~~TOP SECRET~~ [redacted]

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Filed with Classified Information Security Officer
CISO
Date 12/12/24

UNITED STATES OF AMERICA,

- against -

AGRON HASBAJRAMI,

Defendant.

MEMORANDUM AND ORDER

1:11-cr-623 (LDH)

LASHANN DEARCY HALL, United States District Judge:

Agron Hasbajrami ("Defendant") was arrested on September 6, 2011, as he attempted to board a flight to Turkey at John F. Kennedy International Airport in Queens, New York.[1] *United States v. Hasbajrami*, 945 F.3d 641, 645 (2d Cir. 2019). The government charged Defendant with attempting to provide material support to a terrorist organization, alleging that he intended to travel to the Federally Administered Tribal Area of Pakistan, where he expected to join a terrorist organization, receive training, and ultimately fight against U.S. forces and others in Afghanistan and Pakistan. *Id.* During the prosecution, the government disclosed that it had collected Defendant's electronic communications under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978), codified at 50 U.S.C. § 1801 *et seq.*, and that it intended to introduce FISA-derived evidence at any eventual trial. *Id.* Defendant pleaded guilty to attempting to provide material support to terrorists in violation of 18 U.S.C. § 2339A, and was sentenced to 180 months' imprisonment. *Id.*

After Defendant was already serving his sentence, the government disclosed for the first time that some of the evidence it had previously disclosed from FISA surveillance was itself the

[1] The following facts, as relevant to deciding the instant motion, are taken from Second Circuit's opinion. *United States v. Hasbajrami*, 945 F.3d 641, 647–60 (2d Cir. 2019).

fruit of earlier information obtained without a warrant pursuant to Section 702 of the FISA Amendments Act, 50 U.S.C. § 1881a *et seq.* ("Section 702"). *Id.* Following this disclosure, then-district court Judge John Gleeson permitted Defendant to withdraw his guilty plea, and Defendant moved to suppress evidence seized by the government under Section 702 and any fruits thereof. *Id.* Judge Gleeson denied the motion to suppress. *United States v. Hasbajrami*, No. 11-CR-623, 2016 WL 1029500, at *14 (E.D.N.Y. Mar. 8, 2016). Defendant again pleaded guilty, on the condition that he could appeal denial of the suppression motion. *Hasbajrami*, 945 F.3d at 645. On appeal, the United States Court of Appeals for the Second Circuit, largely affirmed the district court's denial of the suppression motion but remanded on issues specific to querying Section 702-acquired information. *Id.* at 645–46.

I. BACKGROUND

A. Section 702

Section 702 authorizes targeted intelligence collection of certain electronic communications with the compelled assistance of electronic communication service providers. *See* 50 U.S.C. § 1881a(a). Section 702 is extremely complex, and provides for a mechanism that allows multiple agencies to collect various types of information for a multitude of purposes. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* ("PCLOB Report") at 2 (July 2, 2014).[2] The history of Section 702 traces back to FISA's passage in 1978. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013). Through FISA, Congress created two specialized courts—the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review ("FISCR"). The FISC approves electronic surveillance for foreign

[2] https://www.pclob.gov/library/702-Report.pdf.

intelligence purposes where probable cause exists that "the target of the electronic surveillance is a foreign power or an 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." *Id.* (citing § 105(a)(3), 92 Stat. 1790; *see* § 105(b)(1)(A), (h)(1)(B)). The FISCR maintains jurisdiction to review any FISC denials of applications for electronic surveillance. *Id.* (citing § 103(b), 92 Stat. 1788).

Following the September 11, 2001 terrorist attacks, the government determined that FISA's requirement of a court order supported by probable cause "unduly restrict[ed the] speed and agility" with which the government could detect and respond to terrorist threats." *See* David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions ("Kris & Wilson") § 16:2 (internal quotation marks omitted). As such, President George W. Bush began to issue a series of highly classified authorizations directing the NSA to collect certain foreign intelligence by electronic surveillance, without a warrant, to prevent acts of terrorism within the United States. PCLOB Report at 16. These authorizations came to be known as the "President's Surveillance Program." *Id.* Over time, the President's Surveillance Program "became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool." *Id.* at 16–17 (citation omitted). In 2005, part of the President's Surveillance Program was revealed to the public, which prompted the White House to seek authorization under FISA to conduct the content collection that had been occurring. *Id.* at 17.

In January 2007, FISC issued orders authorizing the government to conduct certain electronic surveillance of telephone and internet communications carried over listed communication facilities. *Id.* To receive those authorizations, the government was required to make a probable cause determination regarding one of the communicants and determine that the

email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States. *Id.* These FISC orders effectively replaced authorization of the President's Surveillance Program. *Id.* Furthermore, these FISC orders subjected any electronic surveillance that was then occurring under the NSA's program to the approval of the FISC. *See Clapper*, 568 U.S. at 403. After a FISC judge subsequently narrowed authorization of such surveillance, the White House asked Congress to amend FISA to provide the intelligence community with additional authority addressing modern technology and international terrorism. *Id.* at 403–04.

In 2008, Congress responded by enacting Section 702 as an amendment to FISA. While Section 702 largely left FISA in-tact, it "established a new and independent source of intelligence collection authority for the United States government, beyond that granted in traditional FISA." Kris & Wilson § 17:1. In short, Section 702 permits the Attorney General ("AG") and the Director of National Intelligence ("DNI") to jointly authorize surveillance targeting of persons who are not U.S. persons[3], and who are reasonably believed to be located outside the United States, with the compelled assistance of electronic communication service providers, to acquire foreign intelligence information. *See* 50 U.S.C. § 1881a(a). Rather than identify particular individuals to be targeted under Section 702, the AG and DNI submit certifications to FISC identifying categories of foreign intelligence information to be collected, leaving the agencies to determine particular targets consistent with the certifications. *See* PCLOB Report at 24–25. Notably, there is no requirement that the government demonstrate probable cause that a Section 702 target is a foreign power or agent of a foreign power. *Id.*

[3] A U.S. person is defined as "a citizen of the United States, an alien lawfully admitted for permanent residence" or certain unincorporated associations or corporations with ties to the United States. *See* 50 U.S.C. § 1801(i).

Thus, Section 702 differs significantly from traditional FISA surveillance, which requires approval from a FISC judge based on probable cause that an individual is an agent of a foreign power. *Id.* at 104, 115–16.

Once FISC approves Section 702 certifications and procedures, Section 702 unfolds in several steps at the agency level. *First*, individuals are designated for surveillance under the FISC-approved targeting procedures. *Id.* 41–47. Targeting procedures are designed to ensure that any authorized acquisition is "limited to targeting persons reasonably believed to be located outside the United States to acquire foreign intelligence information" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). Put another way, the government may not "intentionally target" anyone located in the United States or a "United States person" outside the United States. 50 U.S.C. §§ 1881a(b)(1), (3). Nor may the government engage in "reverse targeting" of U.S. persons by targeting someone outside the country simply to collect communications with someone inside the United States. 50 U.S.C. § 1881a(b)(2).

The NSA initiates all Section 702 targeting by tasking a specific "selector" for surveillance, which typically consists of an email address or telephone number. *See* PCLOB Report at 42, 111. While an oversight team from the executive branch later reviews each targeting decision to ensure targeting procedures are followed, FISC does not approve individual targeting decisions or review them after they are made. PCLOB Report at 111. [redacted]

[redacted]

[redacted]. Because the NSA ultimately decides whether to task selectors for acquisition, the NSA is responsible for making the requisite foreignness and foreign intelligence purpose determinations. *Id.* at 43–45, 47.

Second, after selectors are targeted, the NSA initiates collection with the compelled assistance of internet service providers. PCLOB Report at 7, 42. Although Section 702 limits surveillance to non-U.S. persons located abroad, communications involving U.S. persons may nonetheless be intercepted. For example, when a U.S. person is communicating with a targeted individual, those communications may be "incidentally" acquired. *Id.* at 6. Communications may also be collected "inadvertently" where a U.S. person is mistakenly targeted. *Id.*

Third, after communications are collected, they are processed under "minimization" procedures maintained by each agency and "best understood as a set of controls on data to balance privacy and national security interests." *Id.* at 50. Accordingly, minimization procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1).[5] [redacted]

[4] The FBI also maintains its own targeting procedures. PCLOB Report at 42, 47.

[5] For example, pursuant to declassified 2011 NSA minimization procedures, NSA analysts will determine whether an acquired communication "is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." *See Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended* ("NSA 2011 Minimization Procedures") § 3(b)(4) (Oct. 31, 2011). Communications fitting that description will be retained; otherwise, the information is destroyed. *Id.* § 3(b)(1).

[redacted]. Unminimized communications have not been reviewed by any agent or analyst to determine whether it meets the criteria for retention. *See* PCLOB Report at 54.

Fourth, once communications are collected or disseminated, each agency establishes databases to store and search among those communications by "querying." *Id.* at 55–56. Querying typically refers to searching unminimized material by using a query "term" or "identifier," similar to an internet search engine. *Id.* at 55. Query terms, for example, could be an email address, telephone number, or other key word. *Id.* Each agency permits the querying of unminimized information, subject to internal procedures, by analysts or agents who have appropriate training and authorization to access the data. *See id.*[6]

B. Querying as to Defendant

In this case, the Government submitted a supplemental record to the Court with evidence of Section 702 querying related to Defendant. The supplemental record primarily consists of [redacted] declarations, [redacted]. These declarations describe querying conducted [redacted] as to Defendant. They also outline the timeline of the investigation into Defendant and, in part, how querying affected the investigation.[7] (Class. Gov. Mem. at 8.)

[redacted]

[6] For example, an FBI agent untrained to view unminimized information would be notified when running a query that responsive information was found, though the agent would need to either take the requisite training or contact a trained agent to access the queried information. PCLOB Report at 56.

