UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
	)	No. 16 CR 181
v.	)	
	)	Judge Sara L. Ellis
AWS MOHAMMED YOUNIS AL-JAYAB,	)	
	)	
Defendant.	)	

OPINION AND ORDER

The government has charged Defendant Aws Mohammed Younis al-Jayab with attempting to provide material support to terrorists in violation of 18 U.S.C. § 2339A in connection with time he spent in Syria between November 2013 and January 2014. As with other cases involving alleged international terrorism, complex issues surrounding electronic and physical surveillance, a defendant's interest in discovery, and the government's national security interests arise here. The Court has before it a number of motions concerning these issues. The government filed an *ex parte*, *in camera* motion for a protective order pursuant to Section 4 of the Classified Information Procedures Act ("CIPA") and Federal Rule of Criminal Procedure 16(d)(1) to authorize the government to withhold classified documents from al-Jayab [55]. The government also seeks a finding that the physical search at issue in this case was lawfully authorized and conducted in compliance with the Foreign Intelligence Surveillance Act of 1978 ("FISA") and a denial of al-Jayab's motion to suppress. Al-Jayab has filed the following: (1) motion to suppress evidence obtained or derived from warrantless surveillance under Section 702 of the FISA Amendments Act ("FAA"),[1] 50 U.S.C. § 1881a [47]; (2) objection to secret *ex parte* CIPA litigation of Fourth Amendment suppression issues and motion for disclosure to

[1] Al-Jayab refers to § 702 of the FAA. As the government points out, although § 702 was added by the FAA, it is appropriately referred to as § 702 of FISA.

cleared counsel [50]; (3) motion for discovery regarding the intelligence agencies' surveillance pursuant to Executive Order 12333 [51]; (4) motion for notice of surveillance techniques used during the course of investigation [52]; and (5) *ex parte* and under seal memorandum of defense [54]. Al-Jayab also seeks disclosure of the underlying FISA and § 702 materials.[2] The Court has carefully reviewed the parties' filings and conducted several hearings on the pending motions. It now sets forth its detailed rulings on each of the pending motions below.

BACKGROUND

I. Factual Background[3]

Al-Jayab was born in Iraq. He moved to Syria with his family in March 2012 and then arrived in the United States as a refugee in October 2012. Initially upon arriving in the United States, he lived in Tucson, Arizona and Milwaukee, Wisconsin.

Almost immediately after his arrival in the United States, al-Jayab indicated to family members and others that he intended to return to Syria, using Turkey as a potential transit point. In his communications on Facebook with various individuals, al-Jayab stated that he wanted to work with Ansar al-Islam or the al-Nusra Front, making specific plans to do so.[4] Al-Jayab explained to an associate that he joined the mujahidin when he was sixteen and fought for the group now known as Ansar al-Islam. He spoke of his prior experience fighting in Syria, sending

---

[2] Al-Jayab has also filed a motion to dismiss the indictment based on combatant immunity [91], which the parties are currently briefing. The Court does not address this motion here, although it takes al-Jayab's arguments into account in determining whether evidence the government seeks to withhold pursuant to CIPA § 4 would be relevant or helpful to al-Jayab's stated intention to pursue a combatant immunity defense.

[3] The Court draws much of the factual background from the criminal complaint filed in *United States v. al-Jayab*, No. 16 CR 08, Doc. 1 (E.D. Cal. Jan. 6, 2016).

[4] The United States has designated both Ansar al-Islam and the al-Nusra Front as foreign terrorist organizations ("FTOs") pursuant to Section 219 of the Immigration and Nationality Act.

photographs of himself with various weapons and at a gun range in Wisconsin. Al-Jayab also communicated with Abu 'Akkab al-Muhajir, who was based in Syria and used his Facebook account to distribute propaganda for the Islamic State of Iraq and the Levant ("ISIL").[5] Al-Jayab requested money from al-Muhajir to travel to Syria, and al-Muhajir indicated he would make arrangements to provide al-Jayab with the needed funds.

On November 6, 2013, al-Jayab received an auto insurance settlement. The following day, al-Jayab wrote to al-Muhajir, indicating that he no longer needed money for his travels and instead would only need help once he arrived in Turkey. Al-Jayab then purchased an airline ticket on November 8, flying directly from Chicago to Istanbul, Turkey on November 9. Analysis of the internet protocol ("IP") addresses al-Jayab used to access Facebook, his email accounts, and other communications imply that he was in Syria from November 2013 through January 2014. In these communications, al-Jayab told his brother he would be entering Syria with the mujahidin and indicated he had an assault rifle. His brother advised him in one message to remove a picture from Facebook that showed him wearing a military uniform. Although al-Jayab discussed infighting among certain Sunni extremist groups in Syria, he suggested that he had joined in the fighting against the Free Army. Al-Jayab represents in his filings that while he was in Syria, he fought with Ansar al-Sham, a group that is not a designated FTO, and which joined with other groups under the umbrella of the Islamic Front to fight against Bashar al-Assad and his regime.[6]

[5] The U.S. Secretary of State designated al Qaida in Iraq as an FTO in 2004. In 2014, the government amended the designation to include the alias "Islamic State of Iraq and the Levant" (or ISIL) as its primary name.

[6] Similar to Ansar al-Sham, the government has not designated the Islamic Front as an FTO.

On January 17, 2014, IP address records demonstrate that al-Jayab left Syria and entered Turkey. On January 23, 2014, al-Jayab returned to Sacramento, California by way of London and Los Angeles. In his customs declaration form, he did not mention traveling to Turkey or Syria, listing only Jordan and the United Kingdom as the countries he visited during his time abroad.

On July 29, 2014, United States Citizenship and Immigration Services ("USCIS") employees interviewed al-Jayab in connection with his application for an adjustment of his immigration status. Al-Jayab admitted in that interview that he had traveled to Turkey and returned approximately six months before the interview, *i.e.,* in January 2014. Al-Jayab had another interview with USCIS on October 6, 2014, during which he denied any terrorist affiliations and indicated that he went to Turkey to visit his grandmother. On June 18, 2015, al-Jayab met with Federal Bureau of Investigation ("FBI") agents at his request regarding issues he experienced at the airport while traveling. He stated during this meeting that he traveled to Turkey for vacation but denied having entered Syria.

II. Procedural History

The government represents that its investigation of al-Jayab began in or around February 2014, [redacted]

[redacted]

[redacted]

Ultimately, on January 7, 2016, officials arrested al-Jayab in the Eastern District of California pursuant to a federal criminal complaint filed in that district, charging him with providing materially false statements to federal agents in a matter involving international terrorism in violation of 18 U.S.C. § 1001. *United States v. al-Jayab*, No. 16 CR 08, Doc. 1 (E.D. Cal.). On January 14, 2016, a grand jury in the Eastern District of California returned an indictment charging al-Jayab with making false statements to a USCIS agent on or about October 6, 2014. *Id.* Doc. 13.

On March 17, 2016, the government indicted al-Jayab in this district and charged him with "attempt[ing] to provide material support and resources, namely, personnel (including himself), knowing and intending that they were to be used in the preparation for, and in carrying out a violation of Title 18, United States Code, Section 956(a)(1) (conspiracy to kill, kidnap, maim, or injure persons outside of the United States)," in violation of 18 U.S.C. § 2339A. Doc. 1. This charge includes an intent requirement, with the government having to prove that "the defendant had the specific intent to provide material support, knowing or intending that it would be used in a conspiracy to kill persons abroad." *United States v. Mehanna*, 735 F.3d 32, 43 (1st Cir. 2013); *see also United States v. Stewart*, 590 F.3d 93, 113 & n.18 (2d Cir. 2009) ("[T]he mental state in section 2339A extends both to the support itself, and to the underlying purposes for which the support is given."). On April 8, 2016, the government provided notice to al-Jayab that, "pursuant to Title 50, United States Code, Section 1825(d) and 1881e(a), the United States

intends to offer into evidence, or otherwise use or disclose in any proceedings in this matter, information obtained or derived from physical searches and acquisitions acquired pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, Title 50, United States Code, Section 1821-1829 and 1881a." Doc. 14.

ANALYSIS

I. CIPA Section 4 [55]

The government has moved for a protective order pursuant to CIPA § 4 to withhold certain classified material from discovery. CIPA's fundamental purpose is to "protect[ ] and restrict[ ] the discovery of classified information in a way that does not impair the defendant's right to a fair trial." *United States v. O'Hara*, 301 F.3d 563, 568 (7th Cir. 2002). CIPA is a procedural statute; it "creates no new rights of or limits on discovery of a specific area of classified information," instead "contemplat[ing] an application of the general law of discovery in criminal cases to the classified information area with limitations imposed based on the sensitive nature of the classified information." *United States v. Yunis*, 867 F.2d 617, 621 (D.C. Cir. 1989). Section 4 of CIPA provides:

> The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

18 U.S.C. App. 3 § 4; *see also* Fed. R. Crim. P. 16(d)(1) & advisory committee notes to 1966 amendment (allowing courts to deny or restrict discovery based on an *ex parte* good cause showing, with advisory committee notes indicating that "good cause" includes "the protection of information vital to the national security").

Although the Seventh Circuit has not addressed the standard a district court should use in analyzing the government's request, other circuits use a four-part test to resolve CIPA discovery motions:

> [1] When considering a motion to withhold classified information from discovery, a district court must first determine whether, pursuant to the Federal Rules of Criminal Procedure, statute, or the common law, the information at issue is discoverable at all.
>
> [2] If the material at issue is discoverable, the court must next determine whether the government has made a formal claim of the state secrets privilege lodged by the head of the department which has actual control over the matter, after actual personal consideration by that officer.
>
> [3] Once a court concludes that the material is discoverable and that the state secrets privilege applies, then the court must determine whether the evidence is relevant and helpful to the defense of [the] accused.
>
> [4] If the information meets the relevant and helpful test, CIPA § 4 empowers courts to determine the terms of discovery, if any.

United States v. Turner, No. 13 CR 572-2, 2014 WL 3905873, at *2 (N.D. Ill. July 29, 2014) (quoting *United States v. Sedaghaty*, 728 F.3d 885, 904 (9th Cir. 2013)). Some courts have also added a final step of balancing "the Government's interest in nondisclosure against the defendant's need for the information." *United States v. Hanjuan Jin*, 791 F. Supp. 2d 612, 619–20 (N.D. Ill. 2011).

"To be helpful or material to the defense, evidence need not rise to the level that would trigger the Government's obligation under *Brady v. Maryland*, 373 U.S. 83, 83 S. Ct. 1194, 10 L.

Ed. 2d 215 (1963), to disclose exculpatory information." *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008); *see also United States v. Mejia*, 448 F.3d 436, 456–57 (D.C. Cir. 2006) ("While *Brady* information is plainly subsumed within the larger category of information that is 'at least helpful' to the defendant, information can be helpful without being 'favorable' in the *Brady* sense[.]"). But because the defendant does not have access to the classified information, the defendant and the Court are disadvantaged in determining whether the classified information at issue is relevant and would be helpful to the defense. *See Mejia*, 448 F.3d at 458 ("[T]he defendants and their counsel, who are in the best position to know whether information would be helpful to their defense, are disadvantaged by not being permitted to see the information—and thus to assist the court in its assessment of the information's helpfulness."). The Court discusses this concern further in connection with al-Jayab's objections to the *ex parte* litigation of the CIPA motion.

If, after its review, the Court finds that the classified information is relevant and helpful to the defense, the Court should consider "the protective options short of full disclosure that are set forth in CIPA § 4, namely permitting the government 'to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.'" *Mejia*, 448 F.3d at 456 n.18 (quoting 18 U.S.C. App. 3 § 4). The Court proceeds first to al-Jayab's objections to the CIPA procedures and then to the substance of the CIPA motion itself.

A. Al-Jayab's Objections to the CIPA Procedures [50]

Al-Jayab objects to the Court's *ex parte, in camera* review of the government's CIPA § 4 motion, arguing that defense counsel with the appropriate clearance should be allowed to review the motion and its underlying documents. Specifically, al-Jayab seeks disclosure to cleared

counsel, under an appropriate protective order, of surveillance-related information that may be relevant and helpful to his defense in seeking suppression as well as disclosure of the government's legal arguments in support of its § 4 application. He argues that the government is improperly using CIPA's procedures to litigate Fourth Amendment suppression issues without defense participation instead of using CIPA merely to make relevancy and admissibility determinations. The Court disagrees, however, and finds the *ex parte* nature of the government's motion appropriate.

