] The Fourth Amendment's protections do not depend on whom the goverment purports to be "targeting." They turn on what it is searching. *See* Orin Kerr, "The Surprisingly Weak Reasoning of *Mohamud*," *Lawfare* (Dec.23, 2016), available at bit.ly/2PfkPWx ("there is no 'targeting' doctrine in Fourth Amendment law").

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).

Certainly, as a whole, the FISC's opinions show how a surveillance program ostensibly designed to monitor, intercept, and collect hundreds of thousands of foreign "targets" has been engineered to afford law enforcement and intelligence agents functionally bruntrammeled access to the communications of U.S. persons, which communications would otherwise be inaccessible absent a warrant.

As the FISC revealed in its 2020 opinion, queries "had been conducted in support of predicated criminal investigations relating to health-care fraud, transnational organized crime, violent gangs, domestic terrorism involving racially motivated violent extremists, as well as investigations relating to public corruption and bribery." *2020 FISC Op*., at 42.[31] Yet, as the FISC pointed out, "[n]one of these queries was related to national security, and they returned numerous Section 702-acquired products in response." *Id*. (citation omitted); *see also 2018 FISC Op*., at 75 ("FBI queries intended to retrieve evidence of crime may be conducted in the course of law-enforcement investigations that are unrelated to national-security threats").[32]

---

[31] An exception, at 50 U.S.C. §1881a(f)(2)(E), with extraordinarily latitude permits access to Section 702 databases if the FBI believes the results "could assist in mitigating or eliminating a threat to life or serious bodily harm."

[32] In its annual report to the FISC regarding the volume of queries used in connection with investigation of non-national security offenses, FBI reported one such incident in 2019, but in its 2020 report amended that number to 91 such instances for 2019, although "[t]he real number was probably larger; the report said it counted all queries by a single persona on a single day as just one episode." Charlie Savage, "National Security Surveillance Plummeted Amid Pandemic and Russia Inquiry Fallout," *The New York Times*, April 30, 2021, available at https://nyti.ms/328vKwu.

Indeed, the *2018 FISC Op.* devotes pages to summarizing the incidents and categories of non-compliance with and abuse of Section 702 querying. *2018 FISC Op.*, at 76-78. The FISC concluded that the improper queries directed at U.S. persons were not reasonably likely to result in foreign intelligence information or evidence of a crime, and included searches for information concerning relatives, potential witnesses, and potential informants. *Id.*

In fact, the FISC disclosed that the "the FBI has conducted tens of thousands of unjustified queries of Section 702 data." *2018 FISC Op.*, at 87. In addition, the FISC explained that the problems mushroom beyond the initial transgression: "[i]n 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.[33]

Subsequently, the *2020 FISC Op.* listed specific improprieties, such as 69 improper queries by a terrorism task-force officer, *2020 FISC Op.*, at 40, "[o]ther reported violations [that] apparently

---

[33] A 2018 amendment to FISA required a warrant "in only a small subset of cases – criminal investigations not relating to national security that had reached a certain stage of the investigation – and only after the query is conducted (but before reviewing the contents of any communications)." *See* Elizabeth Goitein, "ODNI's 2019 Statistical Transparency Report: The FBI Violates FISA … Again," *Just Security*, May 11, 2020 ("*Goitein*"), available at https://bit.ly/3F4aUgn. Yet through the end of 2020 the FBI had *completely ignored* that minimal requirement. As Ms. Goitein, Co-Director of the Liberty & National Security Program at New York University Law School's Brennan Center for Justice, reported, ODNI's *2019 Transparency Report*, available at https://bit.ly/3sfPKsb, "reveal[ed] that the FBI has failed to comply with it in literally every relevant case." *Goitein.* A table in the *ODNI 2019 Transparency Report* cited six instances in 2018 "in which the FBI reviewed the contents of Americans' communications after conducting a backdoor search in a criminal, non-national security case." *Id.*; *see also ODNI 2019 Transparency Report*, at 17. While the "six instances went unreported in the 2018 transparency report because they were not detected until a Department of Justice oversight review in 2019[,]" that "table indicates that the FBI obtained a warrant to review the contents of those communications exactly zero times." *Goitein.* Likewise, "for 2019, the table lists one instance in which the FBI ran a backdoor search in a criminal, non-national security case and reviewed communications content, but zero instances in which it obtained a warrant." *Id.* Each instance was characterized as a "compliance incident." *Id.*

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. *See also 2017 FISC Op.*, at 82 ("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*") (emphasis added) (citations omitted) (footnote omitted).[34]

Moreover, the *2018 FISC Op*. expressed dismay 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. Nor was the FISC even able to identify the level of non-compliance with precision or confidence because of the FBI's failure to adhere to the statutory record-keeping requirements. *See also Muhtorov*, 2021 WL 5817486, at *87 (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 PCLOB Report*, at 59.

That delinquency made it impossible to verify critical distinctions – contrary to the statutory directive – between queries of U.S. persons and those of foreigners. For instance, as the FISC recounted,

---

[34] Nor was that 85% error rate deemed anomalous. As the *2017 FISC Op.* added, "[w]hile the government reports that it is unable to provide a reliable estimate of the number of non-compliant queries since 2012, *id*., there is no apparent reason to believe the November 2015-April 2016 period coincided with an unusually high error rate." *Id*., at 82.

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

2018 FISC Op., at 52.

In response to FBI's protest that its procedures were adequate, and the statute's too burdensome, the FISC admonished that "[r]egardless 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). Thus, "[i]n sum, the Court is merely enforcing what Section 702(t)(1)(B) plainly imposes." *Id*.

Other facets of FBI's querying also troubled the FISC. Querying did not require any showing of individual suspicion; any required high-level approval; any restrictions on use of the resulting information; and/or any requirement that irrelevant or innocent information be promptly destroyed. *2018 FISC Op*., at 73-80.

Ultimately, the FISC concluded that FBI's permissive rules for searching through U.S. persons' communications rendered the surveillance unreasonable under the statute and the Fourth Amendment. *2018 FISC Op*. at 86-88. The lack of sufficient record-keeping constituted one statutory and perhaps constitutional deficiency: "[w]ithout 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. *See also id*., at 75.

In reaching its constitutional determination, the FISC explained that

> [b]ecause 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.

2018 FISC Op., at 82.

Further explicating its reasoning, the FISC noted that "[h]ere, there are demonstrated risks of serious error and abuse, and the Court has found the government's procedures do not sufficiently guard against that risk, for reasons explained above in the discussion of statutory minimization requirements." *Id*., at 88.

Two years later, the problems of non-compliance and abuse remained. As the *2020 FISC Op*. pointed out, "NSD has reported a number of compliance incidents that were discovered during oversight reviews at FBI field offices, which suggest that *the FBI's failure to properly apply its querying standard when searching Section 702-acquired information was more pervasive than was previously believed*." *Id*., at 39 (emphasis added).

Thus, "the Court continue[d] to be concerned about FBI querying practices involving U.S.-person query terms, including (1) application of the substantive standard for conducting queries; (2) queries that are designed to retrieve evidence of crime that is not foreign-intelligence information; and (3) record keeping and documentation requirements." *Id*. *See also 2017 FISC Op*., at 19 ("[s]ince 2011, NSA's minimization procedures have prohibited use of U.S.-person identifiers to query the results of upstream Internet collection under Section 702. The October 26,

2016 Notice informed the Court that NSA analysts had been conducting such queries in violation of that prohibition, with much greater frequency than had previously been disclosed to the Court").

While the FBI subsequently adopted strengthened procedures, and continues to conduct Section 702 surveillance on that basis today, *see 2019 FISC Op.*, those changes cannot salvage the government's materially flawed surveillance of Mr. Hasbajrami in this case. As the Circuit recognized, any improved querying rules "were not in place" during the very period in which Mr. Hasbajrami's communications were intercepted (April 2, 2011, through August 28, 2011), and subsequently queried. *Hasbajrami*, 945 F.3d at 658.[35]

Indeed, the record continues to support the conclusion that FBI agents conducted backdoor searches as part of their investigation of Mr. Hasbajrami, as agents do "whenever the FBI opens a new national security investigation or assessment[,]" *PCLOB Report*, at 59, and that in the process violated the Fourth Amendment and the statute. *See also Muhtorov*, 2021 WL 5817486, at *86

---

[35] The Court in *Muhtorov* pointed out that the provisions in the FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-18, 132 Stat. 3 (2018), designed to enhance oversight and limit non-compliance "were not in effect during the investigation of the foreign target who communicated with Mr. Muhtorov." 2021 WL 5817486, at *8 n.6. Likewise, while "Congress added the requirement to develop querying procedures in 2018 when it extended Section 702. *See* Pub. L. No. 115-18, § 101 (codified at 50 U.S.C. § 1881a(f))[,]" that "was not in place when the foreign target under investigation communicated with Mr. Muhtorov." *Id*., at *9 n.7. The same is true here: neither statutory reform designed to protect Fourth Amendment rights existed during the time frame of the 2011 investigation of Mr. Hasbajrami.

Nevertheless, as the dissent in *Muhtorov* noted, "although the statute did not mandate record-keeping requirements concerning queries of U.S. persons as a distinct category until 2018, the minimization procedures applicable at the time of the investigation into Muhtorov required the maintenance of records of all search terms used to query §702 databases, which would have included searches using identifiers associated with Muhtorov." *Muhtorov*, at *86 n.26 (Lucero, J., dissenting), *citing PCLOB Report*, at 58-59 ("FBI minimization procedures also permit the FBI to query unminimized Section 702-acquired data[,] . . . [and requires the FBI] to maintain records of all terms used to query content").

(Lucero, J., dissenting) ("[i]t blinks reality to assert that, in this one instance, the FBI did not follow its standard operating procedure of querying §702 data when opening a national security investigation").

Although the secrecy and the complexity of the querying procedures have obscured their Fourth Amendment and statutory deficits for nearly a decade, the subsequent FISC opinions have laid bare the broad invasion they licensed with respect to the privacy of U.S. persons' communications that occurred in practice. Unless the government can establish that the multiple and fatal statutory and constitutional flaws identified by the FISC – all reportedly in place during the period Mr. Hasbajrami was subject to Section 702 surveillance and querying – were not, in fact, present, contrary to these now-unsealed FISC opinions and related independent oversight reports, then those statutory and constitutional flaws render the backdoor searches of his communications unreasonable as a matter of law.

3. *Earlier FISC Disclosure of Non-Compliance with Section 702 Procedures*

The persistent problems with Section 702 were recognized even earlier than in the *2018 FISC Op*. In the *2011 FISC Op.*, at *5, n.14, Judge Bates, Chief Judge of the FISC at the time, excoriated the NSA for exceeding its acquisition authority and making repeated misrepresentations to the FISC regarding NSA's activities during the period in which Mr. Hasbajrami's communications were monitored and intercepted pursuant to Section 702 (50 U.S.C. §1881a).

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 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*,

> [w]ith 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). *See* **ante**, at 17-18.

In his opinion, Judge Bates noted the pervasive nature of the violations. For example, Judge Bates stated "[t]he 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*." *2011 FISC Op*., 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, adding that:

- "[t]he Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet 'transactions,' which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities, June 1 Submission at 1-2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals." *Id*., at *5.
- "for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different than what the Court had been led to believe." *Id*., at 9;
- "the Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCT's [multi-communication transactions], are consistent with the Fourth Amendment." *Id*., at 9;
- "NSA's minimization procedures, as the government proposes to apply them to MCT's as to which the 'active user' is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. §1881a(e) with respect to retention[.]" *Id*., at 28;
- "[t]he sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of transactions is not feasible." *Id*., at 10;

- "the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications acquired or the extent to which those communications are to or from United States persons or persons in the United States." *Id*., at 10;
- "[e]ven if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection . . . it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future." *Id*., at 10;
- "the actual number of wholly domestic communications acquired may still be higher in view of NSA's inability conclusively to determine whether a significant portion of the MCT's within its sample contained wholly domestic communications." *Id*., at 11; and
- "the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year." *Id*., at 15.[36]

As a result, Judge Bates required further briefing by the government because "it appeared to the Court that the acquisitions described in [a recent government letter to the Court] exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702." *Id*., at *2.[37]

---

[36] *See also* Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.," *The New York Times*, August 8, 2013, available at https://nyti.ms/3IU86EW (analyzing a document of internal NSA rules disclosed by Edward Snowden).

[37] Subsequently, the government presented the FISC revised minimization standards that were deemed acceptable under statutory and Fourth Amendment standards. However, those modifications were submitted November 30, 2011, well after the electronic surveillance and

Yet despite Judge Bates's iteration of the defects in the Section 702 program's acquisition and minimization protocols, seven years later the *2018 FISC Op.* was compelled to recite a litany of violations in the context of Section 702 database querying. *See also 2019 FISC Op*., at 67-70, 81; *2020 FISC Op*., at 39-44.

C. *The DoJ Inspector General's 2019, 2020, and 2021 Reports Detailing Non-Compliance with FISA's Procedural and Substantive Provisions*

Throughout its 43-year existence, FISA's *ex parte* culture has created and cultivated, and promoted and enabled, the ongoing problems identified with respect to the non-compliance with procedures (and, in turn, the Fourth Amendment) and accuracy of FISA applications. Some of the most egregious have been made public only since the Second Circuit's opinion herein.

The revelations and conclusions in a series of reports issued by DoJ's Inspector General ("DoJ IG") illustrate not only the compounding risk of error inherent in a process that operates *ex parte* from start to finish, but also that courts – either the FISC or traditional federal courts – are by themselves *not* positioned to identify problems, including material misrepresentations and omissions, as well as procedural violations, that afflict the government's FISA process, including querying.

The complexity of the surveillance and the subsequent querying, and the government's reluctance to provide even the Second Circuit with conclusive answers, only amplifies that opportunity for concealment and error. Thus, it is respectfully submitted that participation by and contributions from security-cleared defense counsel is imperative in this case. *See also* **post**, at 82-103.

---

acquisition of Mr. Hasbajrami's communications occurred in this case.

1. *The DoJ Inspector General's 2019 Report Regarding the Carter Page FISA Applications and Renewals*

In December 2019 the DoJ IG issued a 476-page Report detailing the many egregious errors and abuse committed by the FBI and the DoJ in the course of applying for and renewing the 2016 FISA electronic surveillance conducted on Carter Page, at one time Donald J. Trump's presidential campaign advisor, as part of the investigation denominated "Crossfire Hurricane." *See* 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) ("*December 2019 DoJ OIG Report*"), available at bit.ly/2sOu8H4.

In reciting in considerable detail the "FBI's failure to adhere to its own standards of accuracy and completeness when filing FISA applications[,]" the *December 2019 DoJ IG Report* found "basic, fundamental, and serious errors during the completion of the FBI' s factual accuracy reviews . . . which are designed to ensure that FISA applications contain a full and accurate presentation of the facts." *Id*., at 413. As a result, it concluded that the FBI "failed to comply with FBI policies, and in so doing fell short of what is rightfully expected from a premier law enforcement agency entrusted with such an intrusive surveillance tool." *Id*., at 414.