[7] The Court, in the interest of transparency, cites to the public and unclassified version of the Government's opposition wherever possible. Any citations to the Government's classified brief are represented as "Class. Gov. Mem."

[redacted]

[redacted]

[redacted]

[redacted]

On or about April 28, 2011, [redacted] conduct checks in the [redacted] an unclassified database, in connection with Defendant. (*Id.* ¶ 27.) On or about April 29, 2011, [redacted] to conduct a search of a criminal records database for Defendant. (*Id.* ¶ 28.) That database did not contain any Section 702-acquired information. (*Id.*) [redacted]

[redacted] In addition, once the investigation was opened, [redacted] ran "checks of law enforcement and publicly available databases" for information on Defendant. (*Id.* ¶ 30.) [redacted] interviewed Defendant on May 3, 2011 and began physical surveillance of him the next day. (*Id.*)

[redacted]

[redacted]

[redacted] conducted a search of Defendant's home on September 6, 2011, the application for which did not contain Section 702-acquired information. (*Id.* ¶ 38.) Defendant was arrested that same day. (*Id.*)

[redacted]

[redacted]

C. Second Circuit Opinion

After learning that the government obtained Section 702-acquired information without a warrant, Defendant moved to suppress "the fruits of all warrantless FAA surveillance," including evidence derived from the government's Section 702 surveillance and evidence derived from FISA collection that was also derived from Section 702. *Hasbajrami*, 945 F.3d at 648–49. Judge Gleeson primarily addressed the issue of collection and treated the suppression motion as an as-applied challenge to the Section 702 surveillance used to support the Government's initial FISA application. *Id.* at 658. While the district court acknowledged that Defendant was a legal permanent resident located in the United States, the targets of Section 702 surveillance were non-U.S. persons. *Id.* at 658–59. Accordingly, Judge Gleeson found the incidental collection of

Defendant's communications to be lawful because the surveillance was "lawful in the first place." *Id.* at 659.

On appeal, the Second Circuit considered whether the incidental collection of communications by U.S. persons—which constituted the "vast majority" of the information collected from Defendant—violates the Fourth Amendment. *Id.* at 646, 661. Defendant argued that surveillance of individuals within the United States is per se unreasonable without a warrant and that Section 702 generally violates the Fourth Amendment. *Id.* at 662. The Second Circuit found the incidental collection did not require a warrant because the Fourth Amendment does not apply extraterritorially, and where the government lawfully collects communications from a foreign individual but learns the target is communicating with a U.S. person, the government may continue intercepting those communications without a warrant pursuant to the "incidental overhear" doctrine.[9] *Id.* at 662–66. Moreover, the incidental collection here was reasonable, even absent a warrant, considering the national security needs at stake. *Id.* at 666–68.

The government also collected some of Defendant's communications inadvertently, that is, mistakenly based on the presumption that he was a non-U.S. person. *Id.* at 668. Although the district court did not address communications inadvertently collected from Defendant, the Second Circuit nonetheless found that failure to suppress such evidence was harmless because the inadvertent targeting was brief and not used to support the FISA warrants. *Id.* at 669.

Finally, the Second Circuit considered querying of Section 702-acquired information as to Defendant. *Id.* The district court did not make any findings regarding whether any agency

[9] Elaborating on the incidental overhear doctrine, the Second Circuit explained: "The Fourth Amendment generally is not violated when law enforcement officers, having lawfully undertaken electronic surveillance, whether under the authority of a warrant or an exception to the warrant requirement, discover and seize either evidence of criminal activity that they would not have had probable cause to search for in the first place, or the relevant conversations of an individual they did not anticipate or name in a warrant application." *Hasbajrami*, 945 F.3d at 663.

queried databases prior to the FISC order. *Id.* Instead, the district court appeared to accept the Government's argument that it could freely query information it had lawfully acquired without further Fourth Amendment inquiry. *Id.* The Government renewed this argument on appeal, and at oral argument before the Second Circuit, the Government would neither confirm nor deny whether it had queried any databases containing Section 702-acquired information with respect to Defendant. *Id.* at 669–70. The Second Circuit ordered further briefing on the issue. *Id.* at 670.

The Second Circuit counsels in favor of finding that querying constitutes a "separate Fourth Amendment event that, in itself, must be reasonable." *Id.* at 670. The Second Circuit based this conclusion on three considerations—that lawful collection alone does not always justify a future search, Section 702 is sweeping in its technological capacity and broad in its scope, and that querying makes it easier to target wide-ranging information about a given U.S. person.[10] *Id.* at 669–73.

Nonetheless, based on the "sparse" record presented, the Second Circuit remanded the case for this Court to "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.* at 673. The Second Circuit further remanded for consideration of whether any evidence derived from querying should have been suppressed, including whether any exception to the exclusionary rule might apply. *Id.* at 675–77 ("For all we know, any queries conducted by the government may have been entirely reasonable, they may not have yielded any evidence at all, and any material that was uncovered even by a putatively unconstitutional query may not have affected the investigation in any way.").

[10] Although the Second Circuit indicated that there were three considerations driving its opinion, it nonetheless included a fourth—that "much may depend on who is querying what database." *Hasbajrami*, 945 F.3d at 673.

DISCUSSION

Defendant argues that querying a Section 702 database in connection with a U.S. person generally requires a warrant, even where the initial interception was lawfully conducted. (Def.'s Mem. Supp. Mot. ("Def.'s Mem.") at 31–36, ECF No. 191.) That is, the incidental or inadvertent acquisition of Defendant's communications does not automatically permit the government to search among the acquired communications without a warrant. (*Id.*) For the reasons stated below, the Court agrees, at least as applied in this case.

I. Warrant Requirement

The Fourth Amendment bars "unreasonable searches and seizures." U.S. CONST. amend. IV. As the text suggest, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Riley v. California*, 573 U.S. 373, 381 (2014) (internal citation and quotation marks omitted). Where a search is undertaken to discover evidence of criminal wrongdoing, "reasonableness generally requires the obtaining of a judicial warrant." *Id.* at 382 (quoting *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)); *see also Maryland v. Dyson*, 527 U.S. 465, 466 (1999) ("The Fourth Amendment generally requires police to secure a warrant before conducting a search."). Absent a warrant, "a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 573 U.S. at 382; *see also Katz v. United States*, 389 U.S. 347, 357 (1967) (warrantless searches "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions"). Even where a search fits an exception to the warrant requirement, the "search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution." *Maryland v. King*, 569 U.S. 435, 448 (2013). "To say that no warrant is required is merely to acknowledge that 'rather than

employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable.'" *Id.* (quoting *Illinois v. McArthur*, 531 U.S. 326, 331 (2001)).

Here, as an initial matter, the Government asks the Court to bypass the warrant requirement and immediately assess the reasonableness of any querying here by balancing privacy and law enforcement interests. (Gov.'s Unclassified Supp. Opp'n to Def.'s Mot. Suppress ("Gov. Mem.") at 23, ECF No. 196.) In support of this approach, the Government cites extensively to *Maryland v. King*, 569 U.S. 435, 447 (2013). There, the Supreme Court observed that "[i]n some circumstances, such as '[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.'" (Gov. Mem. at 18 (*citing* King, 569 U.S. at 447).) "Those circumstances diminish the need for a warrant," for example, "because 'the public interest is such that neither a warrant nor probable cause is required.'" *Id.*

Importantly, although *King* recognized that there are circumstances where warrantless searches may be reasonable, it did not displace the general rule that a search under the Fourth Amendment requires a warrant unless subject to a specific exception. *See Riley*, 573 U.S. at 382, 392 (affirming that "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement" and citing *King* to support the proposition that even a finding that a defendant has a diminished privacy interest "does not mean that the Fourth Amendment falls out of the picture entirely"). Thus, a warrantless search remains *per se* unreasonable under the Fourth Amendment unless it is subject to a specific exception. Indeed, *King* itself followed that principle in finding that post-arrest DNA collection was reasonable

based on what the Second Circuit has since-labeled the "inventory or booking search exception." *Pretzantzin v. Holder*, 736 F.3d 641, 648 (2d Cir. 2013). And, all but one of the cases cited in *King* each applied a specific exception to the warrant requirement. For example, in *Illinois v. McArthur*, the Supreme Court found that exigency required a warrantless search based on the reasonable conclusion that, without a warrant, the respondent might "get rid of the drugs fast." 531 U.S. 326, 332 (2001). In *National Treasury Emps. Union v. Von Raab*, the Supreme Court found that a drug testing program for government employees presented a "special need" to circumvent the ordinary warrant requirement. 489 U.S. 656, 666 (1989). And in *Maryland v. Buie*, the Supreme Court upheld a warrantless search incident to an arrest where the officers could, "as a precautionary matter . . . look in closets and other spaces immediately adjoining the place of arrest from which an attack could be immediately launched." 494 U.S. 325, 334 (1990).

In *Samson v. California*, the remaining case cited by *King*, the Supreme Court did not apply a specific exception to the warrant requirement, but the search there was nonetheless deemed reasonable because the parolee did not have a "legitimate" expectation of privacy, as a condition to probation authorized the warrantless search of the parolee's home. 547 U.S. 843, 852–53 (2006). Neither of those conditions is present here, particularly after the Second Circuit has indicated that Defendant maintains a legitimate expectation of privacy in the [redacted]. *See Hasbajrami*, 945 F.3d at 666 ("For the purposes of Hasbajrami's appeal, we may assume that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry when the government undertakes to monitor even foreign communications in a way that can be expected to, and in fact does, lead to the interception of communications with United States persons."). In any event, courts have since interpreted *Samson* as representing a specific exception

"pertain[ing] to persons who have been paroled from a sentence of imprisonment and who, as a condition of such parole, have been required to submit their person or property to search without a search warrant." *United States v. DeJesus*, 538 F. Supp. 3d 382, 389 (S.D.N.Y. 2021) (citing *Samson*, 547 U.S. at 852).