Both CIPA § 4 and Federal Rule of Criminal Procedure 16(d)(1) provide for *ex parte*, *in camera* procedures. *See* 18 U.S.C. App. 3 § 4 (government may request authorization to delete classified information from discovery "in the form of a written statement to be inspected by the court alone"); Fed. R. Crim. P. 16(d)(1) (court may deny or restrict discovery for good cause, allowing party to show good cause "by a written statement that the court will inspect ex parte"). Courts have routinely upheld the *ex parte*, *in camera* nature of CIPA § 4 proceedings. *See United States v. Abu-Jihaad*, No. 3:07CR57(MRK), 2007 WL 2972623, at *1 (D. Conn. Oct. 11, 2007) (collecting cases).[7] Following CIPA's legislative history, these courts reason that "[w]hen the 'government is seeking to withhold classified information from the defendant, an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules.'" *Aref*, 533 F.3d at 81 (quoting H.R. Rep. 96-831, pt. 1, at 27 n.22)); *see also United States v. Amawi*, 695 F.3d 457, 472 (6th Cir. 2012) ("The purpose of CIPA is to provide a means for the courts to oversee the government's authority to delete evidence from discovery. To permit defense counsel to participate in such a hearing would frustrate the aim of CIPA."); *cf. United States v.*

[7] The Second Circuit later affirmed the district court's grant of the government's CIPA motions, finding that it properly considered those motions *ex parte*. *See United States v. Abu-Jihaad*, 630 F.3d 102, 143 (2d Cir. 2010).

Daoud, 755 F.3d 479, 482 (7th Cir. 2014) (rejecting contention that "adversary procedure is always essential to resolve contested issues of fact").

A court in the Northern District of Ohio recently rejected the same arguments made by al-Jayab here, finding that cleared counsel for the defendant was not entitled to disclosure of the government's § 4 motion or, alternatively, to the legal arguments supporting the motion. *See United States v. Mohammad*, No. 3:15-cr-358, 2017 WL 2568834, at *2–3 (N.D. Ohio June 13, 2017). This Court adopts the analysis and conclusions of the *Mohammad* court. Although al-Jayab's counsel holds a security clearance, as other courts have found, "[t]he possession of a security clearance only becomes relevant *after* the district court determines, in accordance with section 4, that any classified information is discoverable." *Amawi*, 695 F.3d at 473.

Finally, al-Jayab's concerns about recent disclosures of the government's alleged improper use of CIPA procedures in other cases does not warrant providing counsel access in this case, where the Court's review of the motion and materials indicates that the government is not attempting to litigate Fourth Amendment suppression issues here. Although there have been reports of the government's non-compliance with discovery obligations in unrelated surveillance programs, the Court has closely reviewed the government's submission and does not find that these generalized complaints apply here. The government has not sought to establish an exception to the fruit of the poisonous tree doctrine or the good faith exception, or argued that the surveillance was otherwise lawful by way of its CIPA motion. Instead, the government has restricted its arguments to whether it must disclose the surveillance at issue on relevancy grounds pursuant to CIPA § 4. The Court need not further address al-Jayab's arguments.

Consequently, the Court has considered the government's CIPA motion *ex parte*. The Court provided al-Jayab with the opportunity to outline his theories of defense, which he has

done in an *ex parte* and under seal document [54]. Although this does not amount to access to the documents themselves, courts have recognized this as a reasonable substitute to help the Court assess the documents the government seeks to withhold. *See Turner*, 2014 WL 3905873, at *3 (describing similar process). In reviewing the government's submission, the Court has taken into account al-Jayab's submission and "place[d] [itself] in the shoes of defense counsel, the very ones that cannot see the classified record, and act[ed] with a view to their interests" to determine whether the information would be "relevant and helpful" to al-Jayab. *Amawi*, 695 F.3d at 471; *Mejia*, 448 F.3d at 458 (applying an "'at least helpful' test in a fashion that gives the defendants the benefit of the doubt").

B. Materials at Issue

[redacted]

[redacted]

[redacted] the Court first addresses the classified nature of the material the government seeks to withhold. In seeking to withhold this information pursuant to CIPA § 4, the government acknowledges that it is discoverable. The Court also finds that the materials at issue contain or involve classified information. Carl Ghattas, the Assistant Director for the Counterterrorism Division of the FBI, has provided a declaration asserting the classified information privilege with respect to [redacted] the government seeks to withhold. *See* Ghattas Decl. to CIPA Motion. The Attorney General has delegated original classification authority to Ghattas. *See* Executive Order 13526, § 1.3(c). Ghattas states that disclosure of the existence or content of the materials at issue may reasonably be expected to cause serious damage to the national security of the United States. *See Yunis*, 867 F.2d at 623 (government has a security interest not only in the contents of the classified information but also in "the time, place, and nature of the government's ability to intercept the communications at all," and the

[redacted]

protection of the government's "intelligence-gathering capabilities" that could be gleaned from what documents "revealed about sources and methods" is a legitimate national security concern expressly recognized by the Supreme Court); *CIA v. Sims*, 471 U.S. 159, 175, 105 S. Ct. 1881, 85 L. Ed. 2d 173 (1985) ("The government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service." (quoting *Snepp v. United States*, 444 U.S. 507, 509 n.3, 100 S. Ct. 763, 62 L. Ed. 2d 704 (1980)).

Having made these preliminary findings, the Court turns to whether the material at issue is relevant and helpful to the defense. The government represents that it will not offer the information it seeks to withhold in its prosecution of al-Jayab. It also contends that it has already produced some of the material in other forms. Regardless of these representations, the Court must still consider whether the information would be relevant and helpful to al-Jayab, in light of the crime charged and al-Jayab's possible defenses, as set forth in his memorandum of defense. Specifically, in reviewing the government's arguments and the selected documents, the Court has kept the following potential defenses in mind: the lack of sufficient *mens rea* to commit the crime charged in that although he traveled to Syria to fight Assad, he did this because he thought Assad was a tyrant, shaped by al-Jayab's prior history growing up in Iraq and Syria, the lack of evidence to support the fact that al-Jayab intended to provide material support, and evidence of al-Jayab's activities or time while in Syria, particularly any mention of his association with Ansar al-Islam or the Islamic Front, the organizations with which al-Jayab claims he fought while in Syria and which form the basis of his combatant immunity motion.

To assist its review of the materials provided by the government, the Court met with the parties several times in *ex parte* settings. In the course of some of these meetings with the

government, the Court identified [redacted] about which it needed additional information before making a determination as to whether [redacted] qualified for withholding. The government provided additional information to the Court in both oral and written form.

[redacted]

[redacted] The Court agrees that the government does not need to produce this material, where it contains nothing the defense could deem relevant or helpful.

[redacted]

[redacted] Moreover, the Court does not find these [redacted] helpful to the defense. As the government posits, the [redacted] are inculpatory and unrelated to the charges in this case. [redacted]

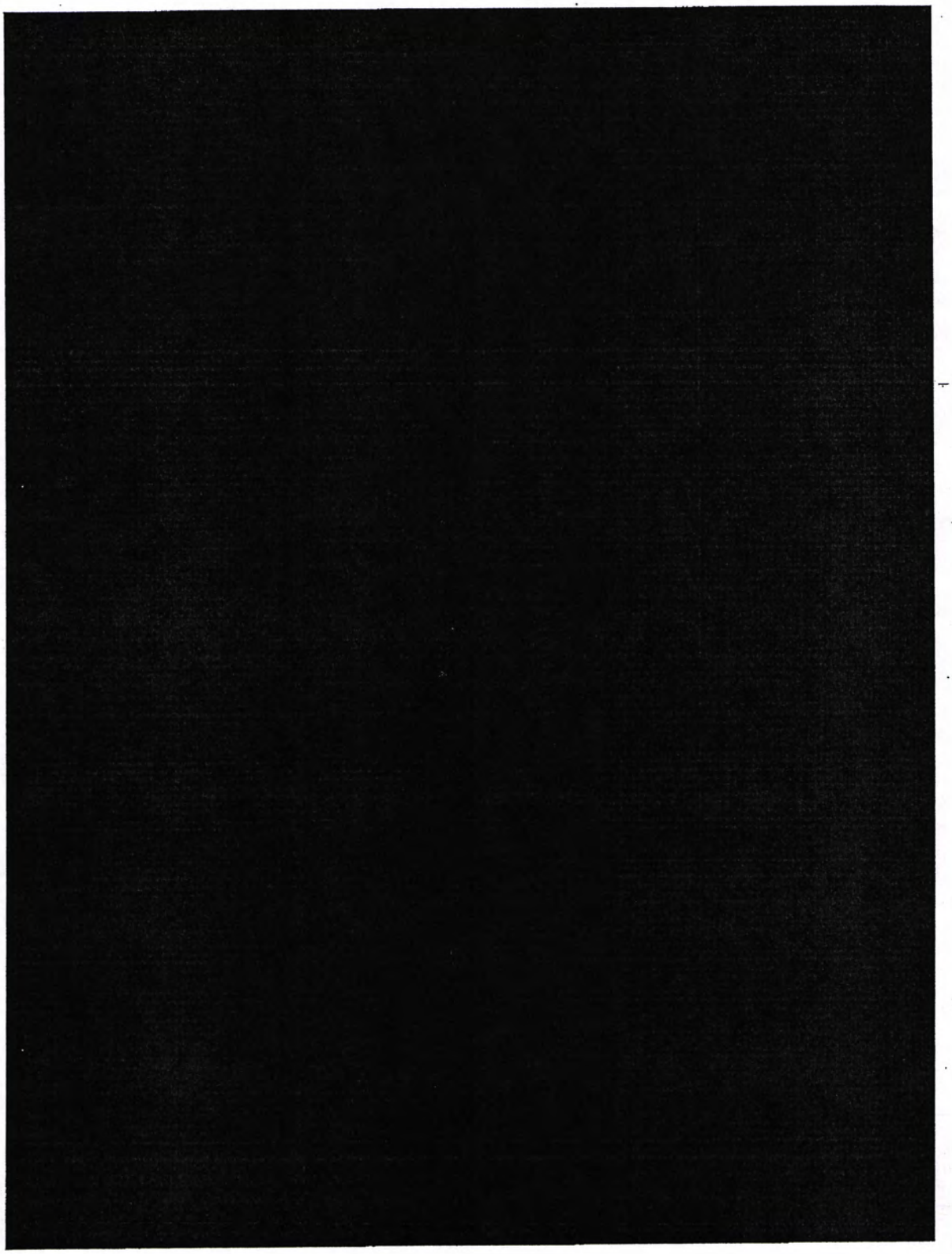
[redacted]

[redacted]

[redacted]. The Court thus fails to see how these [redacted] could aid the defense.