The *December 2019 DoJ OIG Report* identified 17 separate problems with the FBI's four applications to the FISC (the initial application and three renewal applications) – including repeated misrepresentations, factual inaccuracies, and material omissions. *See id.,* at viii-xii. In addition, the *December 2019 DoJ OIG Report*'s conclusions negate any claim that the defects in the Page applications were unique.

As the *December 2019 DoJ OIG Report* declared,

> That so many basic and fundamental errors were made by three separate, hand-picked teams on one of the most sensitive FBI investigations that was briefed to the highest levels within the FBI, and that FBI officials expected would eventually be subjected to close scrutiny, raised significant questions regarding the FBI chain of command's management and supervision of the FISA process.

Id., at xiv.[38]

Also, it was a failure across the entire hierarchy: "In our view, this was a failure of not only the operational team, but also of the managers and supervisors, including senior officials, in the chain of command." *Id*. Those directly responsible for the applications also concealed information from superiors: "the Crossfire Hurricane team failed to inform Department officials of significant information that was available to the team at the time that the FISA applications were dralted and filed." *Id*., at v. *See also id*., at x (describing failure to disclose certain facts to DoJ attorneys).

As a result, "[m]uch of that information was inconsistent with, or undercut, the assertions contained in the FISA applications that were used to support probable cause and, in some instances, resulted in inaccurate information being included in the applications." *Id*. *See also id*., at xiii ("agents and supervisors did not give appropriate attention or treatment to the facts that cut against probable cause, or reassess the information supporting probable cause as the investigation progressed").[39]

---

[38] Indeed, the *December 2019 DoJ IG Report* foreshadowed two subsequent reports, discussed **post**, at 69-73 and 73-74: "In addition, given the extensive compliance failures we identified in this review, we believe that additional OIG oversight work is required to assess the FBI's compliance with Department and FBI FISA-related policies that seek to protect the civil liberties of U.S. persons." *Id*., at xiv.

[39] *See also id*., at xiii ("[a]lthough some of the factual misstatements and omissions we found in this review were arguably more significant than others, we believe that all of them taken

The *December 2019 DoJ OIG Report* identified "seven significant inaccuracies and omissions" in the initial FISA application "based upon the information known to the FBI" at the time[,]" *Id*., at viii, including information that rebutted the premises of the application. For example, the initial application and renewals

> [o]mitted information the FBI had obtained from another U.S. government agency detailing its prior relationship with Page, including that Page had been approved as an "operational contact" for the other agency from 2008 to 2013, and that Page had provided information to the other agency concerning his prior contacts with certain Russian intelligence officers, one of which overlapped with facts asserted in the FISA application[.]

Id. *See also* 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, at 4, available at https://www.clearinghouse.net/chDocs/public/NS-DC-0127-0009.pdf ("the government admits that at least the third and fourth Page applications lacked adequate factual support") (citation omitted).

The *December 2019 DoJ OIG Report* provides detail on the extent of the concealment: "on or about August 17, 2016, the Crossfire Hurricane team received information from another U.S. government agency advising the team that Carter Page had been approved as an operational contact for the other agency from 2008 to 2013 and detailing information that Page had provided to the other agency regarding Page's past contacts with certain Russian intelligence officers." *Id*., at 79.

Yet "this information was not provided to NSD attorneys and was not included in any of the FISA applications." *Id*. The *December 2019 DoJ OIG Report* "also found no evidence that the

---

together resulted in FISA applications that made it appear that the information supporting probable cause was stronger than was actually the case").

Crossfire Hurricane team requested additional information from the other agency prior to submission of the first FISA application in order to deconflict on issues that were relevant to the FISA application."[40]

In addition, that "failure to provide accurate and complete information to the [NSD Office of Intelligence] Attorney concerning Page's prior relationship with another U.S. government agency . . . was particularly concerning because the OI Attorney had specifically asked the case agent in late September 2016 whether Carter Page had a current or prior relationship with the other agency." *Id*., at ix.

Moreover, the application and renewals "overstated the significance" of a source's reliability, and corroboration for that source's information, and omitted information and statements that were part of consensually monitored conversations, but which were contrary to the portrayal of Page and the investigation the applications and renewals sought to convey to the FISC. *Id*., at viii-ix.

For example, the initial application "[i]ncluded Page's consensually monitored statements to an FBI [Confidential Human Source] in October 2016 that the FBI believed supported its theory

---

[40] The *December 2019 DoJ OIG Report* revealed that even when pertinent information was requested, FBI personnel withheld it: "[w]hile FISA discussions were ongoing, on or about August 17, 2016, the Crossfire Hurricane team received information from another U.S. government agency relating to Page's prior relationship with that agency and prior contacts with Russian intelligence officers about which the agency was aware." *Id*., at 123. While "this information was highly relevant to the potential FISA application, the Crossfire Hurricane team did not engage with the other agency regarding this information until June 2017, just prior to the final Carter Page FISA renewal application." *Id*. (footnote omitted). Moreover, "when Case Agent 1 was explicitly asked in late September 2016 by the [NSD Office of Intelligence] Attorney assisting on the FISA application about Page's prior relationship with this other agency, Case Agent 1 did not accurately describe the nature and extent of the information the FBI received from the other agency." *Id*.

that Page was an agent of Russia but omitted other statements Page made that were inconsistent with its theory[.]" *Id*., at ix.

The malfeasance even included altering an email from a liaison to a U.S. intelligence agency to fit the FBI's version of Page's status. In that episode an FBI attorney "altered [the] email by inserting the words 'not a source' into it, thus making it appear that the liaison had said that Page was 'not a source' for the other agency." *Id*., at xiii. Consequently, "[r]elying upon this altered email," the supervising FBI Special Agent "signed the third renewal application that again failed to disclose Page's past relationship with the other agency." *Id*.

Another problem the *December 2019 DoJ OIG Report* illuminated was that "case agents may have improperly substituted their own judgments in place of the judgment of or, or in place of the court, to weigh the probative value of the information." *Id*. *See also* Charlie Savage, "Problems in F.B.I. Wiretap Applications Go Beyond Trump Aide Surveillance, Review Finds," *The New York Times*, March 31, 2020, available at https://nyti.ms/2w2HlxH ("current and former national security officials" attributing the "systemic incompetence" of the FISA process to the fact that it "is inherently vulnerable to the risk that lower-level agents will cherry-pick evidence when compiling factual summaries, leaving out evidence that weakens their case when they seek permission to conduct surveillance either deliberately or through confirmation bias . . .").[41]

---

[41] That same article in *The New York Times* reported

> The F.B.I. and the Justice Department'ds National Security Division also occasionally audit FISA applications for accuracy. The inspector general report said it examined 34 such accuracy review reports covering 42 FISA applications at eight field offices between 2014 and 2019. Those reviews found a total of 390 issues in 39 of the 42 applications, "including unverified, inaccurate, or inadequately supported facts, as well as typographical errors," it

The *December 2019 DoJ OIG Report* also noted the historical tension that has existed between the FISA program and civil liberties: "In every year since 2006, the OIG's annual report on 'Top Management and Performance Challenges Facing the Department of Justice' has highlighted the difficulty faced by the Department and the FBI in maintaining a balance between protecting national security and safeguarding civil liberties." *Id*., at 6, listing years of DoJ OIG reviews and reports.

In the context of this case, the *December 2019 DoJ OIG Report*'s account of the FBI's and the FISA applications' and renewals' suppression of information that might undercut probable cause – even to the extent of a forgery (for which the FBI attorney was prosecuted after release of the *December 2019 DoJ OIG Report*), *see* **ante**, at 66[42] – is particularly relevant.

As set forth **ante**, at 6, "there [was] information to suggest that Individual #1 [wtih whom Mr. Hasbajrami was communicating via email] was not in fact a terrorist, and that he solicited funds from the defendant for purposes unrelated to terrorism." PSR, at ¶ 3. Whether that information was provided to the FISC (or even to DoJ attorneys or FBI supervisors) or any other decision-maker relative to querying, or factored into the decision to query (and/or was subsequently disclosed in either the initial application for Title I and III FISA electronic surveillance of Mr. Hasbajrami, or renewals thereafter), are questions of vital importance (among others).

The government has repeatedly claimed that Individual #1 was "potentially an agent of a foreign government[,]" *see, e.g.*, Gov't Br. at 20, 21, 30, 81, 86, 87, and it appears from the Order

---

said.

[42] *See, e.g.*, Matt Zapotosky, "Ex-FBI lawyer avoids prison after admitting he doctored email in investigation of Trump's 2016 campaign," *The Washington Post*, January 29, 2021, available at https://wapo.st/3ek0C0a.

issued by the District Court after Mr. Hasbajrami's appeal was underway, that the government relied upon that quite possibly inaccurate or even false claim to support its Title I and Title III FISA applications, which had themselves been derived from the Government's Section 702 surveillance. *See* Order, dated, February 25, 2016 (released to the defense in redacted, unclassified, partially modified form, on March 8, 2016) (ECF #165), at 23-25.

Moreover, based upon the District Court's Order, it is apparent that the government also relied upon that potentially false claim in classified *ex parte* submissions presented to the District Court below. Indeed, the failure to confront contrary information has persisted through the appellate process, as the Government's Brief (cited above) demonstrates. Thus, the very distinct probability exists that one of the very same serious abuses that occurred during the Crossfire Hurricane investigation – concealing information that contradicted the government's theory of investigation – plagued the FISA process in this case as well.[43]

An article in *The New York Times* published soon after the *December 2019 DoJ OIG Report* was released reported that "according to interviews with more than two dozen current and former F.B.I. agents and Justice Department officials who have worked with national security wiretaps[,]"

---

[43] In response to the *December 2019 DoJ OIG Report*'s disclosures, the FISC, in a March 5, 2020, Corrected Opinion & Order, available at https://bit.ly/3ehTjpz, required all future FISA applications to include from a DoJ attorney the certification that "this application fairly reflects all information that might reasonably call into question the accuracy of the information or the reasonableness of any FBI assessment in the application, or otherwise raise doubts about the requested findings." *Id*., at 19. Also, FBI agents would have to certify that they "apprised [NSD'S OI]" of all such information. *Id. See also* Charlie Savage and Nicholas Fandos, "Senate Approves Surveillance Bill With Sharper Privacy Safeguards," *The New York Times*, May 14, 2020, available at https://nyti.ms/2WVDKej (proposed Senate amendment "codify a recent FISA court order that wiretap applications must include a government certification that it has shared with the court any information it has that could cast doubt on its suspicions that an investigative target is probably a foreign agent").

the Page applications'/renewals' "problems may be part of a broader pattern in other applications that never receive the same intense scrutiny." Charlie Savage, "National Security Wiretap System Was Long Plagued by Risk of Errors and Omissions," *The New York Times*, February 23, 2020, available at https://nyti.ms/2Ta8aaM.[44]

Here, the FISA surveillance and querying with respect to Mr. Hasbajrami is only beginning to receive the "intense scrutiny" it deserves just the same as for a powerful political figure.

2. *The DoJ IG's March 2020 Management Advisory Memorandum on FBI's Widespread Non-Compliance with Its "Woods Procedures"*

The alarm generated by the fruits of the investigation that produced the *December 2019 DoJ IG Report* motivated the DoJ IG to conduct a further audit of a select number of FISA applications. That produced, in March 2020, a 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 ("*March 2020 DoJ IG Management Advisory Memorandum*"), available at https://bit.ly/3mtppmU.

That *March 2020 DoJ IG Management Advisory Memorandum*'s "initial review of [the FISA] applications [] consisted solely of determining whether the contents of the FBI's Woods File supported statements of fact in the associated FISA application." *Id*., at 2.[45] As the *Management*

---

[44] That article added that those same officials said that while "[t]he system is vulnerable . . . to lower-level agents suppressing or overlooking evidence that weakens their case when they seek permission to conduct surveillance," nevertheless "similar flaws with surveillance have surfaced before, underscoring that the problems may be systemic rather than unique to the Page applications, current and former officials said." *Id*.

[45] The "review did not seek to determine whether support existed elsewhere for the factual assertion in the FISA application (such as in the case file), or if relevant information had

Advisory Memorandum explains, "The stated purposes of the Woods Procedures are to minimize factual inaccuracies in FISA applications and to ensure that statements contained in applications are 'scrupulously accurate.'" *Id*., at 3.[46]

In addition, "[s]pecifically, the Woods Procedures mandate compiling supporting documentation for each fact in the FISA application."[47] A Woods File is supposed to contain "(1) supporting documentation for every factual assertion contained in a FISA application, and (2) supporting documentation and the results of required database searches and other verifications." *Id*.

Yet the DoJ IG concluded, "As a result of our audit work to date and as described below, we do not have confidence that the FBI has executed its Woods Procedures in compliance with FBI policy." *Id*. *See also id*. ("we believe that a deficiency in the FBI's efforts to support the factual statements in FISA applications through its Woods Procedures undermines the FBI's ability to achieve its 'scrupulously accurate' standard for FISA applications").[48]

---

been omitted from the application." *Id*., at 2.

[46] As recounted in the September *2021 DoJ IG Audit*, *see* **post**, at 73-74, "Since April 2001, the FBI has used the FISA Verification Procedures, also known as the 'Woods Procedures,' to minimize factual inaccuracies in FISA applications and to ensure that statements contained in such applications are 'scrupulously accurate.' The FBI instituted these procedures in response to concerns expressed by the FISC in November 2000 regarding errors identified in 75 FISA applications related to FBI counterterrorism investigations.' *Id*., at 2. The FISC's concerns were those raised in the matter discussed above, yet 20 years later FBI's failure to abide by the rules of FISA or the Fourth Amendment have persisted and, as amply demonstrated in the FISC's subsequent opinions, spread unabated to Section 702 querying. *See also* **post**, at 79-80.

[47] As the *March 2020 DoJ IG Management Advisory Memorandum* states, and as discussed further **post**, at 79-80, "FBI implemented its Woods Procedures in 2001 following errors in numerous FISA applications submitted to the FISC in FBI counterterrorism investigations."

[48] In a subsequent April 3, 2020, Order in *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, Docket No. Misc. 19-02, available at https://bit.ly/3H6TQHj,

Elaborating, the *Management Advisory Memorandum* declared that the "lack of confidence that the Woods Procedures are working as intended stems primarily from" four separate and glaring deficiencies characterized as "repeated weaknesses" that "raise significant questions" about FBI compliance with its own policy (*id*., at 8):

(1) the DoJ IG "could not review original Woods Files for 4 of the 29 selected FISA applications *because the FBI has not been able to locate them* and, in 3 of these instances, *did not know if they ever existed.*" (Emphasis added);

(2) the FISA applications for "the associated Woods Files identified *apparent errors or inadequately supported facts in all of the 25 applications [] reviewed*, and interviews to date with available agents or supervisors in field offices generally have confirmed the issues [] identified." (Emphasis added);[49]

FISC Chief Judge James E. Boasberg wrote that "[i]t would be an understatement to note that [the DoJ OIG's] lack of confidence appears well founded." *Id*., at 2. *See also id*. ("[t]he OIG Memorandum provides further reason for systemic concern").