Next, the Government urges the Court not "to stray beyond the bounds of the Second Circuit's remand, which directed this Court to address the reasonableness of queries that may have occurred in this case." (Gov. Mem. at 25.) In advancing this argument, the Government again effectively asks the Court to bypass the warrant requirement. However, the Court cannot examine the reasonableness of any querying done in this case without necessarily answering the question of whether such querying required a warrant. That calculus is simple. The Second Circuit found that querying should be considered a "separate Fourth Amendment event," *Hasbajrami*, 945 F.3d at 670. Accordingly, a warrant was presumptively required. *Riley*, 573 U.S. at 381; *Katz*, 389 U.S. at 357.

In arriving at its conclusion, the Second Circuit observed that several rationales counsel in favor of viewing querying as a distinct Fourth Amendment event. For example, the Second Circuit acknowledged the unique nature of querying, compared to Section 702 surveillance, because the information queried is already in the government's possession. As the Second Circuit observed: "[s]torage has little significance in its own right." *Hasbajrami*, 945 F.3d at 670. In other words, the government cannot circumvent application of the warrant requirement simply because queried information is already collected and held by the government. *See id.* (observing that "courts have increasingly recognized the need for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected").

Riley v. California, which was heavily cited by the Second Circuit, is instructive here. In *Riley*, the Supreme Court held that a warrant was necessary to search a cell phone, even where that cell phone was lawfully seized pursuant to a search incident to a lawful arrest. 573 U.S. at 381. The *Riley* court emphasized that, in contrast to other physical items seized during an arrest, cell phones contain troves of sensitive and private information. *Id.* at 395 (recognizing "an element of pervasiveness that characterizes cell phones but not physical records"). Hence, to view the contents of a cell phone seized incidental to an arrest, the Court provided a simple directive—"get a warrant." *Id.* at 403. As noted by the Second Circuit, other circuits have reached similar conclusions; absent a warrant, the lawful acquisition of evidence does not permit the government to later search the acquired evidence, outside the confines of the original justification. *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) ("Upon failing to find evidence of willfulness in the records pertaining to the preparation of the tax return that were authorized to be seized, the government should not be able to comb through Seda's computers plucking out new forms of evidence that the investigating agents have decided may be useful, at least not without obtaining a new warrant."); *United States v. Runyan*, 275 F.3d 449, 464–65 (5th Cir. 2001) (finding that police exceeded the scope of a private search when they "examined disks that the private searchers did not examine" and would have required a warrant to do so); *United States v. Mulder*, 808 F.2d 1346, 1349 (9th Cir. 1987) (holding that a separate warrant was needed to test packages in suitcase for drugs, even though the suitcase was lawfully seized via private search).

The Court finds the same logic applicable here. A search that relies on an initial warrant or exception to the warrant requirement is limited by its original justification, and to intrude further on lawfully acquired items requires new and independent approval. Just as the Supreme

Court found that the cell phone in *Riley* was lawfully seized pursuant to the search incident to arrest exception, the Second Circuit found that the "vast majority" of Defendant's communications were lawfully acquired as both outside Fourth Amendment protection and subject to the incidental overhear exception.[11] *Riley*, 573 U.S. at 381; *Hasbajrami*, 945 F.3d at 663–64. It follows, therefore, that just as the officers in *Riley* were required to obtain a warrant to search the seized cell phone, so too was the government required to obtain a warrant to view Defendant's communications that were lawfully intercepted.[12] In other words, simply acquiring Defendant's communications under Section 702, albeit lawfully, did not, in and of itself, permit the government to later query the retained information. *See Hasbajrami*, 945 F.3d at 670 ("Storage has little significance in its own right[.]"); *see also Sedaghaty*, 728 F.3d at 913; *Runyan*, 275 F.3d at 464–65; *Mulder*, 808 F.2d at 1349.

To hold otherwise would effectively allow law enforcement to amass a repository of communications under Section 702—including those of U.S. persons—that can later be searched on demand without limitation. But this approach undermines the purpose of the warrant requirement, which is "to interpose a 'neutral and detached magistrate' between the citizen and 'the officer engaged in the often competitive enterprise of ferreting out crime.'" *United States v. Karo*, 468 U.S. 705, 717 (1984) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)).

---

[11] Although the Second Circuit did not expressly frame the incidental overhear doctrine as an "exception" to the warrant requirement, it nonetheless framed the doctrine as "closely related" to the plain view doctrine, which courts have recognized as an exception to the warrant requirement. *Hasbajrami*, 945 F.3d at 664 n.17 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 465–67 (1971)).

[12] The government also appears to cite *United States v. Lustig*, for the proposition that subsequent searches of a lawfully seized item do not require a warrant. (Gov. Mem. at 18 (citing 830 F.3d 1075 (9th Cir. 2016).) As discussed, the Court rejects that argument—though the Court also finds *Lustig* inapposite in this context. In *Lustig*, the Ninth Circuit addressed the narrow question of whether the good faith exception applied to the search of a cell phone before the Supreme Court's decision in *Riley*. *Lustig*, 830 F.3d at 1079. That is, post-*Riley* there was "no question that the searches of Lustig's Pocket Phones were unconstitutional," so "[t]he question on appeal [was] instead whether the good-faith exception to the exclusionary rule nevertheless makes admissible the evidence found in the Pocket Phone searches." *Id.* Thus, because *Lustig* exclusively dealt with application of the good faith doctrine, it does not implicate the present question of whether any querying here required a warrant.

Indeed, "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403 (adding that "[o]pposition to such searches was in fact one of the driving forces behind the Revolution itself").

As the Second Circuit acknowledged, querying [redacted] based on speculation that Section 702 might have intercepted relevant information looks "like a general warrant." *Hasbajrami*, 945 F.3d at 671; *see also United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (general searches "are especially pernicious" and "have long been deemed to violate fundamental rights") (quoting *Marron v. United States*, 275 U.S. 192, 195 (1927)). The comparison to a general warrant is particularly apt given that Section 702-acquired information is retained "not to keep tabs on a United States person, but to keep tabs on the non-United States person abroad who has been targeted." *Hasbajrami*, 945 F.3d at 670. Indeed, Section 702 is specifically designed to avoid the collection of communications by U.S. persons. When the NSA learns that a target is a U.S. person, it must immediately cease targeting that individual and destroy any such communications already acquired, subject to limited circumstances of waiver. 50 U.S.C. § 1881a(b) (outlining "limitations" on targeting procedures); *see also* PCLOB Report at 127–28 (summarizing minimization procedures). Once communications are collected, minimization serves to limit [redacted] involving U.S. persons. 50 U.S.C. § 1801(h); *see also* 50 U.S.C. § 1821(4) (minimization procedures must be "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting [U.S.] persons"). Unless the intercepted communications of U.S. persons contain evidence of a crime or serve a foreign intelligence

purpose, the government must destroy those communications. *See* 50 U.S.C. § 1801(h), 1821(4); *see also* PCLOB Report at 128 (acknowledging that NSA procedures "require the destruction of irrelevant communications of or concerning U.S. persons," even though in practice "this destruction rarely happens"). These procedures mitigate the collection and review of communications of U.S. persons. While communications of U.S. persons may nonetheless be intercepted, incidentally or inadvertently, it would be paradoxical to permit warrantless searches of the same information that Section 702 is specifically designed to avoid collecting. To countenance this practice would convert Section 702 into precisely what Defendant has labeled it—a tool for law enforcement to run "backdoor searches" that circumvent the Fourth Amendment. (Def. Mem. at 19.)

Nonetheless, the Government presses that the Second Circuit "did not suggest" that a warrant is presumptively required in the context of querying. (Gov. Mem. at 17.) This argument misses the point. That the Second Circuit did not expressly conclude that a warrant was required does not undermine the legion of case law holding that a warrant is presumptively required for law enforcement to conduct a search. *See supra* pp. 17–21. Instead, the Second Circuit referred any determination as to the lawfulness of any querying under the Fourth Amendment to this Court. *See Hasbajrami*, 945 F.3d at 673 (instructing this Court to "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.").

The remaining arguments advanced by the Government to avoid application of the warrant requirement are without merit. According to the Government, it would be "anomalous" to require a warrant to query Section 702-acquired information that has already been reviewed for minimization. (Gov. Mem. at 18–19.) But this argument seeks to exploit the purpose of

minimization. Once communications are collected under Section 702, minimization procedures require NSA analysts to review each communication and decide if "it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." NSA 2011 Minimization Procedure § 3(b)(4). Communications fitting that description are retained, and unless subject to a specific exception, the remaining are destroyed. *Id.* By arguing that compulsory review of Section 702-acquired communications justifies later review of even a subset of those communications, the Government seeks to use minimization procedures to bootstrap access to communications of United States citizens for whom the procedures are designed to protect.[13] This argument is akin to claiming that law enforcement can access privileged communications reviewed by a filter team because government employees laid eyes on the privileged communications at some point in the process. The argument makes no more sense in that context than it does here.

Finally, the Government argues that this Court should abstain from analyzing the reasonableness of querying because the FISC, rather than this Court, "has the necessary statutory mandate, expertise, and record evidence before it to undertake that function." (Gov. Mem. at 26.) Of course, the Court acknowledges that the FISC is experienced in reviewing matters of this nature, but that is not to say that this Court cannot competently address them as well. In the surveillance context, the Supreme Court has expressly rejected the argument "that internal security matters are too subtle and complex for judicial evaluation" because "[t]here is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases." *United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S.