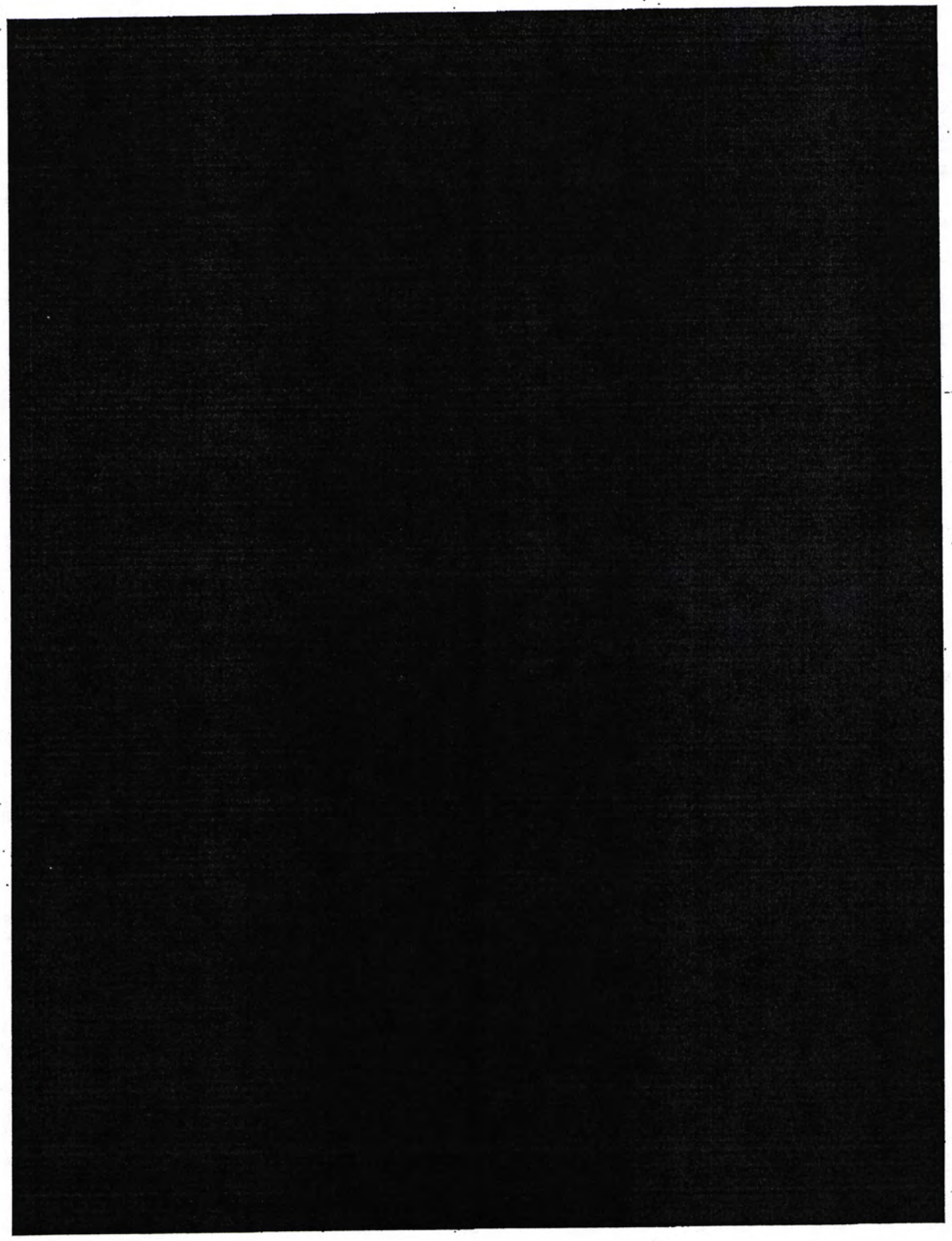
[redacted]. The Court does not find disclosure of the [redacted] necessary, and the government may properly withhold them from discovery.

[redacted]



[redacted] Although the Court may question the sensitivity of this information and whether disclosure would harm national security, it notes the words of another district judge in a similar situation: "And to the extent that I might question whether disclosure of other, apparently less sensitive but still classified information would create any real risk to national security, I should be very cautious about substituting my judgment for that of those who know more than I, and whose job it is to know better than I, just what those risks might be." *United States v. Amawi*, 531 F. Supp. 2 832, 838 n.10 (N.D. Ohio 2008), *aff'd*, 695 f.3d 457 (6th Cir. 2002); *see also Yunis*, 867 F.2d at 623 ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods.").

[redacted] the government acknowledges that any relevant statements by al-Jayab would traditionally be produced as written or recorded statements of the defendant pursuant to Rule 16(a)(1)(B), with any relevant videos, photographs, and other attachments subject to an argument that they are discoverable as either material to the defense or belonging to the defendant pursuant to Rule 16(a)(1)(E)(i) and (iii). But the government contends that none of the statements are both relevant and helpful and that disclosure would harm national security. [redacted]



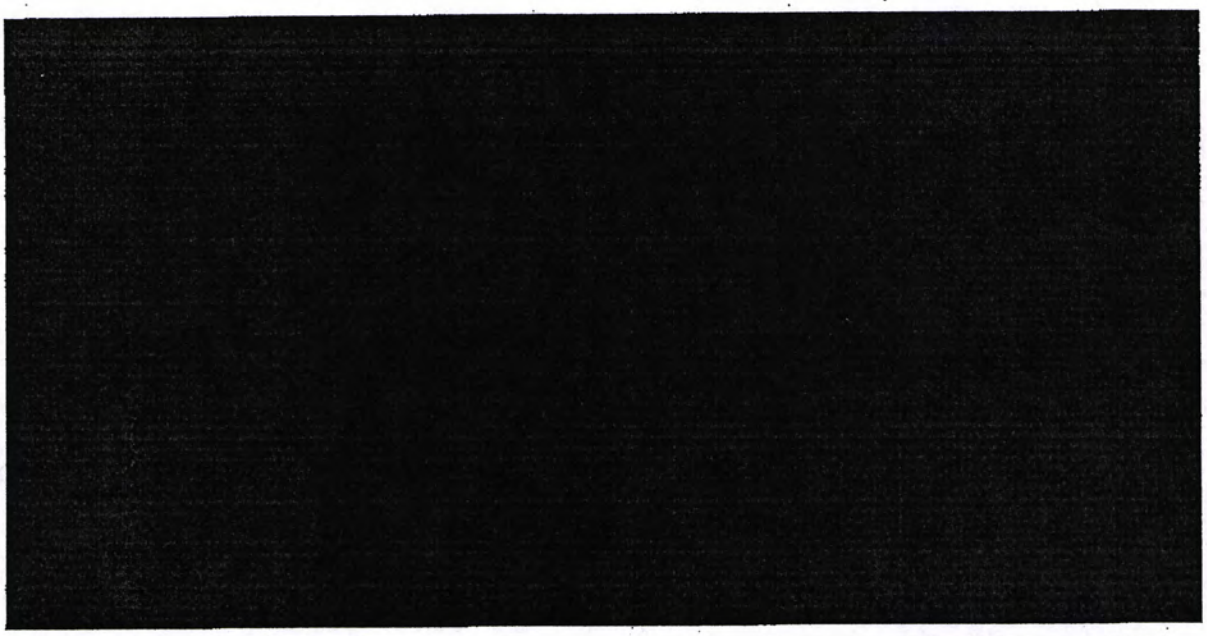
[redacted]

Therefore, having reviewed the [redacted] and found them not relevant or helpful to the defense, the Court finds that the government may properly withhold them.

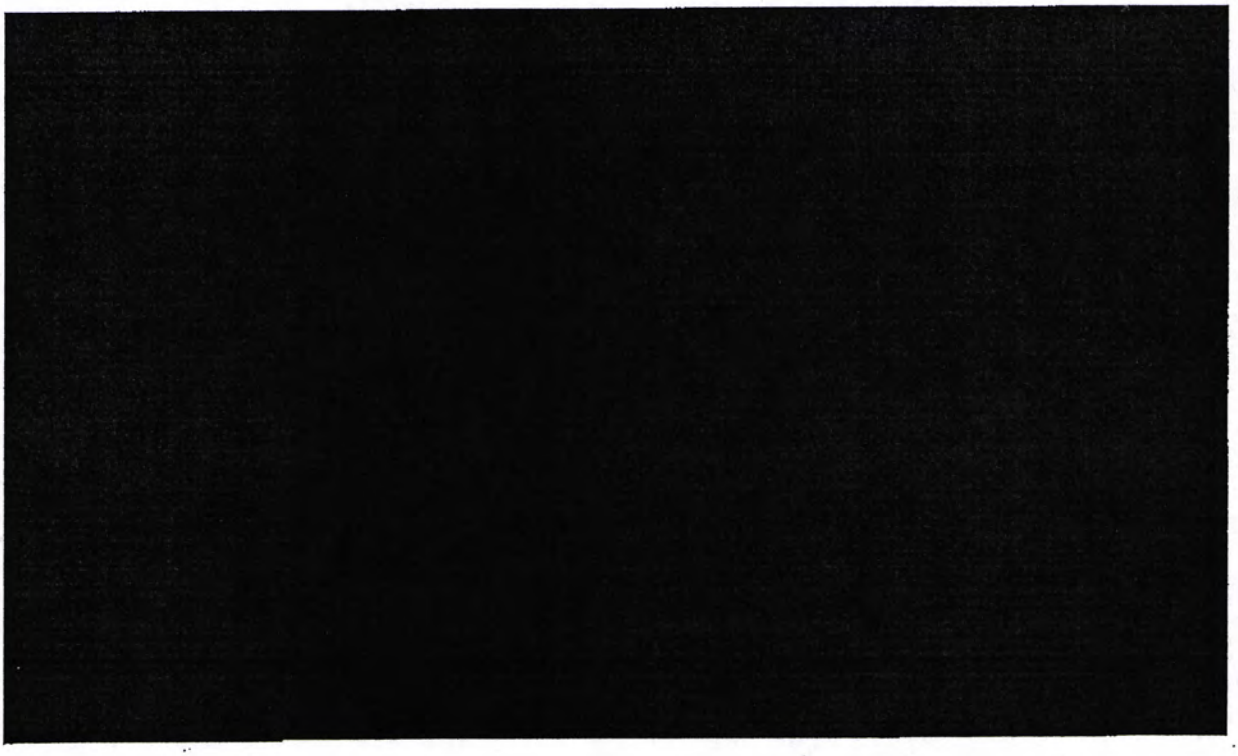
[redacted]

[redacted] The Court agrees that these [redacted] which do not contain any information related to the charges in this case, are irrelevant.

[redacted]



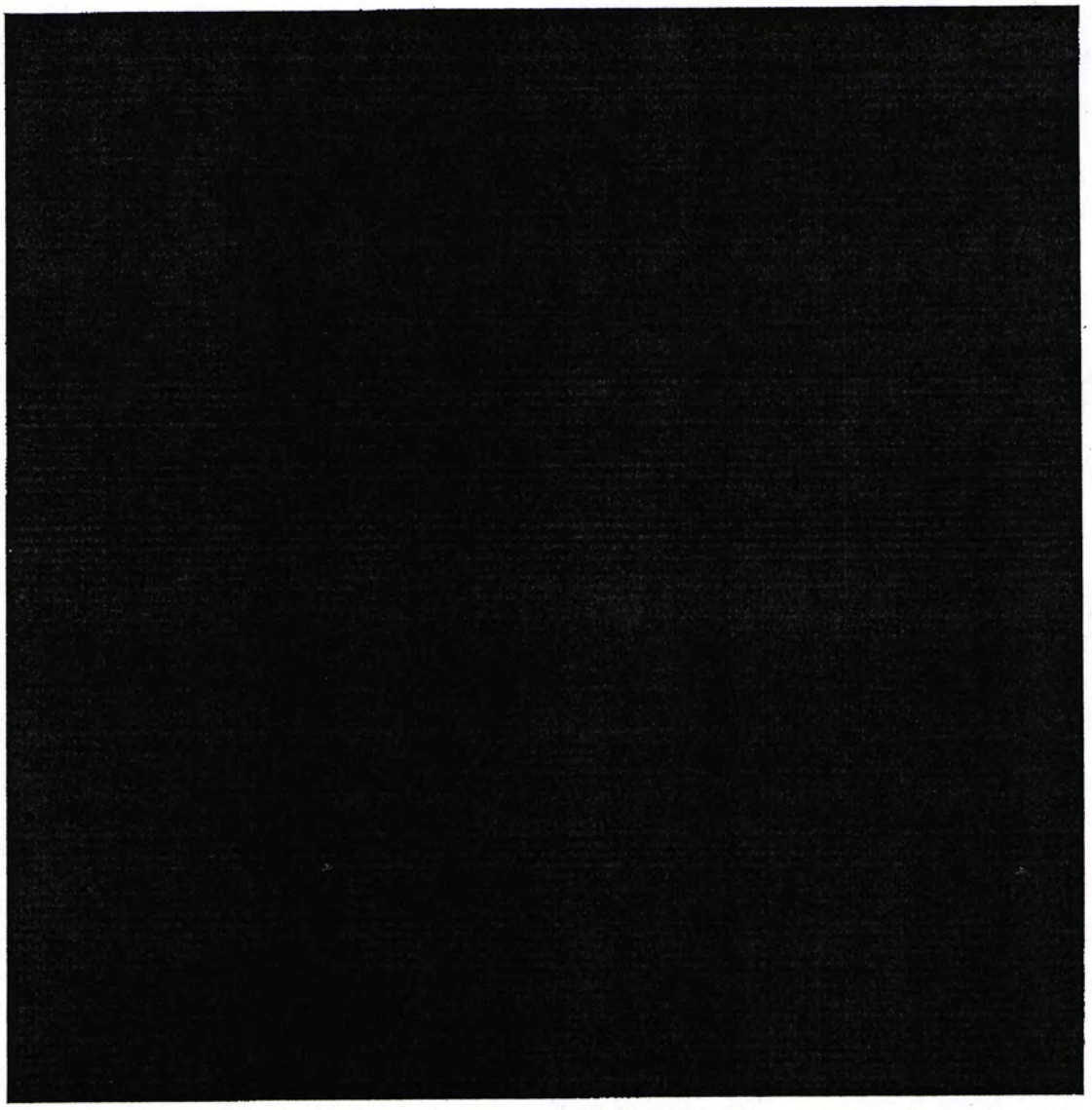
The Court's review of the remainder of the [redacted] provided to it demonstrates that the remaining [redacted] are not relevant or helpful and are properly withheld from discovery.