[49] The *March 2020 DoJ IG Management Advisory Memorandum* adds that

> for all 25 FISA applications with Woods Files that we have reviewed to date, we identified facts stated in the FISA application that were: (a) not supported by any documentation in the Woods File, (b) not clearly corroborated by the supporting documentation in the Woods File, or (c) inconsistent with the supporting documentation in the Woods File.

Id., at 7. Moreover, "[a]lthough reports related to 3 of the 42 FISA applications did not identify any deficiencies, the reports covering the remaining 39 applications identified a total of about 390 issues, including unverified, inaccurate, or inadequately supported facts, as well as typographical errors." *Id*., at 5. *See also id*., at 7 (DoJ OIG "identified an average of about 20 issues per application reviewed, with a high of approximately 65 issues in one application and less than 5 issues in another application").

(3) "existing FBI and NSD oversight mechanisms have also identified deficiencies in documentary support and application accuracy that are similar to those that we have observed to date[;]" and

(4) "FBI and NSD officials we interviewed indicated to us that there were *no efforts by the FBI* to use existing FBI and NSD oversight mechanisms to perform comprehensive, strategic assessments of the efficacy of the Woods Procedures or FISA accuracy, to include identifying the need for enhancements to training and improvements in the process, or increased accountability measures." (Emphasis added).

Id., at 3.

The problems with the Woods Files applied to FISA renewal applications as well. *See id*., at 8 ("preliminary results also indicate that FBI case agents are not consistently following Woods Procedures requirements related to renewal applications"). In fact, "it appears that the FBI is not consistently re-verifying the original statements of fact within renewal applications." *Id*., at 8.[50]

---

[50] The *March 2020 DoJ IG Management Advisory Memorandum* provided some specific examples relevant to renewal applications:

> In one instance, we observed that errors or unsupported information in the statements of fact that we identified in the initial application had been carried over to each of the renewal applications. In other instances, we were told by the case agents who prepared the renewal applications that they only verified newly added statements of fact in renewal applications because they had already verified the original statements of fact when submitting the initial application. *This practice directly contradicts FBI policy*.

Id., at 8 (emphasis added). *See also*

They were also widespread: "the Woods File deficiencies that [DoJ OIG] identified spanned all eight field offices in which we performed fieldwork[.]" *Id*.

3. *The DoJ IG's Subsequent September 2021 Audit Report on Its Further Investigation of "Woods Procedures" Non-Compliance*

In September 2021 the DoJ OIG augmented its earlier March 2020 review of FBI's Woods Procedures non-compliance. *See* OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, No. 21-129, 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 21-129 (September 2021) ("*September 2021 DoJ OIG Audit*"), available at https://oig.justice.gov/sites/default/files/reports/21-129.pdf.

The *September 2021 DoJ OIG Audit* reviewed FISA applications "approved by the [FISC] between fiscal years 2015 and 2019." *Id*., at i. Subsequent to issuing the *March 2020 DoJ IG Management Advisory Memo*, "the FBI conducted an accuracy review of those 29 FISA applications [that were the subject of the *March 2020 DoJ IG Management Advisory Memo*]; thereafter, [DoJ] notified the FISC of 209 instances where the applications were inaccurate, unsupported, or omitted information." *Id*., at 7.

The "additional OIG audit work determined there were another 209 instances where the Woods Files did not contain adequate documentation to support factual assertions in the sampled applications but where the FBI and NSD told [DoJ OIG] they had determined that appropriate support was subsequently located in other holdings." *Id*.

As a result, "in total, there were over 400 instances of non-compliance with the Woods Procedures in connection with those 29 FISA applications." *Id*. Broadening its scope, DoJ OIG's

"review of FBI documentation determined that, out of the universe of over 7,000 FISA applications authorized between January 2015 and March 2020, there were at least 179 instances in which the Woods File required by FBI policy was missing in whole or in part, which are in addition to the 4 referenced in our March 2020 MAM." *Id*.

Thus, "[a]pproximately 20 years after implementing the Woods Procedures to address the FISC's concerns regarding the accuracy of FBI FISA applications, [DoJ OIG's] review of 29 sampled FISA applications found that the FBI was not meeting the expectations of its own protocols." *Id*. *See also* **post**, at 79-80.

Indeed, the *September 2021 DoJ OIG Audit* concluded that "[g]iven the FBI's reliance upon its Woods Procedures to help ensure the accuracy of its FISA applications, we believe the missing Woods Files represent a significant lapse in the FBI's management of its FISA program." *Id*., at ii.

In addition, notwithstanding intervening measures adopted by FBI and DoJ to correct the problems, the DoJ OIG stated it "believe[s] additional action is necessary to ensure rigorous supervisory review and to further strengthen Woods Procedures oversight to reduce the risk of erroneous information being included in FISA applications, which can lead to faulty probable cause determinations and infringement of U.S. persons' civil liberties." *Id*., at i.

D. *Additional Previous FISC Opinions Identifying Non-Compliance Issues Regarding FISA Acquisition and Minimization Procedures and Implementation*

In addition to the 2009, 2011, 2017, 208, 2019, and 2020 FISC opinions, other FISC opinions declassified since 2013 include other examples of the government's persistent and diverse non-compliance with FISC orders and restrictions:

- the "NSA exceeded the scope of authorized acquisition continuously during the more than [redacted] years of acquisition[.]" [*(Case Name Redacted*], PR/TT No. [docket redacted], at 3, (FISA Ct. [date redacted]) (declassified Nov. 18, 2013), available at https://bit.ly/33EBsr3);
- "NSA's placement of unminimized metadata [redacted] into databases accessible by outside agencies, which, as the government has acknowledged, violates not only the Court's orders, but also NSA's minimization and dissemination procedures set forth in [United States Signal Intelligence Directive]," (*In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted]*, No. BR 09-06, at 6-7 (FISA Ct. June 22, 2009) (order requiring government to report and explain instances of unauthorized sharing of metadata) (declassified Sep. 10, 2013), available at https://bit.ly/3m5enUH);
- the Court was "deeply troubled" by previous non-compliance incidents that occurred shortly after the completion of NSA's "end to end review" of the processes for handling BR ["Business Records"] metadata "and its submission of a report intended to assure the court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems." *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) (declassified Sep. 10, 2013).

Judge Bates's *2011 FISC Op.*, *see* **ante**, at 17-18, 57-61, also referred to a 2009 FISC Opinion that was subsequently released to the public. That opinion, by FISC Judge Reggie B.

Walton (who also sits as a District Judge in the District for the District of Columbia) provides further and compelling proof that NSA persistently lies to, conceals from, and misleads (affirmatively and by silence) the FISC, and that the government cannot be trusted even to train its own employees adequately, or even be able to determine for itself the limits on its surveillance activities consistent with statute or FISC Orders. *See In re Production of Tangible Things From [*Redacted*]*, No. BR 08-13, 2009 WL 9150913 (FISA Ct. March 2, 2009) ("*2009 FISC Op.*).

Judge Walton's FISC opinion demonstrates the plethora of statutory violations that pervaded the government's bulk telephony metadata electronic surveillance program (Section 215). For example, Judge Walton's March *2009 FISC Op.* includes the following passages:

- "[t]he government's submission suggests that its non-compliance with the Court's orders resulted from a belief by some personnel within the NSA that some of the Court's restrictions on access to the BR [Business Records] metadata applied only to "archived data" . . . That interpretation strains credulity. . . such an illogical interpretation of the Court's Orders renders compliance with the RAS [Reasonable, Articulable Suspicion] requirement merely optional." *Id*., at *2;
- "[t]he government compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC." *Id*., at *3;
- "[r]egardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the

government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect [REDACTED] call detail records pertaining to telephone communications of US persons located within the United States who are not the subject of any FBI investigation and whose call detail information could not otherwise have been legally captured in bulk." *Id*., at *4;

- "[i]n summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. *The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systematically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively*." *Id*., at *5 (emphasis added);
- "[t]he record before the Court strongly suggests that, from the inception of this FISA BR program, the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures." *Id*., at *7; and
- "[u]nder these circumstances, *no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures*. In fact, the

> government acknowledges that, *as of August 2006, "there was no single person who had a complete understanding of the BR FISA system architecture*." *Id*., at *7 (emphasis added). *See also* Scott Shane, "Court Upbraided N.S.A. on Its Use of Call-Log Data," *The New York Times*, Sept. 10, 2013, available at https://nyti.ms/3GNVe1l(noting that, according to a senior U.S. intelligence official who briefed reporters just prior to release of the 2009 FISC opinion, "only about 10 percent of 17,800 phone numbers on the alert list in 2009 had met [the RAS] test," and that "'[t]here was nobody at N.S.A. who really had a full understanding of how the program was operating at the time").

Judge Walton also recognized the FISC's limitations as a watchdog, pointing out that "*in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified*, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of US persons as required by applicable minimization procedures." *2009 FISC Op.*, at *6 (emphasis added).

Elaborating, Judge Walton noted that "[t]o approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders." *Id*. Yet, he concluded, "*[t]he Court no longer has such confidence*." *Id*. (emphasis added).

Judge Walton's lack of confidence was well-founded, and validated by NSA's continued non-compliance. As if Judge Bates's *2011 FISC Op.* and Judge Walton's *2009 FISC Op.* (and the numerous others cited above) were insufficient to demonstrate NSA's abject inability – whether

deliberate or simply through inexcusably irresponsible negligence or cavalier incompetence – to comply, a subsequent August 13, 2009, report the government submitted to the FISC revealed even more non-compliance issues beyond the myriad enumerated in Judge Walton's opinion, and which were discovered after issuance of that Opinion. *See* Report of the United States, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 09-09, (FISC August 13, 2009), available at https://bit.ly/3EoSrdi.

Further violations of the FISC's Orders included, for example, (a) permitting employees of other government agencies to have external and unsupervised access to the NSA database; (b) failing to audit for compliance issues – at any point over the lifespan of the program – a database used to store information retrieved from the NSA databases; and (c) use of software with a feature permitting analysts to pull more information than NSA was authorized to retrieve. *Id.*

The government's continued non-compliance and recidivism, establishes that the FISC's complaints, and even its attempts at remedial measures, are ineffectual as long as the process remains secret and *ex parte* from start to finish. The public record – and who knows (certainly not defense counsel) what still remains classified – compels but one conclusion: the government agencies responsible for administering FISA cannot be trusted, despite repeated chances, and one of the principal reasons is the absence of any accountability.

The repeated misrepresentations cited by Judge Bates in October 2011 and Judge Walton in 2009 constitute simply a constant and continued feature of government practice with respect to FISA surveillance generally. Indeed, they are reminiscent of those divulged in the FISC's 2002 opinion in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISA Ct. 2002), *rev'd on other grounds sub nom.*, *In re Sealed Case*, 310 F.3d 717 (FISA

Ct. Rev. 2002),[51] in which the FISC, in its first opinion ever, reported that beginning in March 2000, DoJ had come "forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States."

Those errors related to misstatements and omissions of material facts," including:

- "75 FISA applications related to major terrorist attacks directed against the United States" contained "misstatements and omissions of material facts." *In re All Matters*, 218 F. Supp. 2d at 620-21;
- the government's failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance. *Id.*; and
- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id.*

According to the FISC, "[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . ." *Id.*, at 621. Nor were those problems isolated or resolved by those revelations. Instead, they proved persistent. A report issued March 8, 2006, by the DoJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other intelligence-gathering procedures more than 100 times in the preceding two years, and problems appeared to have grown more frequent in some crucial respects. *See* Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March 8, 2006 ("*2006 DoJ IG Report*"), available at https://bit.ly/33q2J00.

[51] The FISCR's 2002 decision in *In re Sealed Case* marked that appellate court's first case since enactment of FISA in 1978.

The report characterized some violations as "significant," including wiretaps that were much broader in scope than authorized by a court ("over-collection"), and others that continued for weeks and months longer than authorized ("overruns"). *Id*., at 24-25.[52] FISA-related overcollection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. *See 2006 DoJ IG Report*, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, *id*., at 29, although the amount of time "over-collection" and "overruns" were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id*., at 25.

The lack of veracity catalogued in the several declassified FISC opinions discussed **ante** is inevitable in a system in which there is no opponent to dispute facts or hold opponents accountable for misrepresenting facts, and in which the court lacks investigative authority or any practical, meaningful means of oversight over the collection/storage/interception process. Indeed, an internal May 2012 audit of NSA's surveillance programs – among the documents disclosed in 2013 by Edward Snowden – found that NSA violated privacy rules protecting domestic U.S. communications 2,776 times in a one-year period. *See* SID OVERSIGHT & COMPLIANCE, NATIONAL SECURITY AGENCY, OC-034-12, QUARTERLY REPORT, FIRST QUARTER CALENDAR YEAR 2012 (May 3, 2012), available at https://bit.ly/30zX9as.

---

[52] The *2006 DoJ IG Report* was not instigated by the government itself. Rather, the publication of documents released to Electronic Privacy Information Center in Freedom of Information Act litigation prompted the DoJ IG to use those and other documents as a basis for the report. In preparing the report the IG reviewed only those 108 instances in which the FBI itself reported violations to the Intelligence Oversight Board – a four-member Executive Branch body that ordinarily does *not* submit its reports to Congress.

Unfortunately, in a system in which the government and its law enforcement and intelligence organs are free to misrepresent without challenge or accountability, little has changed except perhaps the government's enhanced dexterity in abusing and manipulating the FISC and the FISA system as a whole.

E. *Pursuant to Specific Sections of FISA, and Consistent With CIPA, the Information Should Be Provided to Security-Cleared Defense Counsel*

Unless the Court decides as a matter of law that the government's queries of Section 702 databases violated Mr. Hasbajrami's Fourth Amendment rights, and that suppression is required, it is respectfully submitted that participation of security-cleared defense counsel is necessary for FISA and the Fifth Amendment's Due Process protection to be satisfied.

That includes access to both the government's factual submissions and legal briefing, and is authorized, even constitutionally compelled, by provisions of FISA and CIPA, and the constitutional rights they enforce through their provisions. For example, as detailed below, 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, as discussed below, CIPA, which regulates the use of classified information in criminal cases, was expressly designed to afford defendants the same access to helpful classified materials as they would possess if the information were not classified, and even provides courts with discretion to dismiss an indictment if the government refuses to comply with court-ordered disclosure to security-cleared defense counsel. *See* CIPA, 18 U.S.C. App. 3, at §6(e).

Litigation of FISA-authorized electronic surveillance generally, and FAA-authorized electronic surveillance and querying in particular in this case, represents a radical departure from the traditional and essential requirement of the adversary process.[53] While ordinary search and even electronic surveillance warrants (issued pursuant to Title III) are presented initially *ex parte*, once criminal charges are instituted defense counsel and the defendant are afforded access to the underlying submissions in support of those warrants.