[13] Even the Government recognizes that minimization procedures are designed to "restrict how the government treats information of or concerning U.S. persons." (Gov. Mem. at 3); *see* 50 U.S.C. § 1801(h) (minimization procedures serve "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons").

297, 320 (1972) ("Courts regularly deal with the most difficult issues of our society."). While this case undoubtedly raises difficult issues, the Court will not abstain from resolving them because another court, not implicated here, might be just as competent. This Court has a particular interest in resolving these issues because they directly implicate the constitutional rights of a defendant before this Court. In fact, to decide otherwise would directly contravene the clear mandate from the Second Circuit to resolve these issues in the first instance.

Against this backdrop, this Court's "analysis begins, as it should in every case addressing the reasonableness of a warrantless search, with the basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357). Here, the Government maintains that the foreign intelligence exception applies. (Gov. Mem. at 20–21.)

A. The History of the Foreign Intelligence Exception

The history and evolution of the foreign intelligence exception are helpful in determining whether it applies to querying. *See* John Esterhay, *Let's Call A Duck A Duck: The Foreign Intelligence Exception from In Re Directives Should Be Restricted to Combating Global Terrorism*, 2 Elon L. Rev. 193, 197 (2011) (summarizing the history of the foreign intelligence exception). When technology capable of allowing law enforcement to wiretap a telephone line first developed, the Supreme Court held that such surveillance fell outside of Fourth Amendment protection and did not require a warrant. *See Olmstead v. United States*, 277 U.S. 438, 466 (1928). Forty years later, in *Katz v. United States*, the Supreme Court reversed course, ruling that a wiretap generally requires a warrant but, the was silent on whether surveillance conducted

for national security purposes also requires a warrant. *Id.* at 359 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."). However, shortly thereafter, the Supreme Court addressed the question directly in *United States v. U.S. Dist. Court*, better known as the "*Keith*" decision. There, the Supreme Court ruled that domestic surveillance, even when conducted for national security purposes, requires a warrant under the Fourth Amendment. 407 U.S. 297, 320 (1972). Importantly, *Keith* noted that different warrant standards and procedures could apply for domestic national security surveillance, compared to those required for a wiretap under *Katz*, due to "different policy and practical considerations from the surveillance of 'ordinary crime.'" *Keith*, 407 U.S. at 322. As such, *Keith* set the stage for the development of separate warrant procedures for domestic national security surveillance, while leaving unresolved the question of what constitutes "domestic" security surveillance versus "foreign" security surveillance of Americans. *See* Esterhay, *Let's Call A Duck A Duck*, at 198.

Over the ensuing years, before the passage of FISA, several federal appeals courts recognized an exception allowing warrantless surveillance of individuals in the United States for foreign intelligence investigations. *E.g.*, *United States v. Hung*, 629 F.2d 912–16 (4th Cir. 1980) (applying exception to warrantless surveillance of Vietnamese citizen living in the United States who sought to transmit classified government information to Vietnam); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (applying exception to warrantless surveillance of Soviet national living in the United States who sought to transmit military intelligence to the U.S.S.R.); *United States v. Brown*, 484 F.2d 418, 427 (5th Cir. 1973) (upholding surveillance in which the defendant was incidentally overheard via a warrantless wiretap authorized for foreign

intelligence purposes). These courts reasoned that, for example, "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" such that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *Hung*, 629 F.2d at 913.

In 1978, Congress enacted FISA, which required warrants for any surveillance occurring in the United States and directed at U.S. persons. 50 U.S.C. § 101(f), 102(a)(1). Notably, FISA did not place any restrictions on surveillance conducted against targets located outside the United States, even if the targets are U.S. persons. *Id.* In *United States v. Bin Laden*, the court "adopt[ed] the foreign intelligence exception to the warrant requirement for searches targeting foreign powers (or their agents) which are conducted abroad." 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000). In that case, which resulted from the 1998 U.S. embassy bombings in East Africa, one of the defendants was a U.S. citizen in Kenya who had been surveilled without a warrant. *Id.* at 268, 270. On appeal, the Second Circuit did not address the applicability of the exception after finding that "the Fourth Amendment's Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness." *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 157, 171–72 (2d Cir. 2008).

The state and scope of American surveillance developed rapidly following the September 11 terrorist attacks, as the government implemented a series of new surveillance programs. *See* Esterhay, *Let's Call A Duck A Duck*, at 200. In reviewing these new surveillance programs, courts considered the application of the foreign intelligence exception to evolving modern

technologies. For example, in its second-ever ruling in 2008, the FISCR adopted the foreign intelligence exception in connection with Section 702's short-lived predecessor, the Protect America Act ("PAA").[14] *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010–12 (FISCR 2008). American communication service providers petitioned the FISC for review of directives compelling their assistance in the warrantless surveillance of customers believed to be outside the United States. *Id.* at 1008. After the FISC upheld the directives, the FISCR held on review "that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." *Id.* at 1012. In making this determination, the FISCR reasoned that the foreign intelligence exception was warranted because (1) the purpose of surveillance went beyond "garden-variety" law enforcement and safeguarding the nation's security serves a "particularly intense" government interest and (2) there was a "high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *See id.* at 1011–12.

In 2011, when reviewing Section 702's targeting and minimization procedures, the FISC applied the foreign intelligence exception to Section 702 surveillance. *Redacted*, 2011 WL 10945618, at *24 (FISC Oct. 3, 2011). After acknowledging that the "NSA acquires a substantially larger number of communications of, or concerning, United States persons and persons inside the United States than previously understood," the FISC nonetheless applied the exception based on the same rationale embraced by the FISCR in *In re Directives*. *See id.* The

[14] *See Hasbajrami*, 945 F.3d at 651 n.6 (describing the role of the PAA prior to passage of Section 702).

court reasoned that collection goes "well beyond any garden-variety law enforcement objective" and that there was a "high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information." *Id.*

In 2016, the FISCR adopted the foreign intelligence exception in a case involving pen registers directed at persons in the United States. *In re Certified Question of L.*, 858 F.3d 591, 606–07 (FISCR 2016). There, the FISCR held that "when the government . . . seeks to use a pen register directed at a person located in the United States who is reasonably believed to be engaged in clandestine intelligence activities on behalf of a foreign government, it may do so without obtaining a probable-cause warrant even if its monitoring of post-cut-through digits constitutes a search under the Fourth Amendment." *Id.* at 607. Again, the FISCR applied the exception based on the same rationale described in *In re Directives*, which the FISCR said "virtually control[led]" the outcome in *In re Certified Question*. *Id.*

Now, the Government contends that the foreign intelligence exception should be extended beyond the acquisition of foreign intelligence information to the subsequent querying of this information because "[e]very court to have addressed the question, including the FISC, has held that the foreign intelligence exception applies in the Section 702 context." (Gov. Mem. at 21.) The Government reasons that because those courts "have recognized that the government's programmatic purpose in reviewing and querying Section 702-acquired information goes well beyond ordinary law enforcement," the foreign intelligence exception must apply in this case. (*Id.*) This is not necessarily so.[15]

[15] At the same time, the Court rejects Defendant's argument that "in declaring that querying constitutes a separate Fourth Amendment event, the Second Circuit clearly rejected the government's claim that the foreign intelligence exception encompasses the subsequent querying of Section 702 databases." (Def.'s Reply at 10, ECF No. 201.) (internal citation and quotation marks omitted). The conclusion that that querying constitutes a separate Fourth Amendment event does not foreclose the application of any exception to the warrant requirement. Rather, that

B. Application of the Foreign Intelligence Exception

1. Queries at Issue

[redacted]

finding requires the Court to conduct a full Fourth Amendment analysis, which, as discussed, requires the Court to consider whether any exception to the warrant requirement applies.

[16] The Government seems to make much of the distinction between minimized and unminimized data. However, this distinction is not consequential to the Court's analysis regarding whether the applicability of the foreign intelligence exception. [redacted] Because even minimized Section 702-acquired data contains communications to and from U.S. persons, these communications remain subject to Fourth Amendment protection. Thus, the Court's analysis does not turn on whether the data searched was minimized or unminimized, but the very fact that the data was searched at all.

[redacted]

1. **February 11, 2011 Queries**

[redacted] Nonetheless, because [redacted] used terms associated with Defendant in databases containing Section 702-acquired information, these queries are subject to the Court's foreign intelligence exception analysis. *See Hasbajrami*, 945 F.3d at 673.

2. April 2011 [redacted] Query

[redacted]

[redacted] Nonetheless, because [redacted] used terms related to Defendant in databases containing Section 702-acquired information, these queries are subject to the Court's foreign intelligence exception analysis. *See Hasbajrami*, 945 F.3d at 673.

3. April 18 – August 4, 2011 Queries

[redacted]

[redacted]

[redacted] However, any queries conducted in [redacted] are subject to the Court's foreign intelligence exception analysis because they involved terms associated with Defendant across Section 702-acquired information. *See Hasbajrami*, 945 F.3d at 673. Moreover, because the Government does not clarify which of the [redacted] queries were conducted across which databases, the Court must analyze all [redacted] queries as if they were conducted in [redacted], which is subject to the Court's foreign intelligence exception analysis.

[redacted]

However, because [redacted] used terms associated with Defendant in databases containing Section 702-acquired information, these queries are subject to the Court's foreign intelligence exception analysis. *See Hasbajrami*, 945 F.3d at 673.

[redacted]

[redacted] Because [redacted] conducted these queries in databases containing Section 702-acquired information using terms related to Defendant, these queries are subject to the Court's foreign intelligence exception analysis. *See Hasbajrami*, 945 F.3d at 673.