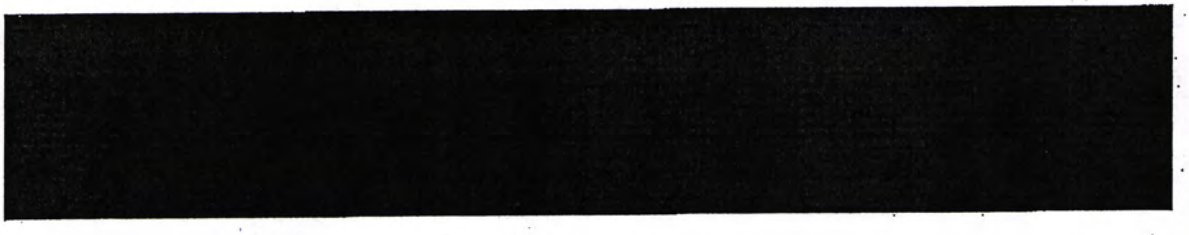
[redacted]

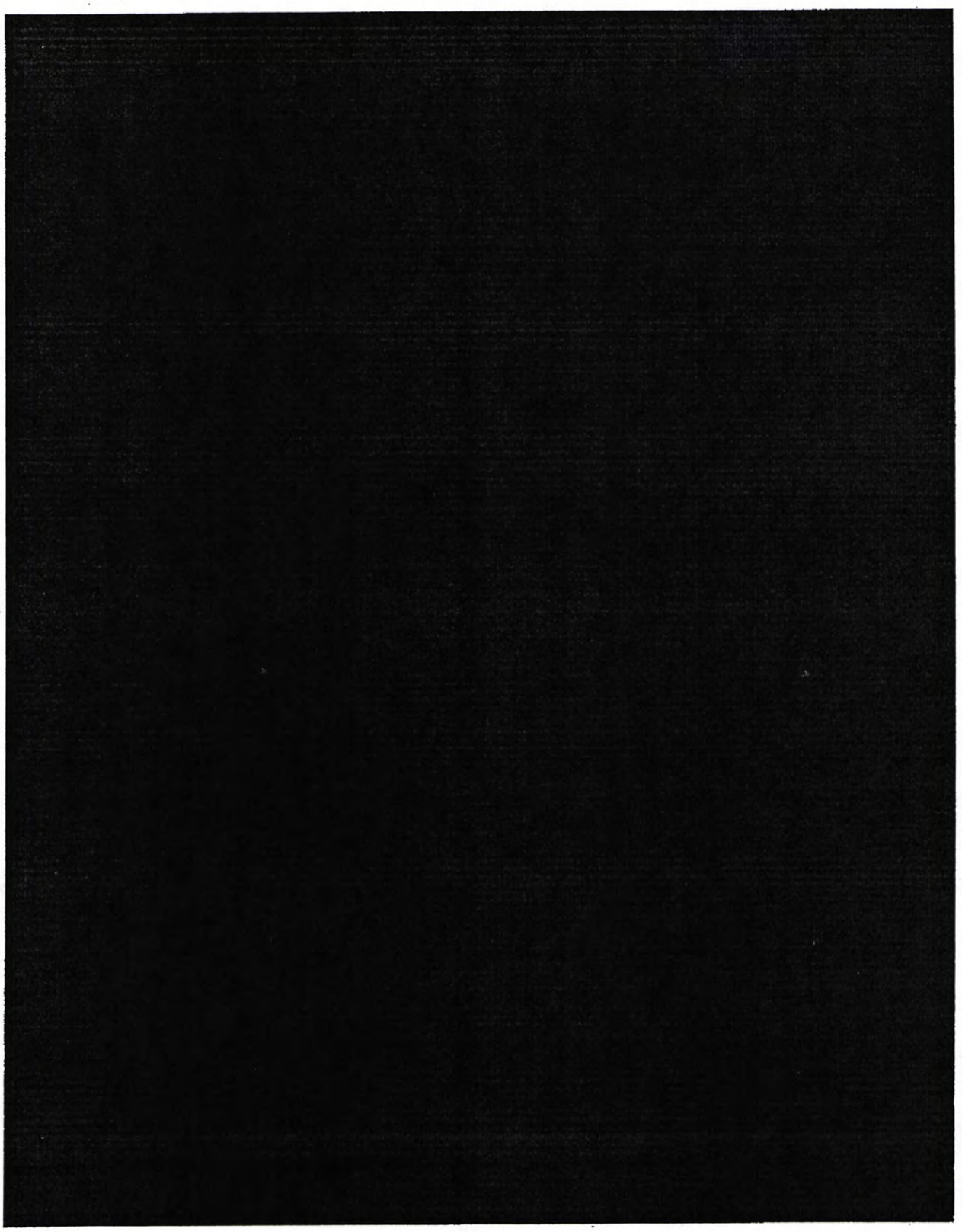
Having reviewed the representative samples provided by the government, the Court finds that the [redacted] are either irrelevant or, to the extent relevant, not helpful to the defense..

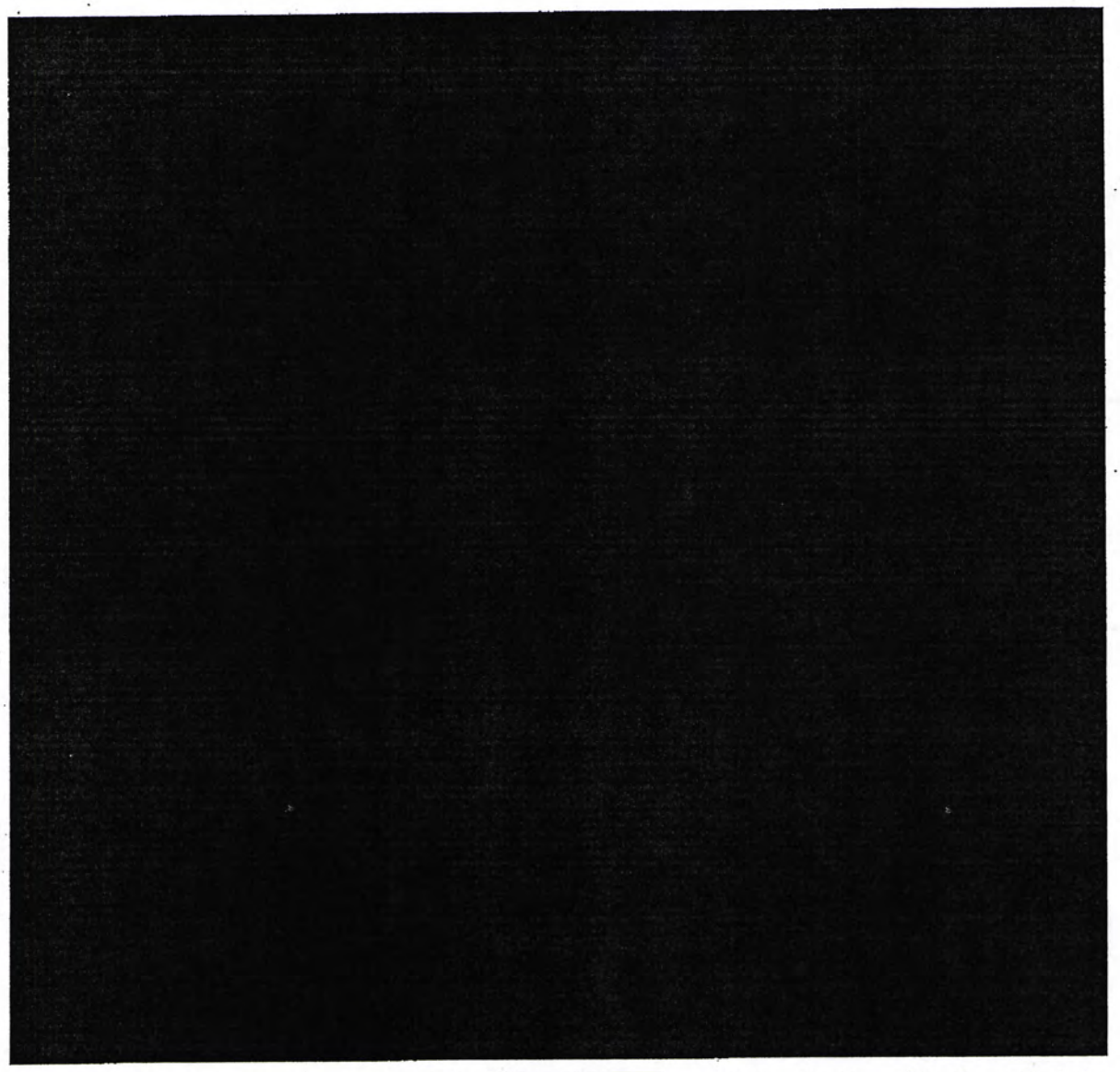
[redacted]



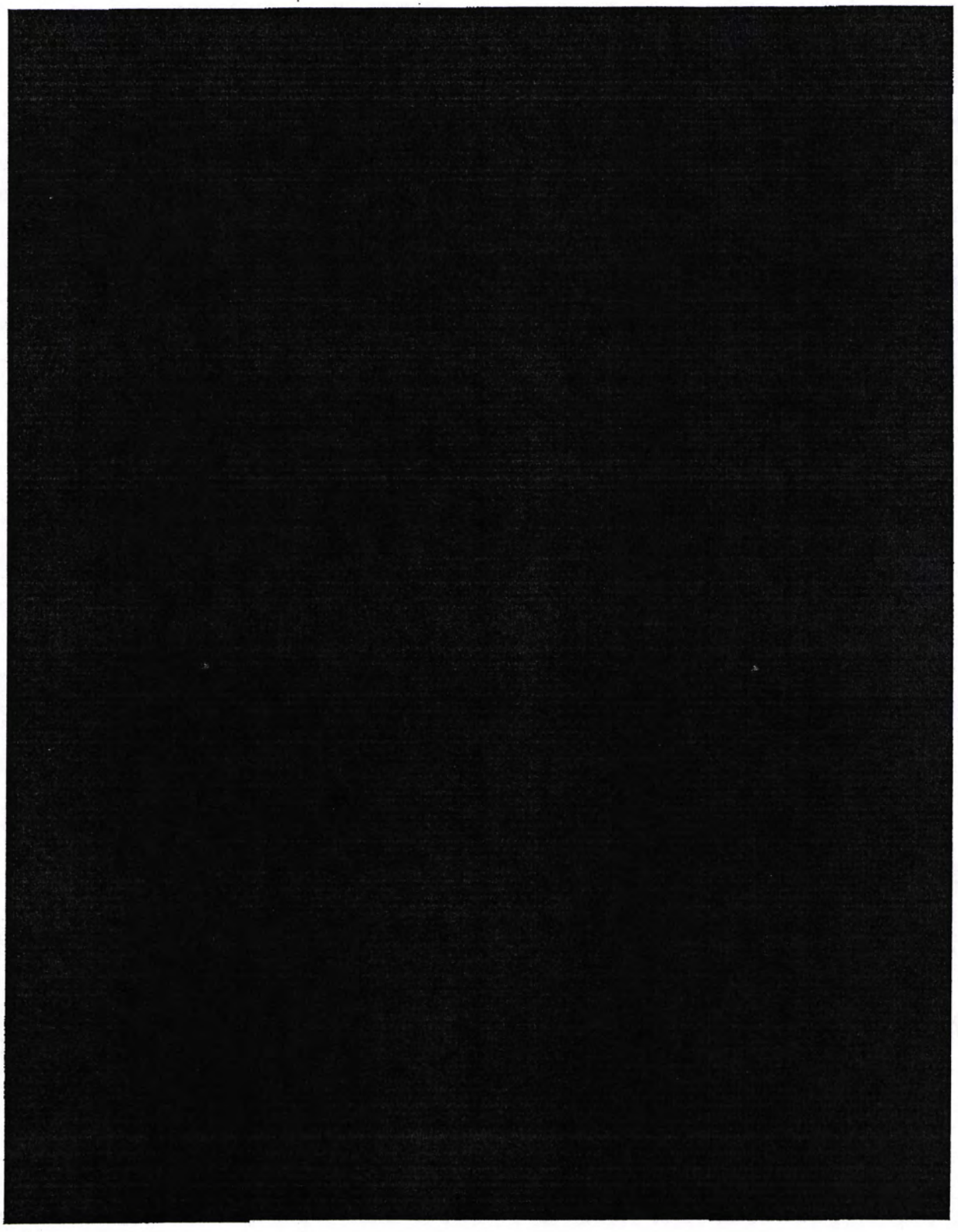
Having reviewed these and the remaining [redacted] the Court therefore finds it proper for the government to withhold them.