However, historically FISA and FAA applications (and supporting documents) are not shared with the defendant or defense counsel – even defense counsel in possession of the requisite security clearance to review classified material. While, FISA includes provisions 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 disclosur[,]" 50 U.S.C. §1806(g) – only one court has ever ordered such disclosure – only to be reversed on appeal. *See United States v. Daoud*, ___ F.Supp.2d ___, 2014 WL 321384 (N.D. Ill. January 29, 2014), *rev'd* 755 F.3d. 479 (7th Cir. 2014). *See also see, e.g., In re Grand Jury Proceedings*, 347 F.3d 197, 203 (7th Cir. 2003)

---

[53] As stated in the Congressional Research Service's Report, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE,

> An underlying principle of the Anglo-American legal system is the adversarial process, whereby attorneys gather and present evidence to a generally passive and neutral decision maker. The basic assumption of the adversarial system is that a "sharp clash of proofs presented" by opposing advocates allows a neutral judge to best resolve difficult legal and factual questions.

Andrew Nolan, Richard M. Thompson II, and Vivian S. CHU, CONG. RESEARCH SERV., R43260, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE 2 (March 21, 2014), available at https://bit.ly/3s7y3Lv.

(citing cases); *United States v. Sattar*, 2003 U.S. Dist. LEXIS 16164, at *19 (S.D.N.Y. Sept. 15, 2003) (same).

Of course, Mr. Hasbajrami's case presents the first instance in the history of FISA that a Circuit court remanded for further factual and legal analysis, and in turn the first instance in which a Circuit court therefore has specifically authorized the District Court to direct the production of such classified material to security-cleared defense counsel if the District Court deems it appropriate. Nor is every fact about the government's reliance on backdoor searches properly classified. *See, e.g.*, *PCLOB Report* 59, 129.

The entirely one-sided nature of FISA litigation, particularly in the context of determining whether the government adhered to the restrictions set forth in 50 U.S.C. §1881a, applies not only to the facts at issue, as only the government knows the facts specific to the FAA electronic surveillance and interception with respect to Mr. Hasbajrami, but also to *the law* as well, as the government has access to the entire body of FISC and FISCR opinions, while defense counsel's access is limited to those few opinions the government or the court has released publicly.

This decidedly unlevel playing field – indeed, it is vertical, with the government at the apex and defense counsel at the bottom – has clear implications, not the least of which is the government's undefeated (and unsurprising, in light of the advantages inherent in *ex parte* litigation) record in FISA litigation in the statute's 43-year history. Also, it imposes upon the Court a responsibility – review of the FISA or FAA submissions as, in effect, surrogate defense counsel – to which courts have acknowledged they are not sufficiently suited to fulfill.

As the dissent in *Muhtorov* recognized, "[o]ur Fourth Amendment analysis must begin with an acknowledgement that CIPA procedures fundamentally alter the structures of our adversarial

process and place courts in a position as uncomfortable as it is unique." *Muhtorov*, 2021 WL 5817486, at *85 (Lucero, J., dissenting).

In the CIPA context,

> Congress has mandated that we step out of our traditional role as neutral arbiters overseeing adversarial presentation of issues and step into a role much closer to that of an inquisitor. As explicitly acknowledged by the government, a district court's role in cases involving CIPA is to act as "standby counsel for the defendants." Similarly, on appeal "we must place ourselves in the shoes of defense counsel, the very ones that cannot see the classified record, and act with a view to their interests."

Id., *citing United States v. Amawi*, 695 F.3d 457, 471 (6th Cir. 2012).

Nevertheless, as the dissent in *Muhtorov* conceded, "[t]he judiciary is neither institutionally suited nor resourced to fulfill this role." *Id*. (footnote omitted). In *Muhtorov*, the majority concluded the District Court had not abused its discretion in denying certain disclosure requests by the defense, noting that "[d]isclosure of classified FISA materials is the exception, not the rule." *Muhtorov*, 2021 WL 5817486, at *41.

Yet if ever there was an exception meriting disclosure, this case is it. This case is unique. It represents the first time in the 43-year history of FISA a District Court's ruling validating FISA-based interception was not affirmed in full, and the first remand for a factual determination. Also, it does so, as set forth **ante**, at 8, 23-27, because the government initially concealed from Mr. Hasbajrami and the District Court the Section 702 surveillance itself, and because, on appeal, the government essentially refused to provide information about querying to the Second Circuit. Consequently, security-cleared defense counsel's access to the government's factual and legal

submissions is an essential element of any determination that would be consistent with sufficient accuracy and Due Process.

1. *Two Sections of FISA Authorize Disclosure to Defense Counsel*

While aggrieved criminal defendants can move to suppress FISA-generated evidence, 50 U.S.C. §1806(f) provides that if the Attorney General files an affidavit that "disclosure or an adversary hearing would harm the national security of the United States," the court deciding the motion must consider the application and order for electronic surveillance *in camera* to determine whether the surveillance was conducted lawfully.[54]

Nevertheless, FISA contains two provisions that authorize disclosure to security-cleared defense counsel.

a. *Disclosure of FISA Materials to the Defense Pursuant to 50 U.S.C. §1806(f)*

At 50 U.S.C. §1806(f), FISA provides this Court with discretion to determine whether to "disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance" to the extent "*such disclosure is necessary to make an accurate determination of the legality of the surveillance.*" (Emphasis added).[55]

---

[54] Although the defense has not been notified whether the Attorney General has yet submitted an affidavit under 50 U.S.C. §1806(f) for purposes of this remand, it is assumed for purposes of this motion that the government has or will make such a filing.

[55] In *Muhtorov*, the Tenth Circuit noted that 50 U.S.C. §1806(f) "applies to Section 702 as well as traditional FISA." 2021 WL 5817486, at *37 n.39, *citing* 50 U.S.C. §1881e(a)(1) ("[i]nformation acquired from an acquisition conducted under [Section 702] shall be deemed to be information acquired from an electronic surveillance pursuant to [Title] I for purposes of section 1806 of this title, except [in circumstances not relevant here]"). That also encompasses 50 U.S.C. §1806(g).

According to FISA's legislative history, disclosure may be "necessary" under 50 U.S.C. §1806(f) "where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation 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.'" *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982), (*quoting* S. Rep. No. 701, 95th Cong., 2d Sess. 64 (1979)); *see, e.g.*, *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (same); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same).

Here, as discussed **ante**, at 6, 23-27, and 67-68, there are ample justifications for disclosure, as the government's repeated lack of candor, misrepresentations, and inaccuracies in one-sided FISA proceedings – both generally and *in this case* – underscore the necessity of adhering to the adversary process here. *Cf*. *Muhtorov*, 2021 WL 5817486, at *41 (District Court did not abuse its discretion in denying disclosure because the defendant's "misrepresentation theory is speculative" and "based solely on the government's behavior in other cases").

Counsel for Mr. Hasbajrami all possess security clearance to at least Top Secret level (and all have been read into more secret programs requiring SCI clearance). In addition, the Court can issue an appropriate Protective Order, to which Mr. Hasbajrami's counsel would of course consent, that would provide elaborate protection for classified information, and which would permit classified materials to be disclosed to defense counsel but not to the defendant. *See* CIPA, 18 U.S.C. App. 3, at §3.

Thus, the circumstances herein compel disclosure of FISA applications, orders, and/or materials related to backdoor searches. Indeed, the existence of 50 U.S.C. §1806(f) is an unambiguous declaration that Congress intended for courts to grant disclosure in appropriate cases. If 50 U.S.C. §1806(f) is to be rendered meaningful at all, and not be rendered superfluous and entirely inert, it should apply in this unprecedented case. *See United States v. Daoud*, 755 F. 3d 479, 485-86 (7th Cir. 2014) (Rovner, J., concurring) (complete absence of disclosure is in conflict with defendants' constitutional rights).

b. *Disclosure of FISA Materials to the Defense Pursuant to 50 U.S.C. §1806(g)*

Even if the Court were to decline to find that disclosure of FISA-related materials to the defense is appropriate under 50 U.S.C. §1806(f), the defense would still be entitled to disclosure of the FISA applications, orders, and related materials under 50 U.S.C. §1806(g), which expressly incorporates the Fifth Amendment Due Process Clause, and provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C. §1806(g) (emphasis added). *See also United States v. Spanjol*, 720 F. Supp. 55, 57 (E.D. Pa. 1989) ("[u]nder FISA, defendants are permitted discovery of materials only to the extent required by due process. That has been interpreted as requiring production of materials mandated by [*Brady*], essentially exculpatory materials").

As a threshold Due Process principle, *ex parte* proceedings are exceedingly disfavored. As the Sixth Circuit has cautioned, "[d]emocracies die behind closed doors." *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 683 (6th Cir. 2002). As the Ninth Circuit has observed, "*ex parte*

proceedings are anathema in our system of justice." *Guenther v. Commissioner of Internal Revenue*, 889 F.2d 882, 884 (9th Cir. 1989), *appeal after remand*, 939 F.2d 758 (9th Cir. 1991).

As the Supreme Court recognized in *Alderman v. United States*, 394 U.S. 165, 184 (1969) – a case involving electronic surveillance – "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." *See also Franks v. Delaware*, 438 U.S. 154, 169 (1978) (permitting adversarial proceeding on showing of intentional falsehood in warrant affidavit because the magistrate who approves a warrant *ex parte* "has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations"); *Dennis v. United States*, 384 U.S. 855, 875 (1966).[56]

Ex parte proceedings impair the integrity of the adversary process and the criminal justice system. In *United States v. Nobles*, 422 U.S. 225, 230-31 (1975), the Court declared that "[w]e have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law[,]" and that "[t]he *need to develop all relevant facts in the adversary system is both fundamental and comprehensive*." (Emphasis added) (quotation omitted).

---

[56] As the District Court in *United States v. Marzook*, 412 F. Supp.2d 913 (N.D. Ill. 2006), also a case involving terrorism-related charges, explained in the context of deciding whether to close a suppression hearing to the public because of the potential revelation of classified information thereat,

> It is a matter of conjecture whether the court performs any real judicial function when it reviews classified documents in camera. Without the illumination provided by adversarial challenge and with no expertness in the field of national security, the court has no basis on which to test the accuracy of the government's claims.

Id., at 921, (*quoting Stein v. Department of Justice & Federal Bureau of Investigation*, 662 F.2d 1245, 1259 (7th Cir. 1981)).

As the Supreme Court has recognized, "'Fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.'" *United States v. James Daniel Good Real Property, et. al.*, 510 U.S. 43, at 55 (1993), (*quoting Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). *See also United States v. Madori*, 419 F.3d 159, 171 (2d Cir. 2005), *citing United States v. Arroyo-Angulo*, 580 F.2d 1137, 1145 (2d Cir. 1978) (closed proceedings "are fraught with the potential of abuse and, absent compelling necessity, must be avoided") (other citations omitted).[57]

The dissent in *Muhtorov* quoted the Supreme Court's opinion in *United States v. Cronic*, 466 U.S. 648, 655 (1984), for the principle that "[t]he very premise of our adversary system of criminal justice is that partisan advocacy on both sides of a case will best promote the ultimate objective that the guilty be convicted and the innocent go free. It is that very premise that underlies and gives meaning to the Sixth Amendment. It is meant to assure fairness in the adversary criminal process." *Muhtorov*, 2021 WL 5817486, at *80 n.13 (Lucero, J., dissenting) ("cleaned up"). *See also id*., *(quoting Strickland v. Washington*, 466 U.S. 668, 685 (1984) ("a fair trial is one in which evidence subject to adversarial testing is presented to an impartial tribunal for resolution of issues defined in advance of the proceeding")).[58]

---

[57] Conversely, as Judge Learned Hand stated in *United States v. Coplon,* 185 F.2d 629, 638 (2d Cir. 1950), "Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which is seeks to forfeit the liberty of its citizens."

[58] The dissent in *Muhtorov* added that

In *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004), the Second Circuit reemphasized the importance of open, adversary proceedings, declaring that "[p]articularly 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 McGrath*, 341 U.S. at 171 n. 17 (Frankfurter, J., concurring) (noting that "the duty lying upon every one who decides anything to act in good faith and fairly listen to both sides . . . always giving a fair opportunity to those who are parties in the controversy for correcting or contradicting any relevant statement prejudicial to their view") (citation and internal quotation marks omitted).

Similarly, in the Fourth Amendment context, including in relationship to electronic surveillance, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman*, the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to the prosecution case against the defendants.

The Court rejected the government's suggestion that the District Court make that determination *in camera* and/or *ex parte*, and observed that

---

> Any other approach would make a mockery of our criminal justice system. We cannot require a defendant to specifically challenge the use of certain evidence when he does not have access to that very evidence to investigate its origins fully or to test its admissibility. To conclude that a defendant may mount a derivative evidence challenge to the use of § 702-derived evidence only if he has access to the evidence – which he does not – would transform the Fourth Amendment inquiry into a dark comedy.

Muhtorov, 2021 WL 5817486, at *85 n.22 (Lucero, J., dissenting).

> An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Alderman, 389 U.S. at 182.

In ordering disclosure of improperly recorded conversations, the Court declared:

> [a]dversary 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 that the Fourth Amendment exclusionary rule demands.

Id. at 184.[59]

Likewise, the Court held in *Franks v. Delaware*, 438 U.S. 154 (1978), that a defendant, upon a preliminary showing of an intentional or reckless material falsehood in an affidavit underlying a search warrant, must be permitted to attack the veracity of that affidavit. 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:

> [T]he hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily *ex parte*, since the subject of the

---

[59] In *Muhtorov*, the Tenth Circuit distinguished *Alderman* in a manner that makes *Alderman* all the more applicable here. In *Muhtorov*, the Court stated that in *Alderman* the "question was whether disclosure was necessary so the parties could litigate the scope of the exclusionary rule." 2021 WL 5817486, at *48. Here, that is precisely what the Circuit has included in the remand, as determining whether any exception to the exclusionary rule – such as "good faith," or the independent source doctrine, or even harmlessness – applies herein has been delegated to the Court. 945 F.3d at 673-77. Indeed, even the government has pressed those exceptions. *Id*.

> search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The 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. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

Franks, 438 U.S. at 169.

The same considerations that the Supreme Court found compelling in *Alderman* and *Franks* compel rejection of *ex parte* procedures in the peculiar context of this case. After all, denying an adversary access to the facts constitutes an advantage as powerful and insurmountable as exists in litigation.

Ex parte proceedings thus present an overwhelming danger of erroneous decisions. The Court, which has not had opportunity to review the discovery, or consult with the defense, cannot be expected to surmise the factual and legal nuances, or implications, of the redacted portions. Consequently, the Court cannot, despite its best efforts, properly function as Mr. Hasbajrami's surrogate advocate, particularly with respect to the critical factual and legal issues in this case, which are considerably more complicated than an ordinary case both factually and legally, thus irremediably impairing further a court's ability to play the role of defense counsel in a manner the Fifth and Sixth Amendments require.

As the Ninth Circuit observed in the closely analogous context of a secret evidence case, "'[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations.' . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will

violate due process because of the risk of error." *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1069 (9th Cir. 1995), (*quoting* District Court); *see, e.g., id*. at 1070 (noting "enormous risk of error" in use of secret evidence); *Kiareldeen v. Reno*, 71 F. Supp. 2d 402, 412-14 (D.N.J. 1999) (same).