4. April 28, 2011 [redacted]

On or about April 28, 2011, [redacted] to conduct checks in the [redacted], an unclassified database that does not contain any Section 702-acquired information, in connection with Defendant. (*Id.* ¶ 27.) The purpose of this check was to obtain information about Defendant related to the allegations of terrorist financing. (*Id.* ¶ 27.) On or about April 29, 2011, [redacted] to conduct a criminal records check for Defendant, also in an unclassified database that did not contain any Section 702-acquired information. (*Id.* ¶ 28.) Because [redacted] April 28 and April 29, 2011 checks were conducted across unclassified databases that did not contain any Section 702-acquired information, these queries are not subject to the Court's foreign intelligence exception analysis. *Hasbajrami*, 945 F.3d at 673.

[redacted]

[redacted]

* * *

In sum, all of the queries conducted by [redacted] are subject to the Court's foreign intelligence exception analysis. In each instance, the government ran queries using terms and identifiers related to Defendant in databases containing or potentially containing Section 702-acquired information. However, where those searches did not yield any Section 702-acquired information, any violation of the Fourth Amendment was harmless. *See id.* at 669 (noting that inadvertent collection of communications involving Defendant was harmless because the "materials collected, whatever they were, were not used in applying for the FISA warrant" . . . and "nothing of intelligence value was being learned.") The Court refers specifically to [redacted] queries and [redacted] queries conducted between [redacted]. Thus, the only queries that the Court must analyze under the foreign intelligence exception are: [redacted] query conducted after it learned of Defendant's

[redacted]; the [redacted] queries conducted between [redacted]; the [redacted] queries conducted between [redacted]; [redacted] The [redacted] conducted by [redacted] is not subject to the Court's foreign intelligence analysis.

2. Foreign Intelligence Exception Analysis

To the extent the Government advances that an exception applies in any case, the Government bears the burden of showing the search fell within any exception to the warrant requirement.[17] *Riley*, 573 U.S. at 381; *Perea*, 986 F.2d at 639 ("If such a privacy interest is established, the government has the burden of showing that the search was valid because it fell within one of the exceptions to the warrant requirement."); *Arboleda*, 633 F.2d at 989 ("The movant can shift the burden of persuasion to the Government and require it to justify its search, however, when the search was conducted without a warrant."). In this case, therefore, the Government must first establish that the querying of Section 702-acquired information goes beyond "garden-variety" law enforcement. *See In re Directives*, 551 F.3d at 1011–12. It has. Indeed, there can be no legitimate debate that the protection of national security interests involved with foreign intelligence, as it pertains to both the surveillance and the querying of Section 702-acquired information, serve purposes that go beyond garden-variety law enforcement. However, this does not end the Court's inquiry in this case.

[17] In the normal course, a defendant seeking to suppress evidence seized during a warrantless search bears the burden of showing that he had a reasonable expectation of privacy in the place or object searched. *United States v. Sparks*, 287 F. App'x 918, 919 (2d Cir. 2008) (citing *California v. Greenwood*, 486 U.S. 35, 39 (1988)). If the defendant makes such a showing, then the burden shifts to the Government to show that the search fell within one of the exceptions to the warrant requirement. *United States v. Perea*, 986 F.2d 633, 639 (2d Cir. 1993) ("If such a privacy interest is established, the government has the burden of showing that the search was valid because it fell within one of the exceptions to the warrant requirement."); *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980) ("The movant can shift the burden of persuasion to the Government and require it to justify its search, however, when the search was conducted without a warrant."). Defendant has undoubtedly made the requisite showing.

To invoke the foreign intelligence exception, the Government must also establish that its aims would have been hindered by adhering to the warrant requirement. *See In Re Directives*, 551 F.3d at 1011–12. The court in *In Re Directives*, having extrapolated its analysis from principles derived from the special needs exception, reasoned that the warrantless acquisition of Section 702-acquired information through the surveillance of foreign powers and their agents was justified. The court arrived at this conclusion not only because the search served purposes beyond ordinary law enforcement. Indeed, key to the court's rationale was the conclusion that the exception was necessary because "[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner."[18] *Id.* Like many cases applying the special needs exception to the warrant requirement, cases applying the foreign intelligence exception have highlighted that the immediacy of the government's need to collect foreign intelligence information justified the Fourth Amendment intrusion.[19] On this element, the Government's submission is wanting.

---

[18] This is consistent with the rationale behind the special needs doctrine, which is the "doctrinal underpinning" of the foreign intelligence exception to the Fourth Amendment warrant requirement. *See In re Certified Question of L.*, 858 F.3d 591, 606 (FISCR 2016). The special needs exception is applicable where "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search." *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 623 (1989). Courts routinely find that the warrant requirement frustrates the governmental objective behind a search when "the delay inherent in obtaining a warrant" makes achieving the objective particularly difficult or impracticable. *See Griffin*, 483 U.S. at 876. For example, in *Griffin v. Washington*, the Supreme Court held that the special needs exception applied where the government's purpose was the close supervision of individuals on probation and the delay inherent in obtaining a warrant "would make it more difficult for probation officials to respond quickly to evidence of misconduct . . . and would reduce the deterrent effect that the possibility of expeditious searches would otherwise create." *Id.* In *Skinner v. Ry. Lab. Execs.' Ass'n*, the Supreme Court held that the special needs exception applied to a government regulation that instituted warrantless drug and alcohol testing for railroad workers after major train accidents in order to determine whether the worker violated safety rules. *See* 489 U.S. at 623–24. There, the court found that, because drugs and alcohol are eliminated from the bloodstream at a constant rate and, thus, blood and breath samples must be obtained as soon as possible, "the delay necessary to procure a warrant [] may result in the destruction of valuable evidence." *Id.* In these cases, the "immediacy of the government's need" was a significant factor in determining whether the government's Fourth Amendment intrusion was justified.

[19] In addition to recognizing the potential to frustrate the government's ability to collect information in a timely manner, courts applying the foreign intelligence exception have highlighted the government's need for stealth and secrecy as justifications to intrude on the Fourth Amendment with respect to foreign intelligence surveillance. *See, e.g., United States v. Hung*, 629 F.2d 908, 913 (4th Cir. 1980) (noting that "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy"). However, these concerns alone do not justify a

The first query at issue is a [redacted] made by [redacted] sometime in [redacted] As to this query, the Government explains only that after learning that [redacted] with [redacted] The Government does not indicate how much time passed [redacted] The Government does not explain the purpose of this query. Most important, beyond a naked assertion, the Government does not explain how obtaining a warrant in advance of running the query would have hindered the Government's specific objective, whatever it may have been. (*See generally* Gov. Mem.) And nothing in the Government's submission allows for this conclusion. Absent an explanation for what its aims were and why they would have been impeded by obtaining a warrant, the Court cannot find that any such circumstance existed. As such, the first query does not meet the requirements of the foreign intelligence exception.

Next, [redacted]. The Government does indicate how many queries were run on any given day. But it is evident that, [redacted] In the context of traditional questions of exigency, courts have held that such extended periods defeat a claim of exigency necessary to overcome the warrant

---

departure from the Fourth Amendment warrant requirement. As the Court in *Keith* found, these security dangers can be minimized by proper administrative measures. *United States v. U.S. Dist. Ct.*, 407 U.S. 297, 321 (1972).

requirement. *See e.g.*, *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 358–59 (1977) (holding that there were no exigent circumstances where IRS agents made a warrantless entry into a corporation's office and seized records two days after an initial warrantless forced entry whereby the agents made no seizures and "more than one day following the observation of materials being moved from the office"); *Dzwonczyk v. Syracuse City Police Dep't*, 710 F. Supp. 2d 248, 265-66 (N.D.N.Y. 2008) (holding that no exigent circumstances existed that would permit a warrantless in-home arrest by city police officers, where officers arrested suspect on misdemeanor aggravated harassment charge based on statement by alleged victim four days prior). In the absence of more information, this Court can see no reason why the same conclusion should not be reached here. This is all the more so because the Government fails altogether to offer any explanation as to how its efforts would have been thwarted or hindered by obtaining a warrant before any query was run on [redacted]. That, as the Government maintains, there was "ample basis to assess that querying the . . . Section 702 acquired information . . . would likely yield foreign intelligence information or evidence of a crime," is not enough. [redacted] At most, this fact, if true, only satisfies the initial prong of the foreign intelligence exception. Accordingly, as to the [redacted], the Government has failed to meet its burden.

The Court's view of the remaining queries at issue is no different. [redacted] (*Id.* ¶¶ 31–32.) According to the Government, these queries were [redacted] (*Id.* ¶ 31.) Certainly. However, in utter disregard for its burden, the Government once again fails to advance any argument as to why it could not have

acquired a warrant to conduct these queries. Put differently, the Government has not articulated how obtaining a warrant would have hindered its objective. (*See generally* Gov. Mem.) It is simply inconceivable that the government's aims would have been frustrated by securing a warrant at any time over the course of many months. Indeed, the Government's contention that it could not have obtained a warrant on any intervening date between [redacted] is belied by the FISA emergency protocol. As set for in 50 U.S.C. § 1805(e), the FISA provides for an emergency procedure whereby the Attorney General may immediately authorize an emergency search and subsequently make an application to the FISC within 24 hours for retroactive approval.[20] This mechanism could have been used to secure a warrant. And, there can be no question that the Government was aware of this procedure, which it seemingly used in September 2011 when the Assistant Attorney General for National Security authorized electronic surveillance and physical searches of Defendant "on an emergency basis." [redacted]

Moreover, there can be no argument that these queries were harmless. That is, the Government could not possibly posit that the queries yielded "nothing of intelligence value." *See Hasbajrami*, 945 F.3d at 673. Indeed, the Government acknowledges that it [redacted]

[redacted]

[20] 50 U.S.C. § 1805(e) provides that "the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; (B) reasonably determines that the factual basis for the issuance of an order . . . exists; (C) informs . . . a judge having jurisdiction under section 1803 . . . that the decision has been made to employ emergency electronic surveillance; and (D) makes an application . . . as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance."