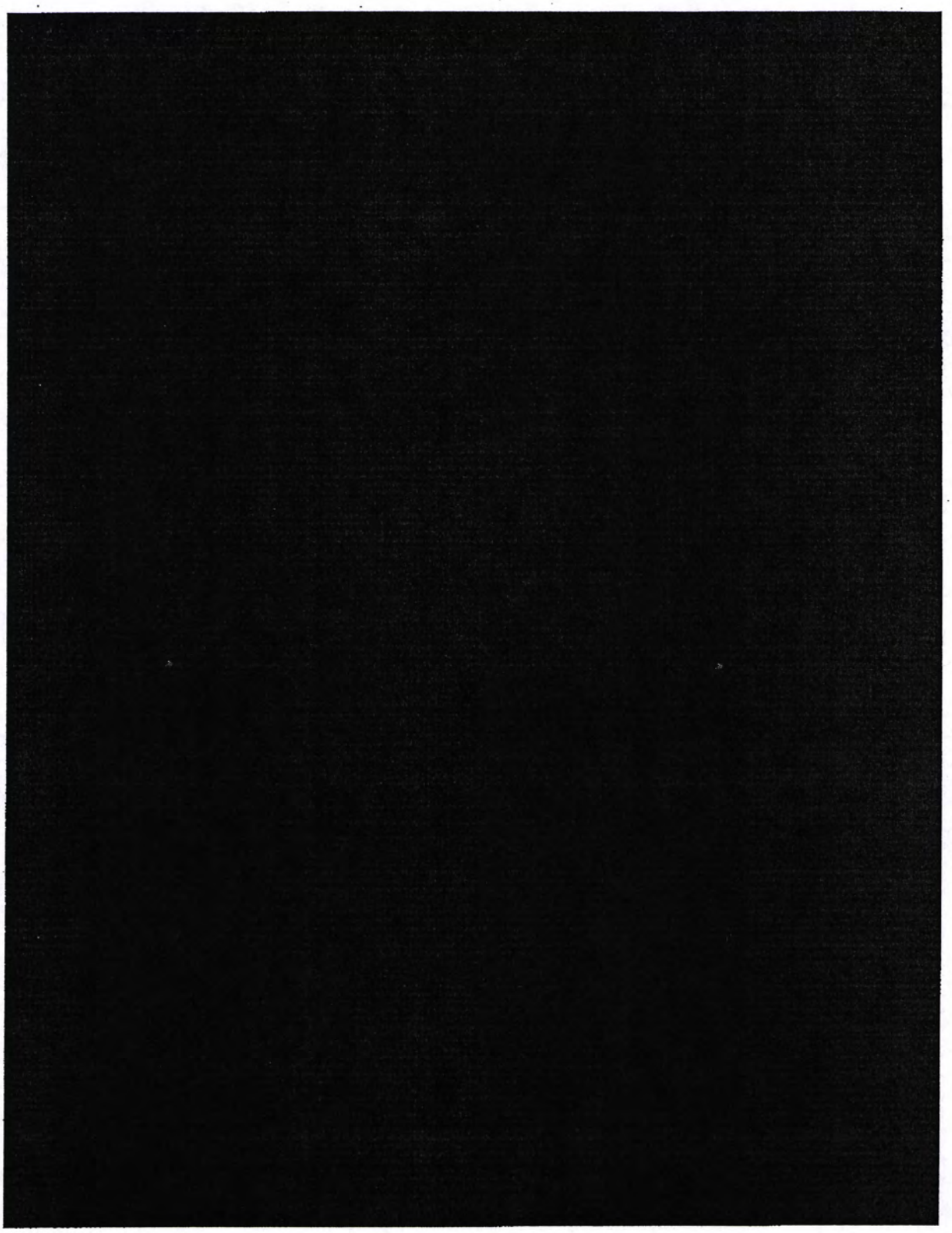


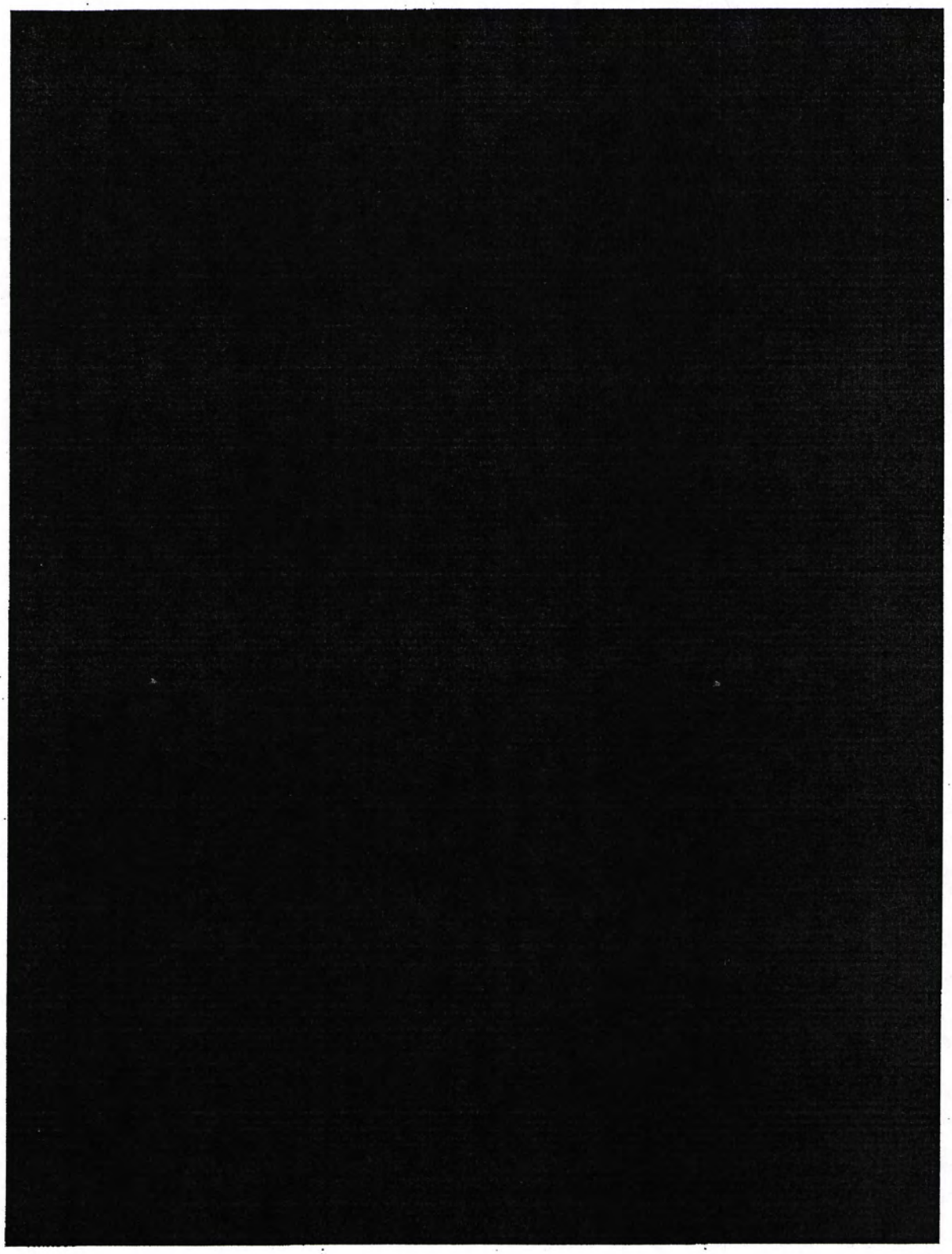


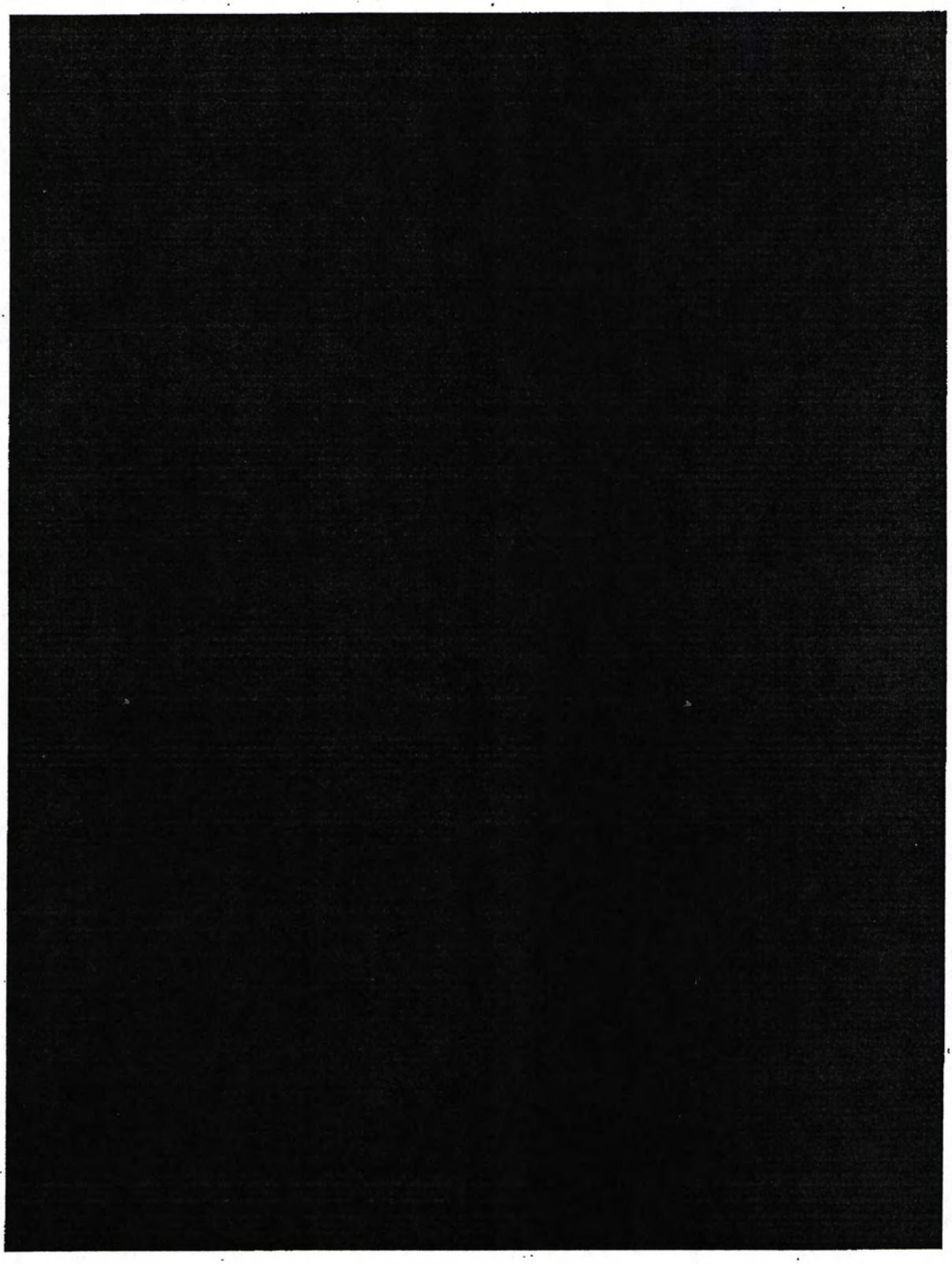


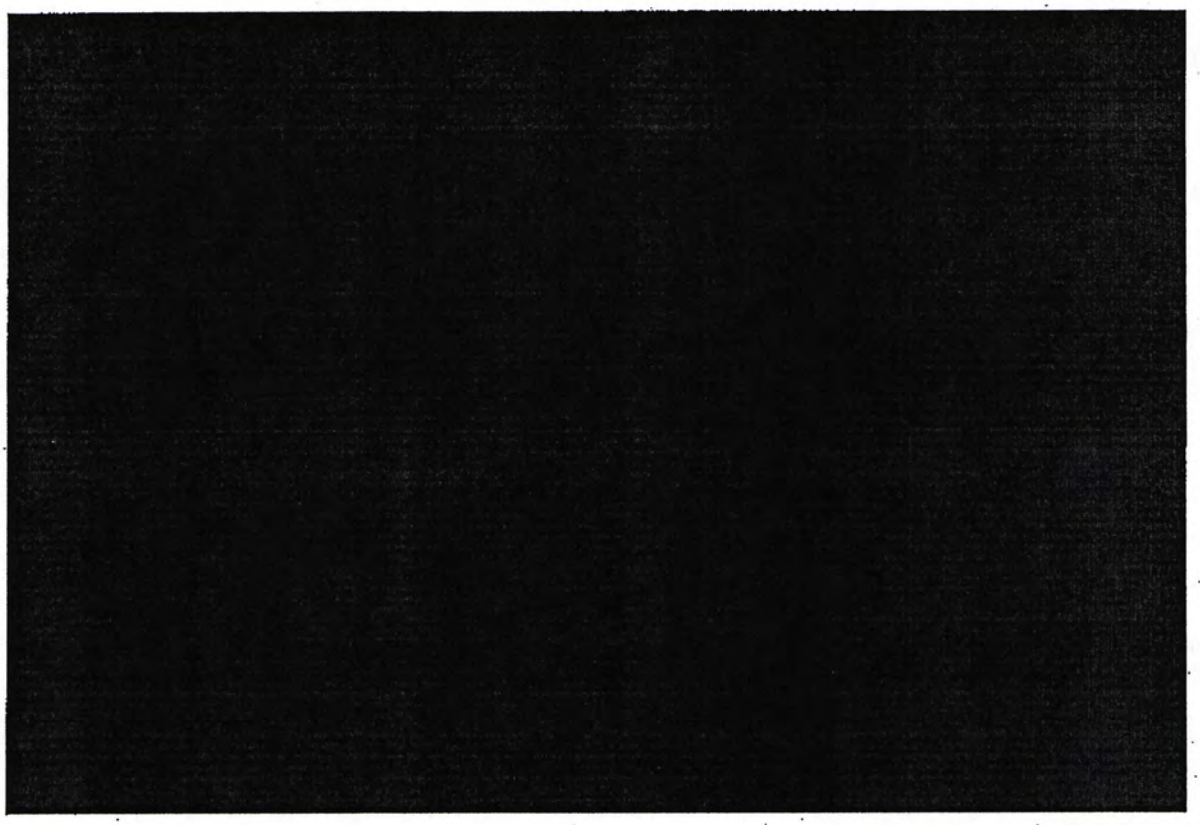
Therefore, having reviewed the [redacted] provided to the Court, the Court finds it includes information that is not relevant, cumulative, or to the extent relevant, not helpful to the defense. The