Moreover, while defense counsel have always been aware that they were operating at an insuperable disadvantage by being denied access to the FISA applications or the underlying supporting documents (unlike any other situation in which the government seizes evidence pursuant to warrant), only since 2013 has it been revealed, through selective and often considerably delayed declassification of FISC opinions, that there has existed for more than a decade a growing body of *law*, in the form of opinions by the FISC and FISCR, that have been available to government counsel, but *not* to even security-cleared defense counsel. *See also* **ante**, at 84-85 & n. 15.

That represents an additional inequity impairing defense counsel's ability to present Mr. Hasbajrami's position effectively, which would only be aggravated by maintaining *ex parte* redactions in the opinions by both the District Court and the Second Circuit, and any in the upcoming submissions by the government. Unless defense counsel are permitted to review the redacted portions, only the defense, the party possessing constitutional rights, and whose counsel hold the appropriate security clearance(s), will be denied the ability to confront those Opinions as it exists in their entirety. *Cf. United States v. Hsu*, 155 F.3d 189, 204-05 (3d Cir. 1998) (neither the Court nor the parties had seen the redacted information, which was arguably related to a defense the Court ruled was not legally viable).

In addition, Due Process does not permit the government to withhold relevant or helpful information on the basis of privilege – and certainly not on the basis of an unsupported claim of

privilege. *See Roviaro v. United States*, 353 U.S. 53, 60-61 (1957); *United States v. Aref*, 533 F.3d 72, 79-80 (2d Cir. 2008) ("information can be helpful [within the meaning of *Roviaro*] without being 'favorable' in the [*Brady v. Maryland*, 373 U.S. 83 (1963)] sense").

The government's initial misrepresentation to Mr. Hasbajrami, which led to the vacatur of his original guilty plea, constituted a Due Process violation that likewise supports disclosure as a remedial measure now. *See, e.g., United States v. Russell*, 411 U.S. 423, 431-32 (1973) (there could exist "a situation in which the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction"), *citing* [*cf.*] *Rochin v. California*, 342 U.S. 165 (1952). *See also United States v. Schmidt*, 105 F.3d 82, 91 (2d Cir. 1997), *citing Russell*, 411 U.S. at 431-432.

As a result, the requisite "analysis of the governmental and private interests that are affected[,]" *Mathews v. Eldridge*, 424 U.S. 319, 334 (1976), including "three distinct factors," *id*., at 335, weigh heavily in Mr. Hasbajrami's favor:

(1) regarding the private interest that will be affected by the official action, Mr. Hasbajrami, as the Circuit and the FISC have recognized in plain language, has a substantial interest in accurately determining whether the government's surveillance violated his rights;

(2) the risk of an erroneous deprivation of such interest through *ex parte* procedures is significant, and the probable value, if any, of additional or substitute procedural safeguards is substantial, particularly in the context of complex factual and legal issues; and

(3) the government's interest can be sufficiently protected because, as contemplated under CIPA (as noted in the Circuit's opinion, *Hasbajrami*, 945 F.3d at 677 n. 24), this Court could order disclosure under a protective order that limits access to security-cleared counsel. *See also Tweak or Overhaul* ("even giving due weight to [the government's] considerations, a categorical rule of permanent secrecy in every FISA case seems impossible to justify").

2. *CIPA Provides a Mechanism for Disclosure to Security-Cleared Defense Counsel Consistent With Due Process and National Security*

The classified nature of the redacted material does not foreclose access by security-cleared defense counsel. The Second Circuit clearly envisioned that disclosure can be arranged "consistent with the requirements of CIPA and FISA." *Hasbajrami*, 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).

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.

The express purpose of CIPA is to protect sensitive national security information, but not at the expense of a defendant's rights. *See United States* v. *Stewart,* 590 F.3d 93, 130 (2d Cir. 2009); *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008) (government's privilege under CIPA "must give

way" when classified information is helpful or material to the defense). *See also United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) (citation omitted).

In fact, in enacting CIPA, Congress warned that "the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without the Act." S. Rep. No. 96-823, at 9 (1980). *See also, e.g., United States v. Poindexter*, 698 F. Supp. 316, 320 (D.D.C. 1988).

Also, CIPA "does not expand or restrict established principles of discovery." *United States v. Sedaghaty*, 728 F.3d 885, 904 (9th Cir. 2013). That includes the disclosure of surveillance materials sufficient for a defendant to fairly litigate suppression issues. Yet without defense counsel's participation in the process of evaluating the factual and legal materials the government will provide, how can the defendant be said to have been placed in the same position as he would if he enjoyed access to those materials?

Further justifying disclosure of FISA and FAA materials to security-cleared defense counsel in this case, the government's non-compliance clearly rises to level described in *United States v. Duggan*, 743 F.2d 59, 79 (2d Cir. 1984), in which the Second Circuit, relying on FISA's legislative history, explained 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 bases for disclosure are at their most compelling: (1) the government has repeatedly misrepresented facts (as it did initially to Mr. Hasbajrami, which formed the basis for Mr. Hasbajrami's withdrawal of his guilty plea, *see* **ante**, at 6); (2) the government has evaded providing accurate and complete information about its backdoor searches in this case *even to the Second Circuit at oral argument and in response to an explicit Order* (*see* **ante**, at 23-27); (3) the *2018 FISC Op.* and other FISC opinions have provided a voluminous catalog of substantive and procedural "irregularities" that flourish in the secret operation of the Section 702 system; and (4) the DoJ IG reports and others that have chronicled the government's non-compliance with and abuse of the FISA process as a whole. *See, e.g.*, **ante**, at 62-74.[60]

Moreover, the legal and factual questions related to the lawfulness of the querying and the fruit of the poisonous tree analysis are technical, novel, and complex, and therefore disclosure to security-cleared defense counsel is "necessary" in this case, precisely as Congress intended when it included 50 U.S.C. §1806(f) within FISA. Also, if the Court conducts an evidentiary hearing, cross-examination regarding the government's queries related to Mr. Hasbajrami would be a nullity absent security-cleared defense counsel's access to the underlying factual materials.

In 2020, in the aftermath of the *December 2019 DoJ IG Report*, *see* **ante**, at 62-69, Robert S. Litt, a former national security prosecutor and general counsel of the Office of the Director of

[60] Again, *Muhtorov* explicitly distinguished itself, as the Court, in discussing *this case*, asserted, "[t]his case [*Muhtorov*] is different." *Muhtorov*, 2021 WL 5817486, at *25 n.20.

National Intelligence during the Obama administration, articulated for *The New York Times* the dangers secrecy poses for accuracy and fairness: "Because the court operates in secret, you are lacking one of the levels to prevent a bad actor that otherwise exist." Charlie Savage, "National Security Wiretap System Was Long Plagued by Risk of Errors and Omissions," *The New York Times*, February 23, 2020, available at https://nyti.ms/2Ta8aaM.

In November 2021, the Supreme Court denied *certiorari* in a civil lawsuit seeking to compel public access to the FISC's opinions generally, thereby in effect confirming the *Executive*'s unilateral and exclusive discretion to determine when FISC opinions could be published. *See American Civil Liberties Union v. United States*, ___ U.S. ___, 142 S. Ct. 22 (Mem.) (2021). However, in dissent, Justices Gorsuch and Sotomayor expressed their view that the case "present[ed] questions about the right of public access to Article III judicial proceedings of grave national importance[,]" *id*., at 23, and observed that "the FISC evaluates extensive surveillance programs that carry profound implications for Americans' privacy and their rights to speak and associate freely." *Id*., *citing ACLU v. Clapper*, 785 F.3d at 818. *See also* George F. Will, "Opinion: The Supreme Court has a chance to shed light on a secretive judicial process," *The Washington Post*, September 29, 2021, available at https://wapo.st/320fDBu.[61]

The dissent also noted that "[u]nlike most other courts, however, FISC holds its proceedings in secret and does not customarily publish its decisions." *ACLU*, 142 S. Ct. at 23, *citing* 50 U.S.C. §1803(c) and *In re Motion for Release of Court Records*, 526 F. Supp.2d 484, 488 (FISA Ct. 2007).

[61] Among the signatories to a brief *amici curiae* supporting ACLU's petition for *certiorari* were James R. Clapper (former ODNI Director), John Brennan (former CIA Director), and Donald B. Verrilli, Jr. (former Solicitor General). *See* Robert Barnes and Spencer S. Hsu, "Supreme Court won't hear case seeking more transparency from secretive surveillance court," *The Washington Post*, November 1, 2021, available at https://wapo.st/32kXr5J.

In denying ACLU's request for access, the FISCR "refused even to consider the question, claiming they lacked authority to do so[,]" *id*., at 23 (citations omitted), and the government "also presse[d] the extraordinary claim that this Court is powerless to review the lower court decisions even if they are mistaken." *Id*.

Thus, as the dissent recognized, "On the government's view, literally no court in this country has the power to decide whether citizens possess a First Amendment right of access to the work of our national security courts." *Id*. Musing that "[m]aybe even more fundamentally, this case involves a governmental challenge to the power of this Court to review the work of Article III judges in a subordinate court[,]" the dissent asked, "If these matters are not worthy of our time, what is?" *Id*.

The secrecy of FISA proceedings that troubled Justices Gorsuch and Sotomayor in the context of the general public's right to know is even more material when a *defendant in a criminal case* is denied access, even through security-cleared counsel, the facts and law that are necessary to a determination of his Fourth Amendment rights and, ultimately, his liberty.

Indeed, most ironically, even the government has recognized that principle, albeit in the context of seeking authorization from the FISC to "potentially use and disclose" information and materials related to the Carter Page FISA surveillance. 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, at 1.

The government cited the need for disclosure in the context of the "ongoing and anticipated litigation with Page[,]" *id*., at 6, and in prescribing the parameters of such potential disclosure, the FISC agreed that "some permissible forms of use and disclosure of Page FISA information are reasonably anticipated here." *Id*.

In evaluating the government's request, the FISC noted that [t]he government also argues that "Congress did not intend FISA or . . . [FISA] minimization procedures . . . *to abrogate the rights afforded to defendants in criminal proceedings*" and submits without explanation "that the same reasoning would apply in civil proceedings." *Id*., at 8 (emphasis added) (citation omitted).

The FISC determined that "[i]nterpreting FISA's criminal prohibitions to hinder pursuit of its complementary civil remedies would violate the principle that "[s]tatutes should be interpreted as a symmetrical and coherent regulatory scheme." *Id*., at 13, *citing Mellouli v. Lynch*, 575 U.S. 798 (2015), (*quoting FDA v. Brown & Williamson Tobacco Com*., 529 U.S. 120, 133 (2000)).

In turn, the FISC concluded that "[i]t would be similarly anomalous to interpret [50 U.S.C.] §§1809(a)(2) and 1827(a)(2) as impeding a target of unlawful surveillance or search from pursuing civil remedies by preventing discovery of surveillance information necessary to prove the existence or scope of the surveillance." *Id*., at 13.[62]

Ultimately, the FISC ruled that §§1809(a)(2) and 1827(a)(2) did "not prohibit use or disclosure insofar as necessary for the good-faith conduct of litigation of any future claims brought by Page seeking redress for unlawful surveillance and search or disclosure of the results of such surveillance and search." *Id*.

[62] As the FISC noted, §§1809(a)(2) and 1827(a)(2) of FISA "restrict the use and disclosure of information acquired by unauthorized electronic surveillance or physical search that was conducted under color of a FISA authorization." June 25, 2020, Order, at 3.

Here, a criminal defendant like Mr. Hasbajrami, with a fundamental liberty interest at stake, should be afforded at least the same right of access (through security-cleared counsel) as a civil plaintiff seeking damages for unlawful surveillance that did not even lead to criminal charges.[63]

Accordingly, it is respectfully submitted that the Court should order disclosure to security-cleared defense counsel the FISA and FAA applications and supporting materials, including those related to backdoor searches, which will enable the Court to render its decisions with full

---

[63] Recent declassifications only reinforce the double standard that exists. For example, when it suited the Trump administration, the government publicly released portions of the Carter Page FISA applications – the first ever such disclosure. *See* Julian Sanchez, "Reforming the FISA Process: Tweak or Overhaul?" *Just Security*, June 30, 2021 ("*Tweak or Overhaul*"), available at https://bit.ly/3F2gVud. Similarly, in response to pressure from plaintiffs in the 9/11 civil litigation, the government ordered declassification of a trove of documents related to its investigation of possible Saudi Arabian assistance to 9/11 conspirators. *See* Exec. Order No. 14040, 86 FR 50439 (Sept. 9, 2021), available at https://bit.ly/3s7zI3H; Eric Lichtblau and James Risen, "9/11 and the Saudi Connection: Mounting evidence supports allegations that Saudi Arabia helped fund the 9/11 attacks," *The Intercept*, Sept. 11, 2021, available at https://bit.ly/3yye8GB. In addition, in response to pressure from the Supreme Court during oral argument in *United States v. Zubaydah*, No. 20-827 (Oct. 6, 2021), the government relaxed its classification decisions with respect to the torture Guantanamo Bay military commission defendants had suffered at CIA black sites. *See* Brief for the Respondent, *United States v. Zubaydah*, No. 20-827 (Oct. 6, 2021); Letter from Brian H. Fletcher, Acting Solicitor General, Office of the Solicitor General, DoJ, to Honorable Scott S. Harris, Clerk, Supreme Court of the United States (October 15, 2021), available at https://bit.ly/3sh0iaJ. *See also* Carol Rosenberg, "Some Sept. 11 Trial Secrets May Not Be Secrets Anymore," *The New York Times*, November 5, 2021, available at https://nyti.ms/329YS6x (prosecutors agreed to review redactions of materials produced to defendants in discovery to ensure that the documents were not redacted more than those declassified and produced in response to independent Freedom of Information Act requests).

These instances expose the government's penchant for a secrecy as a matter of tactics and expediency rather than genuine national security interests. It is respectfully submitted that those partisan and political considerations pale before the constitutional rights of a criminal defendant to a fair and adversary hearing on an issue materially affecting his liberty.

participation by defense counsel consistent with Due Process and the principles of the adversary system.[64]

F. *The Government's Self-Investigation and the FISC's Oversight Have Proven Inadequate and Unable to Stem the Tide of FISA and Section 702 Abuses*

The historical and intractable inability of the U.S. law enforcement and intelligence community to comply with FISA and, in that context, the Fourth Amendment – entailed in the various IG and other reports and FISC opinions discussed **ante**, throughout this memo of law – illustrates the impossibility of not only a wholly *ex parte* system operating by the rules, but also of that system policing and reforming itself.

As discussed **ante** and **post**, time and again the same non-compliance has been repeated without accountability or effective change. Allowing the agencies involved to cherry-pick which FISA applications and cases are reviewed for compliance, and the culture of minimizing non-compliance and the importance of protecting civil liberties simply has not been effective in improving the FISA process and eliminating abuses.

Also, as set forth below, the mechanisms designed for oversight purposes have not fulfilled their role(s) effectively. Neither the FISC nor the PCLOB nor Congress have been able to remediate the FISA process in any material or enduring fashion.