[redacted] The Government's use of the queried Section 702-acquired data results leaves no room for doubt that these searches were not harmless. *Cf. See Hasbajrami*, 945 F.3d at 669 (noting that inadvertent collection of communications involving Defendant was harmless because the "materials collected, whatever they were, were not used in applying for the FISA warrant").

Having evaluated the circumstances surrounding each query in this case—to the extent possible with the information provided by the Government—the Court cannot conclude that obtaining a warrant would have impeded the government's "ability to collect-time sensitive information." *See In re Directives*, 551 F.3d at 1011–12. None of the concerns that the foreign intelligence exception was designed to address are present here. That is, the Government does not claim that it was involved in a fast-moving investigation. It does not argue that there was any danger of evidence being destroyed, becoming inaccessible, or rendered obsolete. Nor does it point to any other circumstance that would allow the Court to conclude that the intrusion on Defendant's Fourth Amendment rights was justified. At bottom, it appears that the Government relies on the mere phrase "foreign intelligence exception" and the general idea behind it in arguing that it should apply to the queries in this case. That is, the Government suggests that simply because their queries pertained to foreign intelligence, without more, they fall within the exception. As discussed above, that is just untrue.

The cases relied on by the Government do not change the Court's conclusion. The Government directs the Court to cases where the foreign intelligence exception was applied to active surveillance. Those cases, however, are of no help to the Government's argument that the foreign intelligence exception applies to the querying here. Querying and surveillance represent

entirely separate steps in the investigatory process. (*See* PCLOB at 55–60.) It is not difficult to imagine why the timely *collection* of foreign intelligence information is inherently critical. Communications occurring in real time can be deleted or corrupted prior to collection if they are not acquired as soon as possible. However, when it comes to querying, this inherent risk does not exist because the universe of information is already securely stored and not at risk of being deleted before it can be reviewed.

In *United States v. Mohamud*, the District of Oregon found that "even if [Section] 702 surveillance triggers the Warrant Clause, no warrant is required because [Section] 702 surveillance falls within the foreign intelligence exception to the warrant requirement." No. 10-CR-00475, 2014 WL 2866749, at *15 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420 (9th Cir. 2016). However, the *Mohamud* court only applied the exception to Section 702 surveillance, finding that the "application of the warrant requirement would be impracticable" due to "[t]he government's need for speed and stealth" as it pertains to the acquisition of foreign intelligence. *See id.* at 18. Although the court briefly addressed the reasonableness of querying after acquisition, it ultimately concluded that querying "is not a separate search," and thus did not address whether querying itself would be subject to the foreign intelligence exception.[21] *See id.* at *26.

In another case cited by the Government, *United States v. Al-Jayab*, the Northern District of Illinois expressly declined to consider the application of the foreign intelligence exception after finding that Section 702 surveillance did not require a warrant. Opinion and Order, No. 16-cr-181, Dkt. No. 115 at 47 (N.D. Ill. June 28, 2018) ("The Court need not reach the foreign

[21] The Second Circuit expressed skepticism with respect to the *Mohamud* court's reasoning in finding that querying did not constitute a separate Fourth Amendment search. *Hasbajrami*, 945 F.3d at 670.

intelligence exception, having found that [Section] 702 does not violate the warrant and probable cause requirements."). Instead, the *Al-Jayab* court merely observed that, even if Section 702 surveillance required a warrant, "the foreign intelligence exception appears suited to [Section] 702 [because] although it does not include a foreign power or agent requirement, [Section 702] has procedures in place to ensure that its targets are non-U.S. persons outside of the United States who are reasonably likely to have foreign intelligence information." *Id.* at 48. Notably, just as the court in *Al-Jayab* expressly declined to consider the foreign intelligence exception, it also expressly declined to assess the reasonableness of querying. *See id.* at 55 ("Because al-Jayab was not aggrieved by any backdoor searches, the Court need not consider the issue further.").

To be sure, there may arise any number of situations in which the need to run queries against Section 702-acquired information is time sensitive such that it warrants the application of the foreign intelligence exception. As with any other search subject to the warrant requirement, exceptions might be available depending on the particular facts of a case. *See Carpenter v. United States*, 585 U.S. 296, 319 (2018) ("Further, even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances."); *Riley*, 573 U.S. at 401–02 ("Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone."). However, on the record of this case, the Court cannot conclude that the foreign intelligence exception applied. As such, the government's queries with respect to Defendant were not exempt from the warrant requirement under the foreign intelligence exception.

II. Balancing Privacy and Law Enforcement Interests

Assuming for argument that the foreign intelligence exception applied to any querying conducted here, that finding alone would not end the analysis. *See Mohamud*, 2014 WL 2866749, at *19 ("Application of the foreign intelligence exception does not end the analysis[.]"); *In re Directives*, 551 F.3d at 1012 ("[E]ven though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement."). Where a search fits an exception to the warrant requirement, the "search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution." *King*, 569 U.S. at 448. A court must weigh "the promotion of legitimate governmental interests against the degree to which the search intrudes upon an individual's privacy." *Id.* at 436 (cleaned up). Under this model, the more important the government's interest, the greater an intrusion may be constitutionally tolerated. *In re Directives*, 551 F.3d at 1012. According to the Government, any querying here was reasonable because it resulted in "minimal intrusion" and promoted "important public interests."[22] (Gov. Mem. at 17–19.) The Court disagrees.

A. Degree of Intrusion

Assessing the degree of intrusion requires addressing both the methods used and the purpose for the intrusion. *Widgren v. Maple Grove Twp.*, 429 F.3d 575, 583 (6th Cir. 2005); *see also San Jose Charter of Hells Angels Motorcycle Club v. City of San Jose*, 402 F.3d 962, 971 (9th Cir. 2005) (acknowledging "[t]he standard of reasonableness embodied in the Fourth

[22] In making this argument, the Government again cites to *King* to suggest that querying does not require a warrant because, just as the Court there upheld matching DNA against a database of previous crimes without obtaining a warrant, no warrant was required to query information lawfully collected under Section 702. (Gov. Mem. at 18.) Although the Supreme Court found the DNA swabbing there to be a "minimal intrusion," that was because "a swab of this nature does not increase the indignity already attendant to normal incidents of arrest." *King*, 569 U.S. at 464. The factual predicate for the Court's conclusion in *King* is too distinct to be analogous here.

Amendment demands that the showing of justification match the degree of intrusion.") (quoting *Berger v. New York*, 388 U.S. 41, 70 (1967) (Stewart, J., concurring)).

Courts across this country have recognized that emails contain some of our most private thoughts. *See United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) ("By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities."); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("The privacy interests in [mail and email] are identical."); *see also Hasbajrami*, 945 F.3d at 666 (assuming "that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry"). Indeed, in reviewing Section 702 minimization procedures, the FISC observed that the privacy interests at stake are "substantial." *Redacted*, 402 F. Supp. 3d at 87. This is why the Supreme Court has suggested that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line." *See City of Ontario v. Quon*, 560 U.S. 746, 762–63 (2010). Or, to use a different comparison, reviewing private emails is just as intrusive as searching one's cell phone.

The Supreme Court observed in *Riley* that, compared to physical records, "the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones." 573 U.S. at 394–95 (adding "there is an element of pervasiveness that characterizes cell phones but not physical records"). The Court further emphasized that "American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives." *Id.* Emails, like cell phones, can provide a glimpse into nearly every aspect of someone's life. *Warshak*, 631 F.3d at 284. As such, there is also "an element of pervasiveness" in searching private emails that resembles searching one's cell phone. *See Riley*, 573 U.S. at 395.

There can be no question that querying is uniquely intrusive considering the remarkable scope of Section 702. A declassified 2011 FISC opinion revealed that the NSA collects more than 250 million internet communications per year under Section 702.[23] FISC Mem. at 29 (FISA Ct. Oct. 3, 2011). In 2022, approximately 246,073 targets were authorized for collection.[24] Fonzone et al., *Senate Judiciary Comm. Joint Stmnt. for the Rec.* at 7 (June 13, 2023).[25] This is why the Second Circuit likened Section 702 to a "dragnet" where querying looks "more like a general warrant." *Hasbajrami*, 945 F.3d at 671.

Carpenter v. United States is instructive here. 585 U.S. 296 (2018). In that case, the Supreme Court considered whether a warrant was required to access physical movements captured by cell-site location information ("CSLI"), which wireless carriers store for business purposes. *Id.* at 300–01. Notably, CSLI "is detailed, encyclopedic, and effortlessly compiled," meaning "[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 309, 311. The Supreme Court held that accessing CSLI required a warrant based on the "deeply revealing nature of CSLI"; its "depth, breadth, and comprehensive reach"; and the "inescapable and automatic nature of its collection." *Id.* at 320. So too here, the collection of communications under Section 702 effectively creates a "repository" of communications the government can

---

[23] The exact number of collected communications involving U.S. persons remains unknown. PCLOB Report at 14 ("As a result of this impasse, lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702.").

[24] The Court recognizes that not all, or even a majority, of these communications implicate U.S. persons or become subject to querying. And Congress contemplated that Section 702 would necessarily capture some communications involving U.S. persons. *See* PCLOB Report at 82–83. Nonetheless, collection at this volume demonstrates the significant risk of incidentally or inadvertently collecting communications concerning U.S. persons. *See id.* at 87 ("Although U.S. persons and other persons in the United States may not be targeted under Section 702, operation of the program nevertheless results in the government acquiring some telephone and Internet communications involving U.S. persons, potentially in large numbers.").