Court finds it appropriate for the government to withhold the [redacted] from discovery.



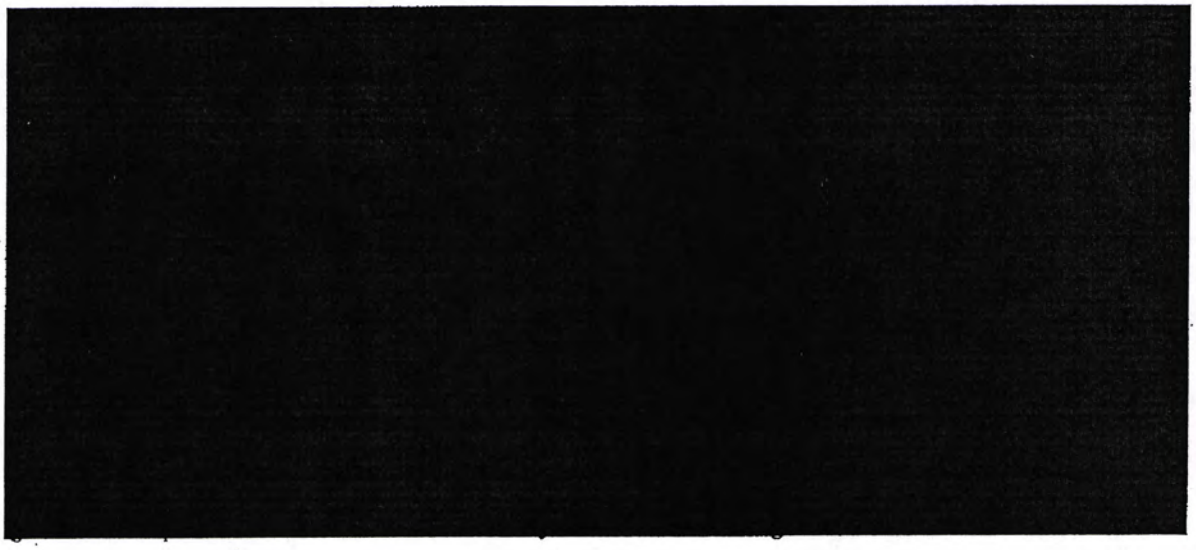








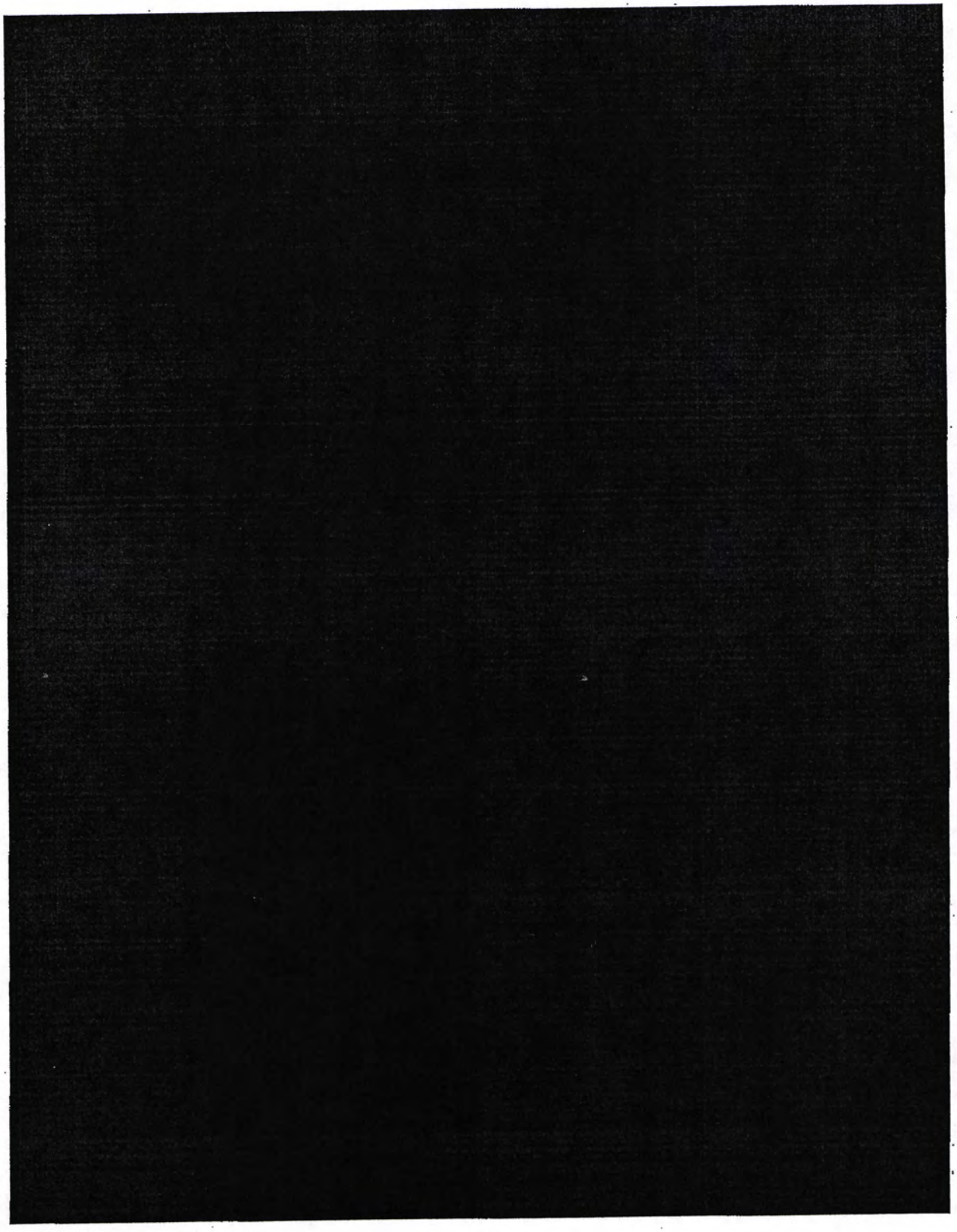
Having reviewed the government's representative samples of [redacted] obtained from [redacted], the Court finds the government may withhold these [redacted] from discovery.