1. *The Government Agencies Responsible for Administering FISA Have Repeatedly Failed to Police and Reform Serial and Serious FISA Abuses*

The FBI and other agencies responsible for administering FISA have been impervious to reform because the FISC, while identifying non-compliance and abuse in a series of opinions, has

---

[64] *See also* Hon. James G. Carr, Op-Ed, "A Better Secret Court," *The New York Times*, July 23, 2013, available at https://nyti.ms/3m8aQoo.

yet to withhold approval for continuation and/or renewal of surveillance programs, including, specifically, Section 702 and backdoor searches. *See, e.g.*, Charlie Savage, "Court Approves Warrantless Surveillance Rules While Scolding F.B.I.," *The New York Times*, September 5, 2020, available at https://nyti.ms/2F2mI9h (the FISC "found that the F.B.I. had committed 'widespread violations' of rules intended to protect Americans' privacy when analysts search through a repository of emails gathered without a warrant, but it nevertheless signed off onanother year of the program, according to a newly declassified ruling [the *2020 FISC Op.*]").[65]

Although the FBI has since the 2011 surveillance in this case adopted strengthened rules at the FISC's insistence, the 2019 and 2020 FISC opinions describe how those rules are frequently violated, and how the FBI's systems are designed in ways that continue to multiply, rather than diminish, the intrusions on U.S. persons' communications. *See 2019 FISC Op.*, at 67-70, 81; *2020 FISC Op*., at 39-44; *see also 2017 FISC Op.*, at 80-84.

As the FISC lamented in the *2017 FISC Op*. "[t]oo often, however, the government fails to meet its obligation to provide prompt notification to the FISC when non-compliance is discovered. *See* FISA Ct. Rule of Procedure l 3(b)." *Id*., at 68 n.57. As the FISC explained, "it is unpersuasive to attribute – even 'in part' – an eleven-month delay in submitting a preliminary notice to 'NSA's efforts to develop remedial steps,' . . ., when the purpose of a preliminary notice is to advise the Court while investigation or remediation is still ongoing. *See also*, *e.g.*, February 28, 2017 Notice of a Compliance Incident Regarding Incomplete Purges of Information Obtained Pursuant to

---

[65] *The New York Times* has resorted to a variety of verbs to describe the annual phenomenon. *See* Charlie Savage, "Court Chides F.B.I., but Re-Approves Warrantless Surveillance Program," *The New York Times*, April 26, 2021, available at https://nyti.ms/3FlTITV. *See also* **ante**, at 78 ("upbraided").

Multiple FISA Authorities [] at 1-2, n.3 (five-month delay attributed 'to administrative issues surrounding the reorganization of NSA offices and personnel'). *Id*. (other citations omitted).

The *September 2021 DoJ OIG Audit* (*see* **ante**, at 73-74) also emphasized the failures of internal controls within FBI and NSD. For example, the audit expressed its "concerns with the FBI's and NSD's oversight efforts – specifically the need to be strategic, accountable, and timely." *Id*., at ii. The audit pointed out that "FBI and NSD conduct periodic reviews designed to ensure FISA applications contain accurate information[,]" but, as reflected in the *March 2020 DoJ OIG Management Advisory Memo* (*see* **ante**, at 69-73), "neither the FBI nor NSD used these tools to their full potential." *Id*. As a result, the *September 2021 DoJ OIG Audit* concluded that "FBI's decentralized oversight is a missed opportunity for ensuring accountability and efficacy of the Woods Procedures as a whole." *Id*.

Regarding the Woods Files reviewed, the *September 2021 DoJ OIG Audit* "observed that the Woods Files generally did not contain evidence of the thoroughness or completeness of this supervisory review." *Id*. As aresult, "[t]he widespread Woods Procedures non-compliance that we identified in this audit raises serious questions about the adequacy and execution of the SSA review process in place at the time of the applications we reviewed." *Id*.[66]

The *March 2020 Management Advisory Memorandum* portrayed an FBI that abjectly failed to utilize internal controls for their intended purposes:

---

[66] Part of the problem is that the FISA files subject to internal reviews are telegraphed in advance to FBI field offices. As the *March 2020 Management Advisory Memorandum* disclosed, prior to such reviews, "field offices are given advance notification of which FISA application(s) will be reviewed and are expected to compile documentary evidence to support the relevant FISA application(s)." *Id*., at 4.

> FBI OGC personnel told us, however, that the FBI CDC and NSD [Office of Intelligence] accuracy review reports had not been used in a comprehensive, strategic fashion by FBI Headquarters to assess the performance of individuals involved in and accountable for FISA applications, to identify trends in results of the reviews, or to contribute to an evaluation of the efficacy of quality assurance mechanisms intended to ensure that FISA applications were "scrupulously accurate." That is, the accuracy reviews were not being used by the FBI as a tool to help assess the FBI's compliance with its Woods Procedures.

March 2020 Management Advisory Memorandum, at 6.

The *September 2021 DoJ OIG Audit* also place the blame squarely on the lack of supervision and the weakness of internal controls:

> We believe that these shortcomings occurred primarily because the FBI and NSD generally did not place sufficient emphasis or attention on the need for rigorous supervisory review of a completed Woods File and robust oversight of the Woods Procedures during the time period covered by our review.

Id., at 7.

Likewise, the *September 2021 DoJ OIG Audit* remarked

> Internal oversight, like supervision, is an integral piece of the quality assurance process. Effective internal oversight should not only include the identification of errors or weaknesses in quality assurance but also the determination of what is causing the errors or weaknesses.

Id., at 20.

Nevertheless, the *September 2021 DoJ OIG Audit* concluded that "FBI and NSD have not used their existing internal oversight roles and mechanisms to their full potential, and this less than optimal oversight has resulted in submission to the FISC of FISA applications that do not meet the FBI's scrupulously accurate standard." *Id*. For example, "FBI does not have a designated entity that

is responsible for ensuring accountability and efficacy of the Woods Procedures across the FBI, which limits the effectiveness of the FBI's internal oversight abilities." *Id*., at 22.

Nor were the errors difficult for supervisors to discern. The *March 2020 Management Advisory Memorandum* pointed out that "FBI's comprehensive, strategic examination of the results of these reviews *would have put the FBI on notice* that the Woods Procedures were not consistently executed thoroughly and rigorously for applications submitted during our review period so as to help ensure the FBI's FISA applications were 'scrupulously accurate.'" *March 2020 Management Advisory Memorandum*, at 6 (emphasis added).[67]

The FBI's and NSD's reaction to the OIG's earlier December 2019 and March 2020 reports has also been problematic. According to the *September 2021 DoJ OIG Audit*, "certain public statements from FBI and NSD officials appeared to display a tolerance for error that is inconsistent with the FBI's policy that applications be scrupulously accurate." *Id*., at 7. *See also* Charlie Savage, "National Security Wiretap System Was Long Plagued by Risk of Errors and Omissions," *The New York Times*, February 23, 2020, available at https://nyti.ms/2Ta8aaM ("investigators have repeatedly misled judges over the years, documents and interviews show. When

[67] In August 2021, nearly 18 months after the *DoJ OIG's March 2020 Management Advisory Memorandum*, DoJ was still in the process of undertaking measures to ensure the integrity of its Woods Procedures. *See* Letter from Kevin O'Connor, Chief Oversight Section, Office of Intelligence, Department of Justice, to Judge Rudolph Contreras, United States Foreign Intelligence Surveillance Court (August 30, 2021), available at https://bit.ly/3q5lnCb ("FBI also is working on technological improvements related to its accuracy procedures, also known as the Woods Procedures, which will ultimately be integrated with" a new FISA-related workflow platform to which the FBI was transitioning).

such episodes have come to light, the Justice Department has blamed errors by or miscommunication with lower-level officials").[68]

In addition, "certain public statements from the FBI and NSD in 2020 failed to recognize the significant risks posed by systemic non-compliance with the Woods Procedures, and during our audit some FBI field personnel minimized the significance of Woods Procedures non-compliance." *Id*., at ii.[69]

Similarly, the *2019 FISC Op*. included an example of FBI's refusal to admit error, and instead to make transparently spurious arguments to the FISC. A query had enabled access to

---

[68] *The New York Times* reported in that February 2020 article, not without appropriate irony, that "[l]ast month, the F.B.I. promised Judge Boasberg to work harder to avoid errors. When [FBI's] general counsel, Dana Boente, signed the memo, he did not notice that whoever drafted it had misspelled his name").

[69] Unsurprisingly, in August 2020, after FBI and NSD conducted an internal review absolving the agencies of any errors that might have affected the validity of any FISA application, Assistant Attorney General for National Security John C. Demers stated in a DoJ press release,

> We are pleased that our review of these applications concluded that all contained sufficient basis for probable cause and uncovered only two material errors, neither of which invalidated the authorizations granted by the FISA Court. These findings, together with the more than 40 corrective actions undertaken by the Federal Bureau of Investigation and the National Security Division, should instill confidence in the FBI's use of FISA authorities.

Statement of Assistant Attorney General for National Security John C. Demers on the Public Release of the Department's Findings with Respect to the 29 FISA Applications that Were the Subject of the March 2020 OIG Preliminary Report, August 3, 2020, available at https://bit.ly/3E2Fgif. Certainly with unintended irony, however, in the public filing of the review, the "details of the errors, and [DoJ's] analysis of their materiality, was censored from the report." *See* Jeremy Gordon, "Justice Department Completes Review of Errors in FISA Applications," *Lawfare*, August 11, 2021, available at https://bit.ly/3F4ePd8.

"unminimized Section 702 information using the identifiers for approximately 16,000 persons." *2019 FISC Op*., at 67. 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*. (emphasis added). *See also id*., at 68 ("[t]here is no relevant distinction between queries and other broad, suspicionless queries previously identified by the government and the Com1 as violations of the querying standard"), *citing 2018 FISC Op*., 402 F. Supp.3d at 75-77.

Likewise, in response to the DoJ OIG's December 2019 report (discussed **ante**, at 62-69) and a December 17, 2019, Order from the FISC (*see* **post**, at 115), FBI Director Christopher Wray instituted 40 corrective measures to the FISA application process, yet the submission to the FISC announcing those actions itself demonstrated FBI's resistance to the rules governing FISA and Fourth Amendment. *See* FBI's (Unclassified) January10, 2020 Response to the Court's Order Dated December 17, 2019 ("*FBI Response*"), available at https://bit.ly/3plwFDh.

For instance, the *FBI Response* set forth the history of prior assurances of compliance, including institution of the Woods Procedures in 2001, *id*., at 4, as well as other documents mandating stringent compliance and reporting requirements that were repeatedly violated without enforcement of any internal discipline or implementation of altered procedures:

- a February 2, 2006, "additional guidance" FBI issued "to its personnel, reminding agents and analysts involved in submitting FISA applications that 'accuracy can only be insured by carefully cross-checking assertions which appear in the FISA declaration with source documentation.'" *FBI Response*, at 5, *(quoting Foreign*

Intelligence Surveillance Act Change in Procedures to Ensure Accuracy in Documents Submitted to the Foreign Intelligence Surveillance Court, Electronic Communication from Executive Assistant Director, National Security Branch, to all Field Offices, at 2 (Feb. 2, 2006));

- a March 24, 2006, letter to the FISC from DoJ's Office of Intelligence Policy and Review ("OIPR"), "advising the [FISC] of the efforts undertaken by the FBI and other members of the Intelligence Community 'to ensure that we include in our applications all of the information that is material to the case, and that all of the information reported in our applications is accurate.'" *FBI Response*, at 5, *(quoting* Letter from James A. Baker, Counsel for Intelligence Policy, to the Presiding Judge of the FISC, dated March 24, 2006); and
- a February 2009, guidance issued by NSD and FBI "to FBI and OI personnel that mandated specific practices and documentary requirements to ensure accuracy of facts in FISA applications, certain procedures that should be followed during the drafting of FISA applications to ensure accuracy, and the parameters of subsequent reviews for accuracy by OI personnel." *FBI Response*, at 6,)*quoting Guidance to Ensure the Accuracy of Federal Bureau of Investigation – Applications under the Foreign Intelligence Surveillance Act, Memorandum from Matthew G. Olsen & Valerie Caproni to all Office of Intelligence Attorneys, All National Security Law Branch Attorneys, and All Chief Division Counsels* (Feb. 11, 2009)).

Not satisfied, the FISC appointed as its "*amicus* attorney" David S. Kris, a former high-ranking DoJ national security lawyer with vast experience with FISA, *see* 945 F.3d at 650-54

(*citing* Mr. Kris's treatise), to evaluate the adequacy of those corrective measures. In a January 15, 2020, letter to FISC Chief Judge James E. Boasberg, Mr. 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.

Mr. 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. Mr. Kris added that "[t]he FBI's recent failures, however, are egregious enough to warrant serious consideration of significant reform." *Id*., at 8. That "significant reform" has not occurred despite continued evidence, in the *2020 FISC Op*., that non-compliance and abuses persist.[70]

Moreover, the failure of internal controls runs across the law enforcement and intelligence community that conducts FISA surveillance pursuant to appropriate minimization protocols. In December 2019, the NSA OIG "conducted [a] study to determine whether NSA's implementation of controls for aging-off signals intelligence (SIGINT) data is compliant with law and policy." *See* OFFICE OF THE INSPECTOR GENERAL, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, SPECIAL STUDY OF NSA CONTROLS TO COMPLY WITH SIGNALS INTELLIGENCE RETENTION

[70] The *2017 FISC Op*. reported that at an October 26, 2016, hearing (*see* **ante**, at 55-56), "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." *Id*., at 19-20. As a result, "[t]he 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*. Yet what followed were four more years of approvals.

REQUIREMENTS – UNCLASSIFIED SUMMARY 3 (December 12, 2019), available at https://bit.ly/3oWYPUJ.

The report stated that "[t]he OIG's findings reflect significant risks of noncompliance with legal and policy requirements for retention of SIGINT data." *Id*. Those "requirements include established minimization procedures for NSA SIGINT authorities, meaning that the deficiencies we identified have the potential to impact civil liberties and individual privacy." *Id*.

While NSA "implemented system compliance certification standards in 2010 to provide reasonable assurance that NSA systems operate in accordance with the laws and policies that address civil liberties and individual privacy[,]" *id*., at 4, nearly a decade later those standards had still not been met (or even fully implemented. *Id*., at 6 ("[p]lanned updates to NSA retention policy and implementation guidance have been delayed and do not incorporate all current legal and policy requirements").

Again, as with FBI and NSD, while "NSA has established an internal compliance standard for verification of age-off activities[,] . . . the OIG found that *the Agency's current oversight efforts and controls are insufficient to meet the standard and ensure compliance with data retention requirements*." *Id*., at 7 (emphasis added).