[25] https://www.justice.gov/d9/2023-06/Section%20702%20of%20the%20Foreign%20Intelligence%20Surveillance%20Act.pdf

access with apparent ease. And just as cell phone users cannot opt out of the "inescapable and automatic" collection of their CSLI, individuals cannot opt out of Section 702 acquisition. As such, because both programs aggregate "deeply revealing" data on a significant scale, it seems likely the Supreme Court would find Section 702 collection to be similarly intrusive. *See id.* at 320.

Turning to the facts here, the Government describes dozens of queries run against an unknown number of communications collected from Defendant. [redacted] Unfortunately, that is the extent of the information provided by the Government with respect to querying in this case. The Government largely fails to identify specific query terms, specific results of querying, or the contents of the underlying communications subject to querying. [redacted] The Government has merely provided [redacted] that purport to reconstruct the record without any supporting evidence.

[redacted]

[redacted]

The Government's opposition is rife with similarly vague and unsupported notions.

Ironically, it was the Government's provision of a "sparse" record in the first place that caused the Second Circuit to remand on this issue. *Hasbajrami*, 945 F.3d at 673. Here again, the Court is left with an incomplete record, from which the Government asks this Court to infer that the querying here was "reasonable." (Class. Gov. Mem. at 51–61.) This, despite the Government bearing the burden of justifying its searches here. *See Arboleda*, 633 F.2d at 989 ("The movant can shift the burden of persuasion to the Government and require it to justify its search, however, when the search was conducted without a warrant."). Perhaps a more complete record would have enabled the Court to make such a finding, but based on the sparse record presented, the Court cannot do so.

Accordingly, based on the volume of queries conducted, the length of time during which the queries occurred, and the type of communication subject to querying, the Court finds that the querying here involved more than a "minimal" intrusion.

B. Public Interest

According to the Government, "the public has a powerful interest in permitting the government to conduct" queries, including for example "discovering potential links between

foreign terrorist groups and persons within the United States in order to detect and disrupt terrorist activity." (Gov. Mem. at 19.) And requiring law enforcement "to apply for and obtain a warrant before conducting any such targeted query would hinder the government's ability to timely identify and respond to time-sensitive information and, thus, would impede the vital national security interests that are at stake." (*Id.*) (internal quotation marks omitted).

The Court agrees that there is a "powerful" public interest in allowing law enforcement to run queries for national security purposes—but public interest alone does not justify warrantless querying. *See King*, 569 U.S. at 448 ("Urgent government interests are not a license for indiscriminate police behavior."). Rather, "[i]n assessing whether the public interest demands creation of a general exception to the Fourth Amendment's warrant requirement, the question is not whether the public interest justifies the type of search in question, but whether the authority to search should be evidenced by a warrant, which in turn depends in part upon whether the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search." *Camara v. Mun. Ct. of City & Cnty. of San Francisco*, 387 U.S. 523, 533 (1967). Certainly, the Court can imagine situations where obtaining a warrant might frustrate the purpose of querying, particularly where exigency requires immediate querying. This is why the Court does not hold that querying Section 702-acquired information always requires a warrant. As with any other search subject to the warrant requirement, exceptions will sometimes be made based on the circumstances. But just as the Court does not hold that all querying requires a warrant, it likewise cannot hold that all instances of querying are of such paramount public interest as to never require a warrant.

Here, according to the Government, it would have been unreasonable *not* to run queries with respect to Defendant after receiving intelligence that [redacted]

[redacted] That is, the Government argues that it was "eminently reasonable" for [redacted] to [redacted] based [redacted]. (*Id.*) Whether it would have been "irresponsible" for [redacted] not to further investigate Defendant based on these claims has no bearing on whether the government can circumvent the warrant requirement to do so. If running such queries truly presented "critical, time-sensitive clues," as the Government contends, then perhaps exigency could have justified the warrantless querying. (*Id.*) But, as discussed above, the Government does not set forth the facts necessary for the Court to conclude that the requisite exigency existed. In any event, it cannot be said that each query conducted here, including dozens across the span of [redacted] months, was uniquely "time-sensitive" as to not require a warrant.

The Court further recognizes that imposing a warrant requirement presents an added burden to the government.[26] As the Supreme Court has held, however, the burden caused by obtaining a warrant is not enough, by itself, to circumvent the warrant requirement. *See Riley*, 573 U.S. at 401 ("We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."); *Johnson v. United States*, 333 U.S. 10, 15 (1948) ("No reason is offered for not obtaining a search warrant except the inconvenience to the officers and some slight delay necessary to

[26] More specifically, the Government argues that FISC "would face a staggering burden if every query of a database containing Section 702 information required a separate judicial warrant." (Gov. Mem. at 19.) The Government cites to *Johnson v. Quander*, where the D.C. Circuit observed that "[p]olice departments across the country could face an intolerable burden if every 'search' of an ordinary fingerprint database were subject to Fourth Amendment challenges." 440 F.3d 489, 499 (D.C. Cir. 2006). However, the court there drew the analogy to fingerprints to support its holding that "accessing the DNA snapshots contained in the [DNA] database does not independently implicate the Fourth Amendment." *Id.* Because the Second Circuit already found that querying constitutes a separate Fourth Amendment event, *Hasbajrami*, 945 F.3d at 670, the "intolerable burden" contemplated in *Johnson* is inapplicable.

prepare papers and present the evidence to a magistrate. These are never very convincing reasons and, in these circumstances, certainly are not enough to bypass the constitutional requirement.").

Accordingly, balancing the substantial degree of intrusion with the powerful public interest, the Court finds that the queries conducted as to Defendant were unreasonable under the Fourth Amendment even had an exception to the warrant requirement applied.[27]

III. Exclusion of Evidence

Typically, to remedy a Fourth Amendment violation, *i.e.*, an impermissible warrantless search, courts apply the exclusionary rule to exclude unlawfully seized evidence and any fruits thereof. *See, e.g.*, *Segura v. United States*, 468 U.S. 796, 804 (1984) ("[T]he exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.' "); *see also Mapp v. Ohio*, 367 U.S. 643, 655 (1961) ("[T]he Fourth Amendment include[s] the exclusion of the evidence seized in violation of its provisions."). Nonetheless, the exclusionary rule is not absolute. *See* Wright & Miller, § 408 Privileges in General—Illegally Obtained Evidence, 2A Fed. Prac. & Proc. Crim. § 408 (4th ed.) (summarizing exceptions to the exclusionary rule). "[T]he significant costs of this rule have led [courts] to deem it 'applicable only . . . where its deterrence benefits outweigh its substantial social costs.'" *Utah v. Strieff*, 579 U.S. 232, 237 (2016) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). One exception to the exclusionary rule, the good faith exception, is a "judicially created" doctrine, *Herring v.*

[27] To be clear, the Court's ruling as to querying applies only to this case. This narrow holding accords with the clear mandate from the Second Circuit to only address the reasonableness of any querying "in this case." *Hasbajrami*, 945 F.3d at 676. In any event, the law has drastically changed since the relevant events here. When Congress renewed Section 702 in 2018, it imposed a requirement for the FBI to obtain a probable cause order from the FISA Court before reviewing the results of U.S. person queries in predicated criminal investigations unrelated to national security. 50 U.S.C. § 1881a(f)(2)(A). Because that amendment was passed after Defendant's arrest, the Court expressly declines to consider whether querying under the current statutory scheme comports with the Fourth Amendment.

United States, 555 U.S. 135, 139 (2009), and applies to government agents who "act with an objectively reasonable good-faith belief that their conduct is lawful," *Davis v. United States*, 564 U.S. 229, 238 (2011). Thus, "searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule." *Id.* at 232. This is because, in such cases, the "deterrence rationale" of the exclusionary rule "loses much of its force." *Id.* at 238 (internal quotation marks omitted).

In *Davis*, the Supreme Court applied the good faith exception to the warrantless search of a vehicle's passenger compartment because the search occurred before the Supreme Court's decision in *Arizona v. Gant*, 556 U.S. 332, 343 (2009), which announced a new rule governing automobile searches incident to an arrest. 564 U.S. at 239–41. While the officers' conduct "was in strict compliance with then-binding Circuit law and was not culpable in any way," it would have been unconstitutional under *Gant*. *Id.* at 239–40. Accordingly, because "[a]bout all that exclusion would deter in [that] case is conscientious police work," the Supreme Court declined to impose the "harsh" sanction of exclusion. *Id.* at 241 ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule."). In coming to this conclusion, the Court emphasized that

> [e]xclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth . . . . Our cases hold that society must swallow this bitter pill when necessary, but only as a "last resort." For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

Id. at 237 (internal citations omitted).

Likewise, here, the Court declines to impose the "harsh sanction" of exclusion because the good faith exception applies. According to the Government, [redacted] followed minimization procedures approved by the FISA Court and in place at the time when querying

Section 702-acquired information as to Defendant. [redacted] More importantly, the relevant queries here occurred in [redacted], long before agents could have been expected to know that the querying required a warrant. Exclusion based upon sequent legal developments, indeed based upon the holding in this opinion, would not serve the "deterrence rationale" when the agents running those queries at the time had an "objectively 'reasonable good-faith belief'" that those queries did not require a warrant. *Davis*, 564 U.S. at 238. As such, because the agents here conducted queries "in reasonable reliance on binding precedent" at the time, there in the form of FISC-approved procedures, the Court finds that exclusion is not warranted. *Id.* at 240.

Resisting this conclusion, Defendant argues that the good faith exception is unavailable because FISA provides a statutory remedy for the violation of his rights. (Def.'s Reply at 11.) Pursuant to 50 U.S.C. § 1806(g), if the Court "determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person." As the Government correctly notes, however, Defendant does not allege any violation of FISA procedure. Rather, Defendant alleges a violation of the Fourth Amendment. The question, therefore, is whether suppression under Section 1806(g) may remedy a Fourth Amendment violation.