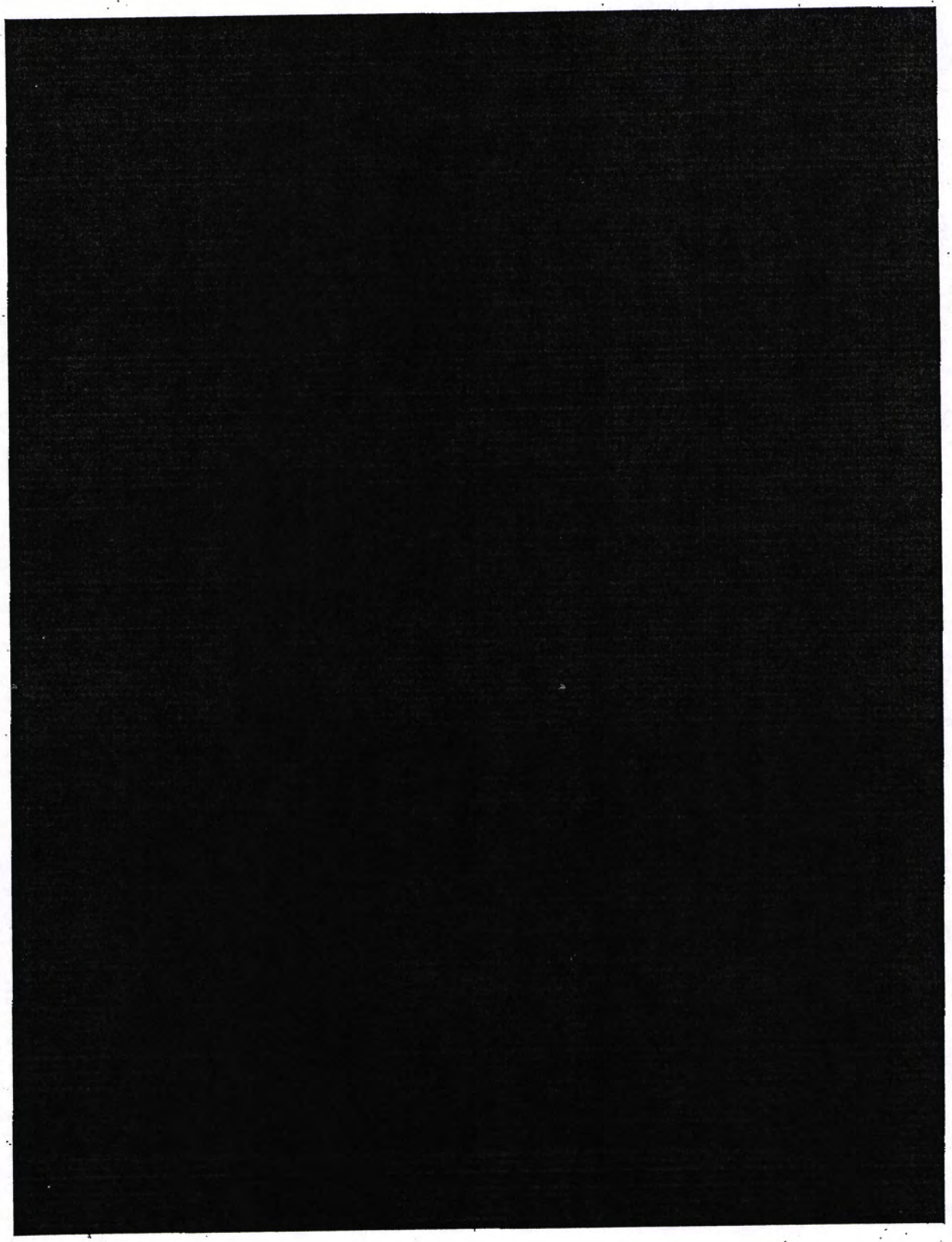


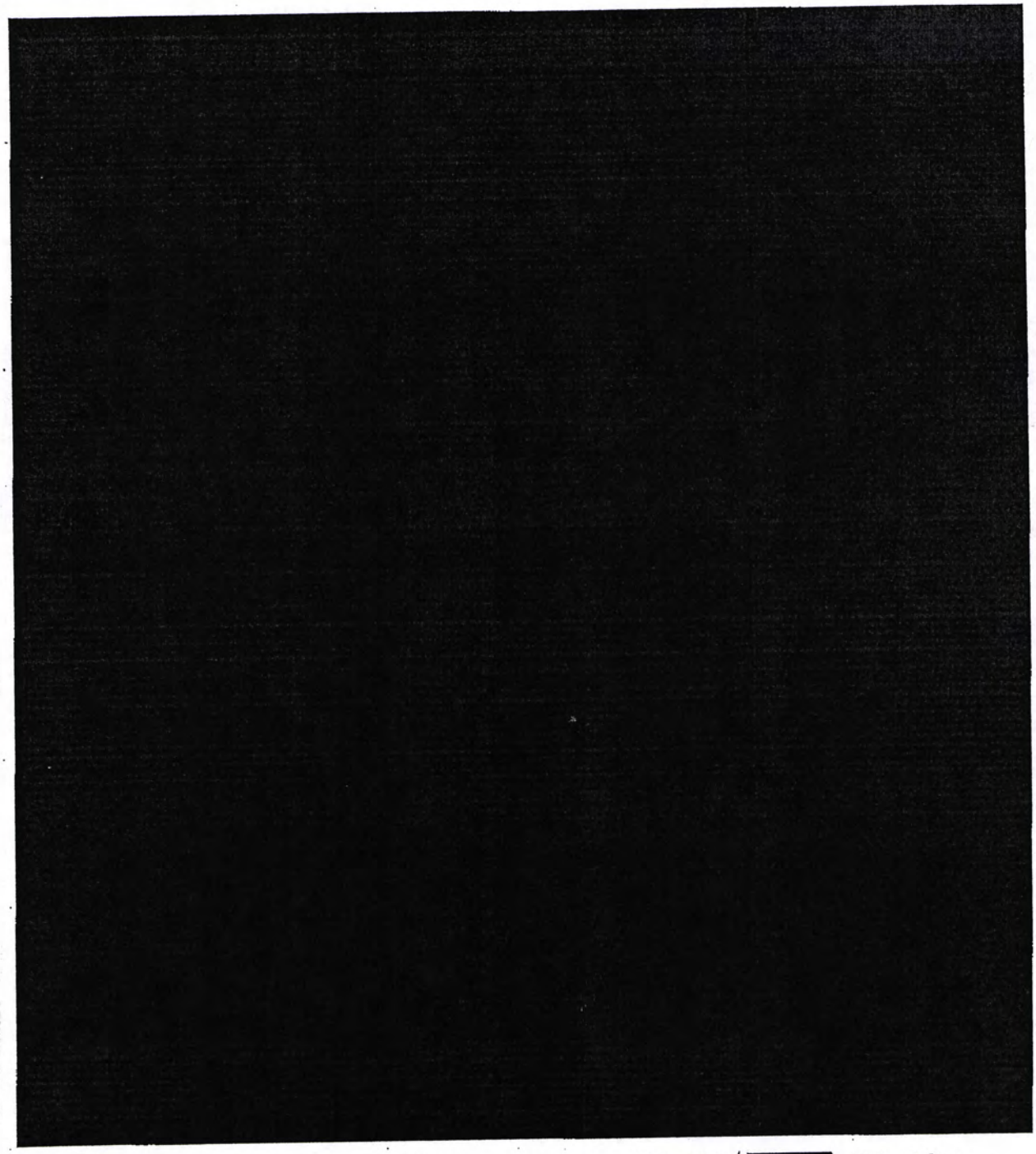
[redacted]

the Court finds it appropriate for the government to withhold [redacted] from discovery, finding that, [redacted] these [redacted] are not helpful to his defense.

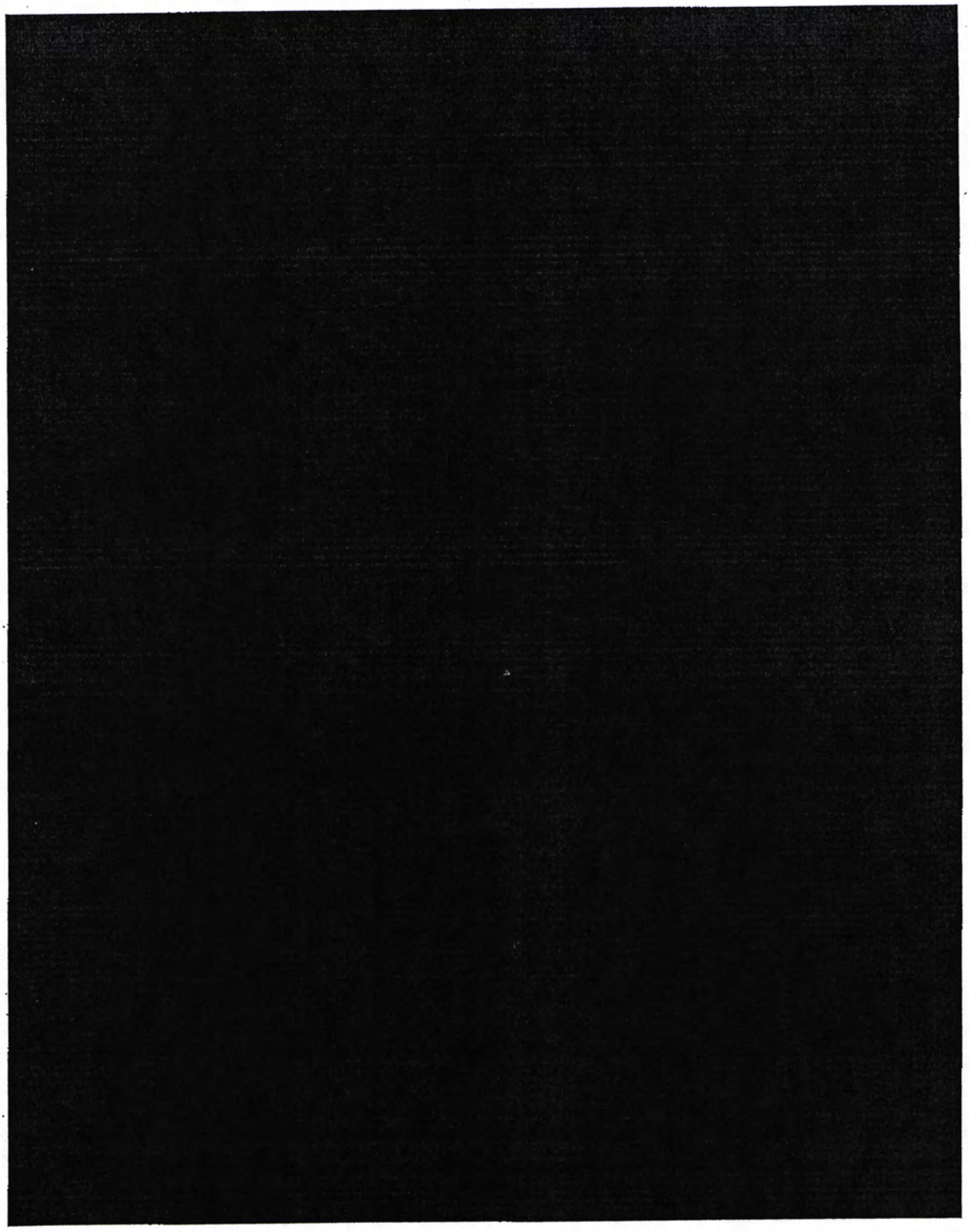
[redacted]