Consequently, FBI, NSD, and NSA have had ample opportunity to correct FISA's, and Section 702's, serious and recurring problems through supervision and internal review. They have failed to do so abysmally, and cannot be delegated that responsibility unilaterally to ensure compliance with the statutory and constitutional imperatives.[71]

---

[71] *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

2. *Criticism of the FISC's Ability to Perform Its Necessary Oversight Function*

Compounding the problem of *ex parte* review of FISA and FAA materials once a criminal prosecution is commenced are the FISC's historical institutional limitations as an independent factor in reining in abuse of FISA and FAA authority, and the fact that the FISC's capacity for oversight of Section 702 (50 U.S.C. §1881a) electronic surveillance, acquisition, and retention (including querying) is so narrowly defined by statute.

Regarding the former, unlike the judiciary's traditional threshold Fourth Amendment role as a gatekeeper for particular acts of surveillance, the FISC's role in Section 702 electronic surveillance is simply to ratify in advance the vaguest parameters pursuant to which the government is then free to conduct acquisition of communications for up to one year. In the alternative, the FISC also engages in dialogue with DoJ in order to amend applications with the objective of facilitating subsequent approval of re-submitted Section 702 minimization, targeting, querying, and other protocols. *See, e.g., 2018 FISC Op.*, at 92-94; *2020 FISC Op.*, at 38.[72]

---

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 Foreign Intelligence Surveillance Court imposed to remedy the resulting Fourth Amendment violation").

[72] A former NSA attorney has advanced the position that the FISC is powerless to deny Section 702 applications, but can only modify them in a manner that conforms them to statutory and constitutional standards. *See* George Croner, "To Oversee or to Overrule: What is the Role of the Foreign Intelligence Surveillance Court Under FISA Section 702?" *Lawfare*, May 18, 2021, available at https://bit.ly/325x8jB. Thus, according to Mr. Croner, even if the FISC concluded that certain proposed or already-conducted Section 702 surveillance and/or querying fundamentally violated the Fourth Amendment – for instance, because it involves the warrantless collection, querying, and use of U.S. persons' communications – the FISC could not simply deny the application, but instead would be limited to offering the government a means to "correct any deficiency identified." *Id.*, *citing* 50 U.S.C. §1881a(j)(3)(B)(I)

Nor, unlike courts discharging their requisite Fourth Amendment responsibilities, does the FISC consider individualized and particularized surveillance applications, or make individualized probable cause determinations, or supervise the implementation of the government's targeting or minimization procedures.[73]

In addition, as set forth **ante**, at 100, the government has even advanced the position that certain of the FISCR's decisions are not reviewable by the U.S. Supreme Court. *See ACLU v. United States*, 142 S. Ct. at 23 (Gorsuch, J., *dissenting from the denial of certiorari*).

Indeed, the FISC is for practical purposes at the mercy of the Executive agencies' willingness to be forthright and complete in their presentations to the FISC. As the *September 2021 DoJ IG Audit* recognized, at 2, "[d]uring its review of the application, the FISC relies on the government's declaration that the information supporting probable cause is factually sound[,]" admonishing that "[t]herefore, it is imperative that the FISC has confidence in the accuracy of the FISA applications submitted on behalf of the FBI."[74]

---

[73] Nor are judicial rulings from the FISC precedential, as they have not been issued in the context of "Cases" or "Controversies" within the constitutional meaning of Article III because only one party was involved. *See Camreta v. Greene*, 131 S. Ct. 2020, 2028 (2011) (authority to adjudicate legal disputes requires adverse litigants with the "concrete adverseness which sharpens the presentation of issues"), (*quoting Los Angeles v. Lyons*, 461 U.S. 95, 101 (1983)).

[74] As the *September 2021 DoJ OIG Audit* points out,

> FISC proceedings are *ex parte*, meaning that unlike most court proceedings, the government is present but the government's counterparty is not, and FISA orders generally are not subject to scrutiny through subsequent adversarial proceedings. As a result, the FBI and NSD FISA application process is critical to ensuring that DOJ officials asked to authorize FISA applications, and judges on the FISC asked to approve them, have a complete and accurate set of facts in the FISA application on which they can rely.

The FISC's response to the non-compliance and abuses detailed in the *DoJ OIG's December 2019 Report* illustrates the inability of the FISC to act as an effective brake on FISA violations. In a December 17, 2019, Order in *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, Docket No. Misc. 19-02, available at https://bit.ly/3p0zAB3, FISC Presiding Judge Collyer, noted that "[w]hen FBI personnel mislead NSD in the ways described [in the DoJ OIG's Report], they equally mislead the FISC." *Id*., at 1.

The Order endeavored to stress "the seriousness of that misconduct and its implications[,]" *id*., including documentation of "troubling instances[,]" *id*., at 2, and, citing from FISC opinions from 2007 through 2015, pointed out the government's duty of candor to the FISC, which it described as "fundamental to this Court's effective operations . . ." *Id*., at 2, *(quoting No. [Redacted], Mem . Op. and Order issued on Nov. 6 , 2015*, at 59 , available at https://bit.ly/3ytWi7K).

However, the Order also noted that the FISC first learned of certain of the misstatements and omissions as early as July 2018, and of others months prior to issuance of the *DoJ OIG's December 2019 Report*, yet acted only after the DoJ OIG's report was released publicly. *See id*., at 1 n.1.

Ultimately, the Order admonished that

> [t]he frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable.

Id., at 3.

Id., at I. *See also* **ante**, at 73-74.

Nevertheless, the Order entrusted the reliability of the materiality determination to that very same FBI. In addition, in a subsequent opinion, the FISC continued to authorize Section 702 surveillance *despite identifying continuing violations of the backdoor search protocols*. *See, e.g., 2020 FISC Op.*, at 41, 43-44 ("widespread violations of the querying standard" with "similar violations of Section 702(f)(2) likely hav[ing] occurred across the [FBI]").[75]

In fact, the *2020 FISC Op.* notes more than once that the violations described therein were the same as had occurred the previous year, and had even been pointed out in the *2019 FISC Op. See 2020 FISC Op.*, at 42-43. *See also Muhtorov*, 2021 WL 5817486, at *92 n.35 (Lucero, J., dissenting) ("[t]here is ample evidence that the Executive routinely fails to comply with the FISC-approved procedures without facing any sanction"), *citing 2020 FISC Op.* and *2018 FISC Op.*, at 76-82; Jake Laperruque, "Key Takeaways From Latest FISA Court Opinion on Section 702 and FBIWarrantless Queries," *Just Security*, April 28, 2021 ("*Laperruque: Key Takeaways*"), at 4, available at https://bit.ly/3Fp845R, at 1, 3 ("despite this long-running pattern" violations, FISC's continued approvals of FBI's querying procedures" leads to the conclusion that "even if we did expect the frequent compliance problems to be remedied, the newly declassified opinion shows the current court approval requirements are woefully inadequate").[76]

---

[75] The FISC stated its approval was due to its "lack[of] sufficient information at this time to assess the adequacy of the FBI system changes and training, post- implementation." *2020 FISC Op*., at 44. Notwithstanding a decade of persistent FBI non-compliance documented annually in the FISC's opinions, the FISC nevertheless determined that "[t]he number and nature of the reported querying violations nonetheless suggest that ongoing monitoring and auditing will be critical to evaluationg whether the current measures are adequate." *Id*.

[76] *See also* Order, *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, Docket No. Misc. 19-02, April 3, 2020, available at https://bit.ly/327oUHU (because "[t]he [*March 2020 Management Advisory Memorandum*] provides further reason for systemic concern[,]" ordering the government to report to the FISC whether any of the FISA applications

Consequently, in the wake of the disclosures of the Section 702's (and other FISA programs') vast and unprecedented dragnet approach to electronic surveillance, through the years the FISC has been the subject of much criticism and reconsideration.[77] As the Congressional Research Service notes, "[r]ecent controversies over the nature of the government's foreign surveillance activity have prompted some to argue that the judiciary's review of government surveillance requests under the Foreign Intelligence Surveillance Act of 1978 (FISA) should be far more exacting." Andrew Nolan, Richard M. Thompson II, and Vivian S. Chu, CONG. RESEARCH SERV., R43260, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE 2 (March 21, 2014), available at https://bit.ly/3s7y3Lv.

In fact, proposed reforms have focused on the absence of adversarial proceedings:

> lawmakers and others have suggested transforming FISA proceedings such that the process is more adversarial in nature. Critics of the current FISA proceedings have cited the infrequency of the FISC's rejections of government surveillance request as evidence that the lack of an adversarial process has prevented the court from fully and

---

in questions "involved material misstatements or omissions"). Naturally, the government's review exonerated itself. *See* **ante**, at n. 69.

[77] In addition to the sources discussed in the text above, *see also, e.g., Report on the FISA Amendments Act of 2008*, The Constitution Project, Liberty and Security Committee, September 6, 2012, available at https://bit.ly/3md49BB; *PCLOB Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act*, July 9, 2013, available at https://bit.ly/3oZZl4e; *Remarks prepared for the Oct. 2, 2013 Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Senate Committee on the Judiciary*, Professor Laura K. Donohue, Georgetown Law School, available at https://bit.ly/3H4T6Th (arguing that the "rather remarkable success rate" raises a "serious question about the extent to which FISC and [the Foreign Intelligence Surveillance Court of Review] perform the function they were envisioned to serve"); Stephen I. Vladeck, "It's Time To Fix the FISA Court (the Way Congress Intended)", MSNBC (Aug. 1, 2013), available at https://on.msnbc.com/3m9gV42; Connor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate*, 66 STANFORD LAW REVIEW (Feb. 2014), at *n. 2, available at https://stanford.io/3GJd45A

> properly scrutinizing the government's position. While some reject this line of reasoning, those who have found the *ex parte* nature of FISA proceedings troubling have argued that allowing another attorney to argue in opposition to the requests of the Department of Justice (DOJ) to conduct foreign intelligence activity would allow the FISC to better protect civil liberty interests.

Id., at 2-3. *See also id*., at Preamble ("[i]n response to concerns that the *ex parte* nature of many of the proceedings before the FISA courts prevents an adequate review of the government's legal positions, some have proposed establishing an office led by an attorney or 'public advocate' who would represent the civil liberties interests of the general public and oppose the government's applications for foreign surveillance").[78]

While the U.S.A. Freedom Act of 2015 established a process by which FISC judges *may* appoint an *amicus curiae* attorney to advise on legal issues in a limited number of cases (and with that lawyer's limited access to the factual information presented by the government to the FISC), *see* 50 U.S.C. §1803(I), that has not ameliorated the problems. Nor was such a function in place during the time frame of the surveillance and querying that captured and retrieved Mr. Hasbajrami's communications.

The FISC may appoint an *amicus* for "an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such

---

[78] Regarding the FISC's *ex parte* proceedings, *The New York Times* reported that Geoffrey R. Stone, professor of constitutional law at the University of Chicago, and co-author of *Liberty and Security In a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013, available at https://bit.ly/3q2Fxg3, "said he was troubled by the idea that the court is creating a significant body of law without hearing from anyone outside the government, forgoing the adversarial system that is a staple of the American justice system. 'That whole notion is missing in this process,' [Prof. Stone] said." Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *The New York Times*, July 6, 2013, available at https://nyti.ms/3yAWiCP.

appointment is not appropriate," 50 U.S.C. § 1803(i)(2)(A), or to "to provide technical expertise," 50 U.S.C. § 1803(i)(2)(B).

However, the role of the *amicus* is confined to the legal issues before the FISC, and "it does not extend to the impacts of proposed surveillance on privacy and civil liberties." "Foreign Intelligence Surveillance Court (FISC): The FISC *Amicus* Process," *Electronic Privacy Information Center*, available at https://bit.ly/3yv9tW5. Moreover, the *amicus* is not permitted to "represent U.S. persons subject to surveillance orders" or "petition FISC to certify a question of law to the FISCR for appellate review." *Id.* The *amicus*'s role is contingent upon the discretion of the FISC, both initially to be appointed and subsequently to have access to sufficient evidence to effectively participate. *Id.*, Faiza Patel and Raya Koreh, "Improve FISA on Civil Liberties by Strengthening Amici," *Just Security*, Feb. 26, 2021, available at https://bit.ly/3oXhujk.

Despite the 2015 U.S.A. Freedom Act authorizing the FISC to designate five or more individuals with expertise in privacy, technology, intelligence, and / or civil liberties to serve as *amicus curiae*, 50 U.S.C. § 1803(i)(3)(A), "[a]s of May 14, 2020, the FISC had only appointed *amici* about sixteen times since the 2015 Act passed . . . [and] had not appointed an *amicus* in any case involving an individual surveillance application." "Foreign Intelligence Surveillance Court (FISC)," Electronic Privacy Information Center, available at https://bit.ly/3yv9tW5.[79]

While Congress and others debate whether adversarial proceedings should be instituted in the FISC at *front end* of the FISA and FAA process, there remains no good rationale for continuing *ex parte* proceedings at the *back end*, in the federal courts in the context of criminal prosecutions

[79] Efforts to expand the role of *amici curiae* in FISA cases have repeatedly been blocked. *See, e.g.*, Jake Laperruque, "The Justice Department's Unconvincing Explanation for Its Reversal on FISA," *Lawfare*, May 29, 2020, available at https://bit.ly/33pQwbE.

when, as here, a defendant's liberty is being infringed and the evidence the government seeks to use either consists of or is derived from FISA or FAA surveillance and acquisition.

Since the revelations by Edward Snowden in 2013, Congress has assumed a more active oversight role, but resistance from large sectors of the House and Senate have stymied the level of reform required. *See, e.g.,* Susan Landau and Asaf Lubin, *Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?*, 11 HARVARD NATIONAL SECURITY JOURNAL 308 (2020), at *350-57, available at https://bit.ly/30CHEyA; Sharon Bradford Franklin, "Rethinking Surveillance on the 20th Anniversary of the Patriot Act," *Just Security*, Oct. 26, 2021, available at https://bit.ly/3q3LnOk; Ellen Nakashima, "NSA surveillance program still raises privacy concerns years after exposure, member of privacy watchdog says," *Washington Post*, June 29, 2021, available at https://wapo.st/3q1LdH7; Patrick Eddington, "The Snowden Effect, Six Years On," *Just Security,* (June 6, 2019, available at https://bit.ly/3sg1tXJ.

Also, again, that interest, further invigorated by the DoJ IG's report regarding the Carter Page FISA applications, *see* **ante**, at 62-69, was neither evident nor a factor during the period of the interception and querying of Mr. Hasbajrami's communications. *See, e.g.*, Margaret Taylor, "The Specter of FISA Reform Haunts Capitol Hill," *Lawfare*, May 29, 2020, available at https://bit.ly/3q1Lnyd; Elizabeth Goitein, Andrew G. McCabe, Mary B. McCord, and Julian Sanchez, "Top Experts Analyze Inspector General Report Finding Problems in FBI Surveillance," *Just Security*, Apr. 27, 2020, available at https://bit.ly/3yz3rU4.

Congress's oversight capacity is also impaired by the lack of accurate or reliable information. The undercounting that is a feature of government reporting, *see*, *e.g.*, **ante**, at 15 & n.5, provides a level of comfort and assurance that is not warranted. *See Laperruque: Key Takeaways*, at 4 ("[i]f

Congress had accurate data on how common law enforcement queries returning Section 702-acquired information were during previous legislative debates on this issue, the restrictions it imposed might have been stricter").