United States v. Ning Wen is instructive on this question. 477 F.3d 896 (7th Cir. 2007). There, the Seventh Circuit considered whether to suppress evidence obtained from a FISA warrant that was used in a domestic criminal investigation. *Id.* at 898. The Seventh Circuit found that suppression was not required under Section 1806(g) because "the statutory standards for an intercept order have been satisfied." *Id.* at 897. After finding that Section 1806(g)

provided no basis for suppression, the Seventh Circuit proceeded to consider whether the Fourth Amendment required exclusion. *Id.* It did not, the court reasoned, because an "*in camera* review reveal[ed] that well-trained officers were entitled to rely on this warrant." *Id.* at 898.

The Court follows the approach in *Ning Wen* and will consider exclusion under Section 1806(g) and the Fourth Amendment as separate inquiries. The remedy provided for in Section 1806(g) is unavailable here because Defendant does not argue that the querying in question failed to meet FISA's statutory standards. And, although that querying violated the Fourth Amendment, such violations cannot be cured by Section 1806(g). In other words, any remedy for a violation of Defendant's rights under the Fourth Amendment must arise under the Fourth Amendment. Exclusion under the Fourth Amendment is inappropriate here because, as discussed, the good faith exception applies.

Defendant further argues that any claims of good faith ignore Judge Gleeson's "blunt characterization" of the government's purported misrepresentations in this case. (Def.'s Reply at 11.) This argument misses the mark. To the extent government lawyers misrepresented facts in the course of this litigation, such misconduct has no bearing on the good faith exception, which looks to whether the "executing officer" had an "objectively reasonable belief" to conduct the search. *See United States v. Eldred*, 933 F.3d 110, 121 (2d Cir. 2019). For the same reason, Defendant cannot avoid application of the good faith exception based on the reports he cites outlining general misconduct across law enforcement. (Def.'s Reply at 13–14.) Such reports, concerning as they may be, have no bearing on the law enforcement agents' conduct here.

IV. Disclosure to Defendant

Defendant moves for disclosure of the Government's unredacted briefing and factual record submitted on remand. (Def.'s Mem. at 82.) According to Defendant, "participation of

security-cleared defense counsel is necessary for FISA and the Fifth Amendment's Due Process protection to be satisfied." *Id.* The Court disagrees.

A. Disclosure Under FISA

When a defendant moves to suppress FISA evidence, the Government may file a declaration from the Attorney General stating that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). If the Attorney General files such a declaration, as done here, the district court must review the FISA materials *ex parte* and *in camera*, and may order disclosure of those materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* Disclosure is warranted only if the court finds that it cannot accurately resolve the lawfulness of the collection. *See United States v. Daoud*, 755 F.3d 479, 481,83 (7th Cir. 2014). But "disclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule." *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010) (internal quotation marks and citation omitted).

Here, disclosure under FISA is unnecessary. Having reviewed the supplemental record on remand, the Court agrees with the Government that such evidence is "relatively straightforward" and "not complex." *See id.* at 129 (affirming denial of disclosure request where "review of the FISA materials in this case [was] relatively straightforward and not complex"). Indeed, as the Government correctly notes, the record on remand is significantly less voluminous and complex than the general Section 702 materials that Judge Gleeson was able to review without ordering disclosure, and which finding the Second Circuit did not disturb. *See United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500, at *14 (E.D.N.Y. Mar. 8, 2016) ("After careful review of the FISA and Section 702 materials here it is clear to me that disclosure was unnecessary here."). As discussed, the record here is minimal. It consists of [redacted]

declarations, the longest of which is 21 pages, that themselves are summaries of the querying done here. This record, while lacking, does not require Defendant's review.[28]

Defendant also argues that failure to disclose would violate his right to due process. (Def.'s Mem. at 88.) In analyzing FISA, the "Second Circuit has made clear that proceeding *ex parte* does not, standing alone, offend notions of fundamental fairness." *United States v. Medunjanin*, 2012 WL 526428, at *9 (E.D.N.Y. Feb. 16, 2012) (collecting cases). While the Court recognizes the difficulties that a lack of disclosure must present defense counsel, the Court must also adhere to procedures designed to protect national security. *United States v. Fishenko*, 2014 WL 4804215, at *4 (E.D.N.Y. Sept. 25, 2014) ("Though the court is mindful of the difficulties that defense counsel must face in such circumstances, the FISA procedures are in place in the interest of national security."). Accordingly, having found that FISA does not warrant disclosure, the Court finds no violation of due process. *Abu-Jihaad*, 630 F.3d at 129 (2d Cir. 2010) (finding "no denial of due process in the district court's decision not to order disclosure of FISA materials to the defendant"); *see also Muhtorov*, 20 F.4th at 630 ("Neither the Supreme Court nor this court has recognized a due process right to notice of specific techniques the government used to surveil the defendant in a foreign intelligence investigation, nor to evidence collected when the evidence is not grounded in a specific due process right[.]"); *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987) (holding that FISA's ex parte in camera proceedings did not violate due process, even though defense counsel had high security clearances).

[28] Outside courts hearing Section 702 challenges have likewise found that disclosure was unwarranted. *E.g.*, *United States v. Muhtorov*, 20 F.4th 558, 623 (10th Cir. 2021) ("The district court did not abuse its discretion by declining to order disclosure under § 1806(f) after carefully reviewing the traditional FISA and Section 702 application materials."); *United States v. Mohamud*, 666 F. App'x 591, 597 (9th Cir. 2016) ("The district court did not abuse its discretion by denying Mohamud's security-cleared counsel access to classified [Section 702] materials under [FISA]").

B. Disclosure Under CIPA

The Classified Information Procedures Act ("CIPA") "establishes rules for the management of criminal cases involving classified information." *In re Terrorist Bombings*, 552 F.3d at 115. CIPA "is designed 'to protect[] and restrict[] the discovery of classified information in a way that does not impair the defendant's right to a fair trial.'" *Abu-Jihaad*, 630 F.3d at 140 (internal citation omitted). Section 3 of CIPA requires a district court to issue, upon "motion of the United States," a protective order "protect[ing] against the disclosure of any classified information disclosed by the United States to any defendant." 18 U.S.C. A. § App. 3 § 3. Section 4 establishes the procedures for the "[d]iscovery of classified information by defendants." *Id.* § App. 3 § 4. This provision "provides that, if the discovery to be provided to the defense pursuant to the Federal Rules of Criminal Procedure includes classified information, the district court may, 'upon a sufficient showing . . . authorize the United States to delete specified items of classified information . . . to substitute a summary of the information . . . or to substitute a statement admitting relevant facts that the classified information would tend to prove.'" *In re Terrorist Bombings*, 552 F.3d at 116 (quoting 18 U.S.C.A § App. 3 § 4).

Here, Defendant argues that CIPA provides a mechanism for disclosure to security-cleared defense counsel consistent with due process and national security. (Def.'s Mem. at 96.) While Defendant correctly notes that CIPA provides a "mechanism" for disclosure, "it does not provide [Defendant] a freestanding right to classified information." *United States v. Lustyik*, 833 F.3d 1263, 1271 (10th Cir. 2016); *see also United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) ("CIPA does not create any discovery rights for the defendant."). This is because CIPA "does not give rise to an independent right to discovery." *United States v. Lustyik*, 833 F.3d 1263, 1271 (10th Cir. 2016). Rather, it "provides guidance to trial judges applying [Rule 16(d)]

where confidential information is involved," *id.*, and "clarifies district courts' power under [Rule 16(d)] to issue protective orders denying or restricting discovery for good cause." *United States v. Aref*, 533 F.3d 72, 78 (2d Cir. 2008). Because the Court already found disclosure to be inappropriate under FISA, the operative statute here, CIPA does not confer any additional disclosure obligation.

C. Remaining Arguments for Disclosure

Defendant raises several other arguments for disclosure, none of them persuasive to the Court. For example, Defendant cites past instances of government abuse in applying for and renewing FISA surveillance, along with prior FISC opinions identifying non-compliance issues with FISA acquisition and minimization. (Def.'s Mem. at 62–82.) While the Court is receptive to Defendant's concerns about the FISA process evidenced in those examples, past instances of misconduct do not confer any disclosure obligation here. *See Muhtorov*, 20 F.4th at 622 (rejecting argument for disclosure of information acquired under Section 702 "based solely on the government's behavior in other cases"); *United States v. Warsame*, 547 F. Supp. 2d 982, 987–88 (D. Minn. 2008) ("The fact that the government has included misstatements and critical omissions in other FISA applications not at issue here cannot justify disclosure in this case.").

Defendant also argues for disclosure of the supplemental record here based on the Government's alleged lack of candor that led to the remand. (Def.'s Mem. at 85–86.) According to Defendant, this case uniquely merits disclosure because "[i]t 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." *Id.* at 85. And the Second Circuit remanded, Defendant maintains, because the Government "essentially refused" to provide the Second Circuit with information about querying. *Id.* While the Court is mindful of

the unique nature of this appeal—due largely to the Government's delayed and incomplete disclosures—those reasons alone are insufficient to require disclosure here.

Finally, Defendant requests notice of any other surveillance tools used in his investigation. (Def.'s Mem. at 124–30.) Defendant is entitled, so he argues, "to notice of whatever *other* surveillance tools" were used in his investigation, including from programs other than Section 702 or FISA. (*Id.*). As the Government correctly notes, the limited remand from the Second Circuit provides no basis to grant Defendant this relief, the request is denied.

CONCLUSION

For the foregoing reasons, Defendant's supplemental motion to suppress is DENIED.

SO ORDERED.

Dated: Brooklyn, New York
December 2, 2024

/s/ LDH
LASHANN DEARCY HALL
United States District Judge