Nor are other organs created for oversight purposes capable or even empowered to penetrate the insular and essentially unrestrained FISA process that generates abuses. Indeed, the PCLOB even lacked a quorum for much of 2017 and 2018, and has been criticized for its recent passivity. *See* Justin Doubleday, "Privacy, technology groups urge Biden to revive surveillance oversight board," *Federal News Network*, September 8, 2021, available at https://bit.ly/3IVecVK ("[t]he panel currently has two members, but needs at least three of its five seats filled to reach the quorum necessary to issue reports and launch new investigations. The Senate would have to confirm any nominees that Biden puts forward").[80]

A September 8, 2021, letter from "the American Civil Liberties Union, the Project On Government Oversight and 17 other groups urged [President Biden] to appoint three new members to the board 'as expeditiously as possible and with nominees that will vigorously protect privacy and civil liberties while upholding government transparency.'" *Id.* *See also* September 8, 2021, Coalition Letter, available at https://bit.ly/3m9loUm.[81]

---

[80] *See also* "Additional Unclassified Statement by Board Member Travis LeBlanc, March 12, 2021," at 1, available at bit.ly/35Z8RdF (PCLOB member dissenting from PCLOB report regarding a surveillance program, XKEYSCORE, because it was issued "without adequate investigation, analysis, review, or process," including with respect to the program's querying process, which Mr. LeBlanc deemed "worthy of review for separate legal analysis, training, compliance, and audit processes"). *See also id.*, at 6 ("[e]ffective oversight necessitates a robust investigation into the efficacy of the programs we oversee. The Board's former majority has failed to do that").

[81] PCLOB's Chair published a unilateral "white paper" in June 2021 that again left to intelligence community insiders the role of any effective oversight, and was more concerned with

Thus, neither the FISC nor Congress nor any commission has been willing or able to confront the problems each have recognized with the administration of FISA and Section 702. It has been left to this Court, with the assistance of security-cleared defense counsel if this Court permits, to do so, and not merely another legion of insiders who have ignored every directive to that effect.

G. *The Nature and Type of Disclosure This Court Should Order the Government to Provide Herein*

The Second Circuit's opinion contemplates a thorough fact-finding by this Court. *See, e.g., Hasbajrami*, 945 F.3d at 661, 677. *See also* **ante**, at 27-30. In order to conduct that review, in addition to receiving (and disclosing to security-cleared defense counsel) the materials voluntarily provided by the government, it is respectfully submitted that this Court should require the government to disclose the following information, all of which is relevant to whether the surveillance, including querying, was reasonable under the Fourth Amendment:

(1) information about the rules and procedures governing the querying and use of Section 702 information at the time Mr. Hasbajrami was investigated;

(2) each of the Section 702 queries FBI agents or analysts conducted that sought or produced information about Mr. Hasbajrami;

(3) what query terms were used by FBI, when, and by whom;

---

streamlining internal reviews in order not to tax DoJ and FBI resources than with measures that would ensure elimination of FISA non-compliance and abuses. *See* ADAM I. KLEIN, PCLOB, CHAIRMAN'S WHITE PAPER: OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (June 2021), available at https://bit.ly/33pQL6y. *But see Tweak or Overhaul* (Mr. Klein's "modest procedural tweaks . . . do not, in my view, get at the root cause of dysfunction in the FISA process: the fact that 'FISA applications are not tested in the adversarial process, and FISA surveillance is classified'").

(4) what databases were searched by FBI, and with respect to the Section 702-acquired data in these databases, what was the volume of that data, how many communications were included, and how many individuals' communications were included;

(5) what justifications and/or reasons did FBI agents or analysts provide for the queries;

(6) did the FISA applications, the renewal applications, and/or the querying process, include or account for "information to suggest that Individual #1 was not in fact a terrorist, and that he solicited funds from the defendant for purposes unrelated to terrorism." *See* PSR, at ¶ 3. *See also* **ante**, at 6, 67;

(7) what information did the FBI queries produce;

(8) who gained access to that information, when, and with what justification;

(9) with whom was that information shared, when, and with what justification(s);

(10) what queries were made by other intelligence agencies, including NSA and CIA;

(11) what query terms were used by personnel from those agencies, when, and by whom;

(12) what databases were searched by personnel from those agencies, and with respect to the Section 702-acquired data in these databases, what was the volume of that data, how many communications were included, how many individuals' communications were included;

(13) what justifications did those agencies' agents or analysis provide for the queries;

(14) what information did those agencies' queries produce;

(15) who gained access to that information, when, and with what justification;

(16) with whom was that information shared, when, and with what justifications;

(17) the circumstances of the retention of Mr. Hasbajrami's communications intercepted/collected pursuant to Section 702;

(18) details regarding how information gleaned from the queries was used in the government's investigation of Mr. Hasbajrami; and

(19) a list of the full range of investigative techniques and measures used in the investigation of Mr. Hasbajrami.

H. ***The Impact on Mr. Hasbajrami's Conditional Plea of Guilty***

The Circuit recognized in its opinion that should Mr. Hasbajrami prevail, and the evidence be suppressed, he would be entitled to withdraw his guilty plea, *Hasbajrami*, 945 F.3d 675-76, which would be a formality because it is believed that the entirety of the government's case – or at least that portion that would render it legally sufficient – against Mr. Hasbajrami emanates in some fashion from the Section 702 surveillance and any subsequent backdoor searches.

Accordingly, Mr. Hasbajrami's guilty plea would be withdrawn concurrent with dismissal of the prosecution against him outright.

POINT II

MR. HASBAJRAMI IS ENTITLED TO NOTICE OF THE ELECTRONIC SURVEILLANCE TECHNIQUES THE GOVERNMENT EMPLOYED IN ITS INVESTIGATION

The Constitution, applicable statutes, and the Federal Rules of Criminal Procedure entitle Mr. Hasbajrami to notice of whatever *other* surveillance tools, including a definitive answer with respect to backdoor searches, the government utilized in its investigation(s) of Mr. Hasbajrami beyond the simple Section 702 and traditional FISA interceptions.

A. *Notice Is Required By the Constitution*

Subsequent to the Second Circuit's decision herein, the Ninth Circuit, in *United States v. Moalin,* 973 F.3d 977, 997-1001 (9th Cir. 2020), ruled that that the Fourth Amendment required the government to provide notice of its collection and use of a defendant's telephone metadata under Section 215, as well as other forms of foreign intelligence surveillance.

As the Court stated

> [T]he Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence surveillance authorities.

Moalin, 973 F.3d at 1000.

In fact, the circumstances replicate in many respects the collection/querying circumstances present here: the defendant's (as well as essentially all persons in the U.S.'s) call records were collected pursuant to Section 215. *See also ACLU v. Clapper*, 785 F.3d at 826. In *Moalin*, that metadata was resident in a database the government subsequently searched to match defendant's telephone number with that which was a party to a suspicious call. *See Moalin*, 973 F.3d at 987-88.[82]

The constitutional imperative of notice is a longstanding principle. The Supreme Court and appellate courts have long recognized that the Constitution requires notice of government searches

---

[82] In *Moalin*, while the Court determined, on the basis of the classified record, that any lack of notice was not prejudicial to the defendants, its Fourth Amendment holding supports Mr. Hasbajrami's right to notice here. *Moalin*, 973 F.3d at 1001. The Court's decision in *Moalin* not to remand the case to the District Court for *Alderman* disclosures and a suppression hearing was based on "the particular circumstances of [the *Moalin*] case," and "in a different case," disclosure under *Alderman* might be required in order for the defense to "intelligently litigate" a challenge to unlawful surveillance – including the government's collection of metadata. *Id*.

– especially surreptitious searches. *See Berger*, 388 U.S. at 60; *Dalia v. United States*, 441 U.S. 238, 247-48 (1979); *United States v. Donovan*, 429 U.S. 413, 429-30 & n.19 (1977) (Title III's notice provisions "satisfy constitutional requirements"); *United States v. Chun*, 503 F.2d 533, 536-38 & n.6 (9th Cir. 1974) (same).

Although *Berger* and *Dalia* do not require disclosure of each minute technical detail involved in the surveillance, those two cases do require notice of basic information about the searches, so that (among other things) a defendant may bring an informed motion to suppress. *See Berger*, 388 U.S. at 60; *Dalia*, 441 U.S. at 247-48.

In addition, the government's Fifth Amendment Due Process obligation pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963), requires disclosure of information that could affect the outcome of a suppression hearing. *See United States v. Gamez-Orduno*, 235 F.3d 353, 461 (9th Cir. 2000); *Smith v. Black*, 904 F. 2d 950, 965-66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992).

Reliance on overbroad and contrived claims of secrecy to refuse to produce such material and information denies Mr. Hasbajrami Due Process. Exaggerated or false claims of the need for secrecy cannot overcome a defendant's constitutional interest in an adversarial proceeding that ensures it will be fair and accurate. *See Roviaro v. United States*, 353 U.S. at 60-61; *Matthews v. Eldridge*, 424 U.S. 319, 335 (1976). *See also* James Bovard, "Supreme Court Should End 'State Secrets' Privilege," *The American Conservative*, November 16, 2021, available at https://bit.ly/3q52a3k

("State Secrets doctrine provides a license for federal agencies to lie to their victims and to federal judges").[83]

B. ***Notice Is Required By the Federal Statutes and Rules***

Notice is also mandated by 18 U.S.C. §3504, and does not permit the government to condition notice on its own determination of whether its evidence was tainted.[84] Rather, upon a colorable claim like Mr. Hasbajrami's, the statute requires the government to affirm or deny the precise forms of surveillance. *See* 18 U.S.C. §3504(a)(1); *United States v. Apple*, 915 F.2d 899, 904-06 (4th Cir. 1990). At that point it is incumbent upon the parties to litigate whether the surveillance was unlawful, and which evidence flowed from it. *See United States v. Hamide*, 914 F.2d 1147, 1149 (9th Cir. 1990); *Apple*, 915 F.3d at 906, 909-10.

As the Court in *Muhtorov* explained, 18 U.S.C. §3504 "contemplates a multi-step process. The defendant must allege unlawful use. If the allegations are sufficient to require a response, the

---

[83] In his article, Mr. Bovard observes that a case currently before the Supreme Court in a civil context, *Husayn v. Mitchell*, 938 F.3d 1123 (2nd Cir. 2021), *cert. granted United States v. Zubaydah*, No. 20-827 (Oct. 6, 2021), offers "a superb opportunity to debunk that pernicious legal doctrine that has become a protective wall around the worst abuses of the war on terror[,]" as "[t]he FBI has been able to trample Americans' rights and privacy because it shrouds its abuses." The article also notes that the case establishing the state secrets privilege, *Reynolds v. United States*, 345 U.S. 1 (1953), involved a false claim of national security to hide a cover-up of the crash of a B-29 bomber. The Air Force said that any disclosure of the case would expose vital national security secrets, and the Court deferred to the military. Half a century later, the government declassified the official report which contained no national security secrets but proved that negligence caused the crash. *Id*. *See also* BARRY SIEGEL, CLAIM OF PRIVILEGE (2008).

[84] 18 U.S.C. §3504(a)(1) reads as follows: "upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act[]."

government issues a confirmation or denial. The court must then weigh whether disclosure is warranted based on the sufficiency of the government's explanation." 2021 WL 785 F.3d 787, at *45

Such notice is also required under Rule 16(a)(1)(E)'s "materiality" provision. Rule 16(a)(1)(E) plainly "permits discovery related to the constitutionality of a search or seizure." *United States v. Soto-Zuniga*, 837 F.3d 992, 998, 1000-01 (9th Cir. 2016). *See also United States v. Hanna*, 661 F.3d 271, 295 (6th Cir. 2011) (information is discoverable if it is "relevant" and "helpful" to a motion to suppress).

In addition, even under statutorily authorized programs, the government regularly conceals certain pivotal aspects of its electronic surveillance and evidence collection. *See* Charlie Savage, "Door May Open for Challenge to Secret Wiretaps," *The New York Times*, October 16, 2013, available at http://nyti.ms/1r7mbDy (describing government's continuing efforts to avoid giving notice of Executive Order 12,333 surveillance); *id*. (describing government's five-year effort to avoid giving notice of FAA surveillance such as occurred herein). *See also Dark Side: Secret Origins of Evidence in U.S. Criminal Cases*, Human Rights Watch, January 9, 2018, at *1, available at https://bit.ly/3DZAcuT ("a growing body of evidence suggests" that U.S. intelligence agencies obtain information about U.S. persons "incidentally" through foreign intelligence surveillance, share it with federal, state, and/or local law enforcement agencies, which then "re-discover[] the evidence in some other way" to create an alternative, sanitized version of how the information was acquired"); John Shiffman & Kristina Cooke, "U.S. Directs Agents to Cover Up Program Used to Investigate Americans," *Reuters*, August 5, 2013, available at http://reut.rs/15xWJwH (describing "parallel construction" as "just like money laundering – you work it backwards to make it clean"); *id*. ("[a]lthough these case rarely involve national security issues, documents reviewed by *Reuters* show

that law enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges"); Ronan Farrow, "How a C.I.A. Coverup Targeted a Whistle-blower," *The New Yorker*, October 30, 2020, available at https://bit.ly/3F7t54X (DoJ whistleblower "realized that C.I.A. officers and F.B.I. agents, in violation of federal law and Department of Justice guidelines, had concealed the information's origins from federal prosecutors, leaving judges and defense lawyers in the dark. Critics call such concealment 'intelligence laundering'").[85]

Even in the FISA context of national security, effective notice is not a shell game in which a defendant must guess at which programs or techniques the government has employed, and whether they contributed in some fashion to the government's investigation. *See* 50 U.S.C. § 1806(c) (FIFA); 18 U.S.C. § 2518(8)(d) (Title III). Accordingly, Mr. Hasbajrami is entitled to notice and the opportunity to challenge the surveillance tools that the government used in its investigation.[86]

---

[85] Due Process rights grounded in the Fourth and Fifth Amendments entitle criminal defendants to know how the government monitored their communications and activities, and then to challenge – in an adversarial proceeding – whether the government's evidence has been derived from that surveillance, and to seek suppression of the resulting evidence that was obtained unlawfully. *See, e.g.*, *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972); *Alderman v. United States*, 394 U.S. 165 (1969). *See also United States v. Gelbard*, 408 U.S. 41 (1972). *See also Wong Sun,* 371 U.S. at 486-88 (describing "fruit of the poisonous tree" doctrine); *Murray v. United States*, 487 U.S. 533, 536-37 (1988) (describing right to seek suppression of evidence "derived" from an unlawful search).

[86] Even beyond this case, the government's withholding of notice of electronic surveillance is now widespread. *See generally* Patrick C. Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 865-895 (2014).

Conclusion

Accordingly, it is respectfully submitted that the Court should order disclosure and discovery of the relevant materials to security-cleared defense counsel, and, ultimately, grant Mr. Hasbajrami's motion to suppress.

Dated: 23 December 2021
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

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

Attorneys for Defendant Agron Hasbajrami

– On the Brief –

Joshua L. Dratel
Michael K. Bachrach