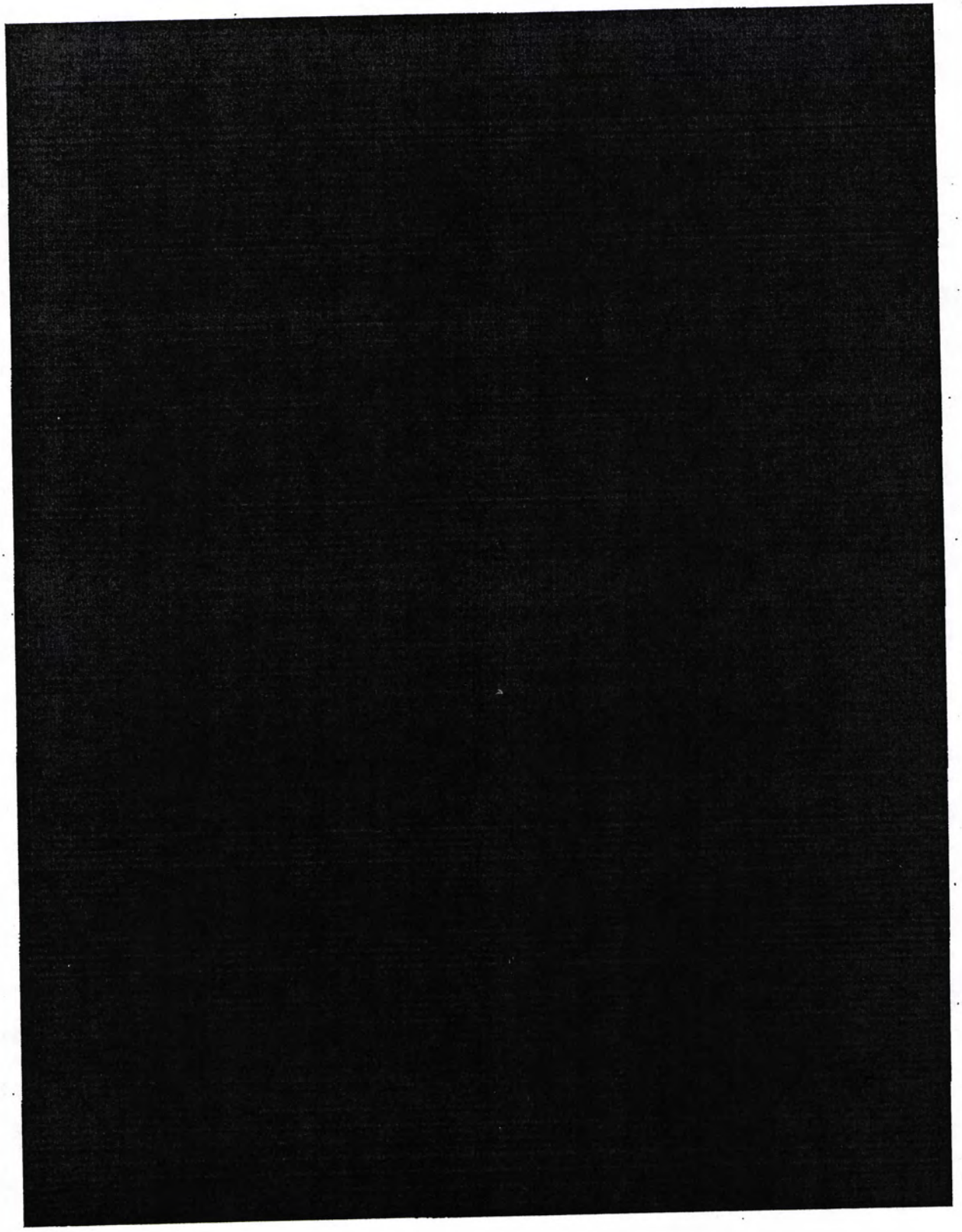


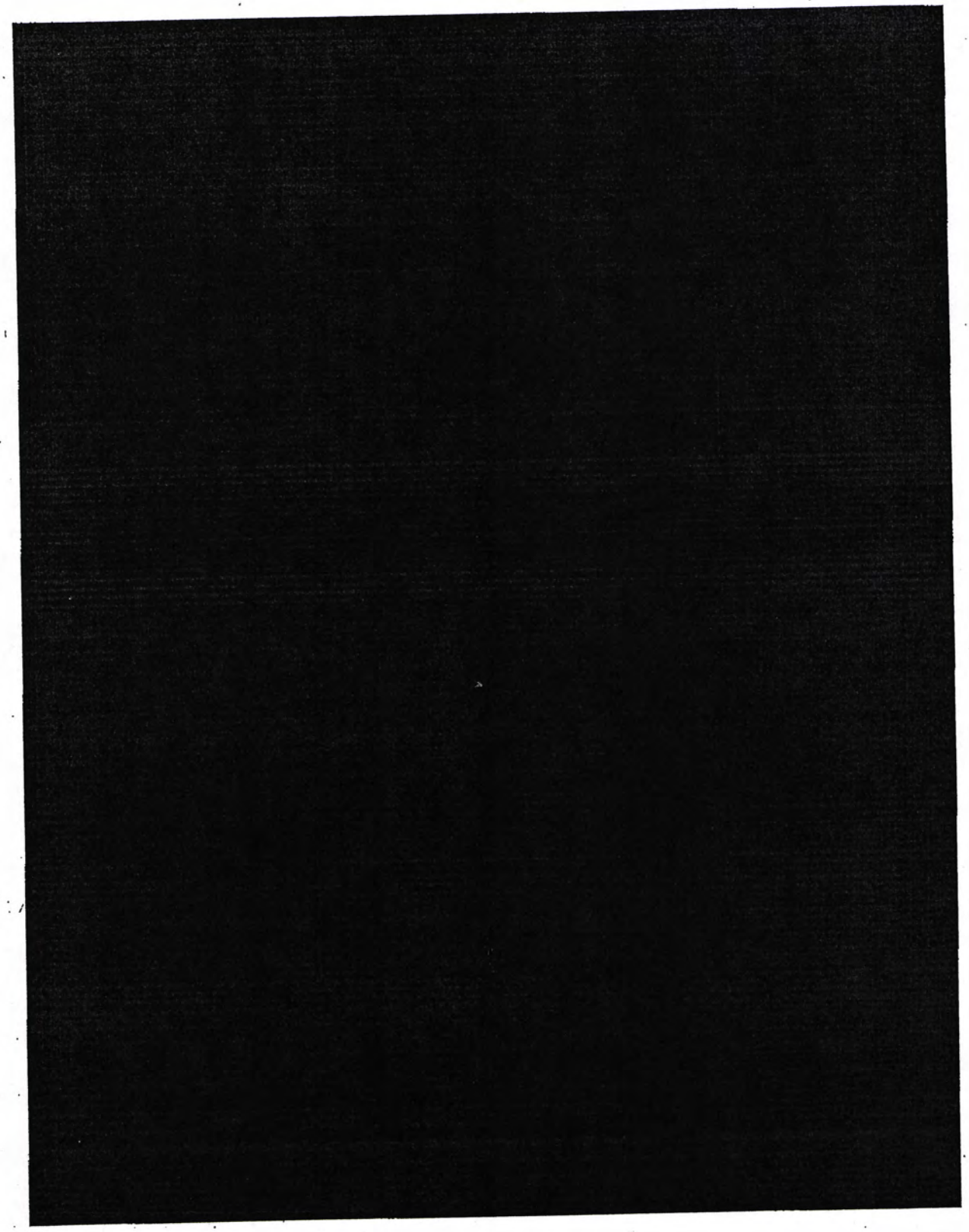




[redacted] Therefore, the Court agrees that the government may withhold the [redacted] obtained from [redacted]







II. FISA Section 702 [47]

Next, the Court considers al-Jayab's motion to suppress evidence obtained or derived from surveillance under FISA § 702, 50 U.S.C. § 1881a. Al-Jayab argues both that § 702 is unconstitutional and that the Court should suppress the § 702 acquisition in this case because it may have violated the statute. [redacted]

A. Statutory Overview

Before addressing al-Jayab's specific arguments, the Court provides a general overview of FISA and § 702. Under FISA, the FISA Court has jurisdiction to review *ex parte* applications for electronic surveillance "for the purpose of obtaining foreign intelligence information." 50 U.S.C. § 1802. To issue a FISA warrant, a FISA Court judge must determine that probable cause exists to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and "each of the 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." 50 U.S.C. § 1805(a)(2). FISA also requires minimization procedures to minimize the acquisition [redacted]

and retention, and prohibit the dissemination of, the communications of non-consenting United States persons. 50 U.S.C. §§ 1801(h); 1805(a)(3).

Under FISA as originally enacted, "electronic surveillance" encompassed only domestically-focused foreign intelligence surveillance, leaving extraterritorial surveillance outside of its purview. *See* 50 U.S.C. § 1801(f) (defining "electronic surveillance" as four types of surveillance involving the acquisition of the contents of communications of persons or devices "in the United States"). In 2007, Congress enacted the Protect America Act ("PAA") to address certain communication technology advances since FISA's enactment. The PAA allowed the Director of National Intelligence ("DNI") and the Attorney General to authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States." Pub. L. No. 110-55 § 105B(a), 121 Stat. 552 (2007). Among other things, the DNI and Attorney General had to certify that reasonable procedures existed to determine that the acquisition concerned individuals "reasonably believed to be located outside the United States," that minimization procedures satisfying FISA's requirements were in place, and that a "significant purpose" of the acquisition was to obtain foreign intelligence information. *Id.* § 105B(a)(1)-(5). The PAA expired on February 16, 2008. *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1007 (FISA Ct. Rev. 2008).

In July 2008, Congress enacted the FAA, which includes § 702, the provision al-Jayab challenges here.[29] Section 702 "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the [FISA Court's] authorization of certain

[29] The FAA includes a sunset provision. The President signed into law the FISA Amendments Reauthorization Act of 2017 on January 19, 2018, reauthorizing Title VII of FISA, which includes § 702, until December 31, 2023. To the extent the FISA Amendments Reauthorization Act made changes to the law, those changes do not affect this Court's analysis of actions that took place before those amendments went into effect.

foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S. Ct. 1138, 1144, 185 L. Ed. 2d 264 (2013). Upon the issuance of an order from the FISA Court, the DNI and Attorney General may jointly authorize, for up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). As with the PAA, certain limitations apply. Specifically, the acquisition:

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) may not intentionally target a person believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (4) may not intentionally acquire 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; and
>
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

50 U.S.C. § 1881a(b). "United States persons" includes "a citizen of the United States" and "an alien lawfully admitted for permanent residence." Al-Jayab acknowledges that he does not fall within the definition of a "United States person" ("U.S. person") under FISA.

Section 702 does not require the government to show probable cause that the target is a foreign power or agent of a foreign power, nor does the government have to specify the nature and location of the facilities or places where the electronic surveillance will take place. *Clapper*, 133 S. Ct. at 1144; *see* 50 U.S.C. § 1881a(d)(1), (g)(4), (i)(3)(A). Instead, the DNI and Attorney General present the FISA Court with annual certifications for the authorization of foreign

intelligence acquisition. 50 U.S.C. § 1881(i)(3). The certifications must include, among other things, information concerning proposed targeting and minimization procedures, and guidelines adopted to ensure compliance with the targeting limits and the Fourth Amendment. 50 U.S.C. § 1881a(g)(2). If the FISA Court finds that the certification meets the statutory requirements and concludes that the targeting and minimization procedures comport with the statute and the Fourth Amendment, the FISA Court issues an order authorizing the certification. 50 U.S.C. § 1881a(i)(3)(A).

The government undertakes two forms of § 702 collection: PRISM and upstream. The government represents that only PRISM collection is at issue in this case, and so the Court restricts its discussion to this form of collection here. PRISM involves the government sending certain selectors (*i.e.*, a "specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number") to United States-based electronic communications service providers for collection. Privacy & Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* ("PCLOB Report") at 32–33 (July 2, 2014), *available at* https://www.pclob.gov/library/702-report.pdf. A government directive compels service providers to provide the government with communications sent to or from that selector. *Id.* at 33.

The National Security Agency ("NSA") and FBI both conduct acquisitions under § 702, and each have separate targeting and minimization procedures. *Id.* at 42. The NSA takes the lead in making targeting determinations. *Id.* Once the NSA identifies a potential target, the NSA makes two determinations: (1) whether the potential target is a non-U.S. person reasonably believed to be located outside the United States (the "foreignness determination"); and

(2) whether the target has or is likely to have communications or receive foreign intelligence information that is authorized under an approved certification (the "foreign intelligence purpose determination"). *Id.* at 43. In making the foreignness determination, the NSA considers the totality of the circumstances and cannot rely solely on its initial information but must perform additional due diligence. *Id.* at 43–44. NSA analysts routinely review samples of acquired communications to ensure that the selectors remain associated with their foreign intelligence target and that the user remains a non-U.S. person located outside of the United States. *Id.* at 48. If a review shows otherwise, the selector must be detasked and, if the selector was being used by a U.S. person or a person located in the United States, the information acquired from that selector is subject to deletion. *Id.* at 49.

Once the government agency acquires information, the NSA and/or FBI employ minimization procedures to minimize the acquisition of information concerning U.S. persons consistent with the need to obtain foreign intelligence information. 50 U.S.C. §§ 1801(h), 1881a(e)(1). These procedures limit, for example, the types of queries that can be conducted on the acquired information and who has access to the § 702 acquired data. PCLOB Report at 50–66.

Where a defendant files a motion to suppress § 702 information and in response the Attorney General files an affidavit stating that disclosure of the materials or an adversary hearing relating to the § 702 surveillance would harm the national security of the United States, the Court conducts an *in camera* and *ex parte* review of those materials to determine whether the surveillance was lawfully authorized and conducted. 50 U.S.C. §§ 1806(f), 1825(g). After undertaking this review, the Court may order disclosure of the materials to the defense only

where "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f).

B. Al-Jayab's Arguments Challenging § 702's Constitutionality

Although al-Jayab appears to make a broad facial challenge to § 702's constitutionality, the Court treats al-Jayab's arguments as an as applied challenge limited to how the government implemented the statute in his specific case as opposed to considering whether no circumstances exist under which the Court could find § 702 valid. *See United States v. Hasbajrami*, No. 11-CR-623(JG), 2016 WL 1029500, at *7 (E.D.N.Y. Mar. 8, 2016) (collecting cases declining to consider facial challenges to § 702 collections). Thus, the Court declines to consider or address al-Jayab's broader arguments concerning the alleged impropriety of upstream collection or other aspects of § 702 not applicable to this case.

Al-Jayab argues that § 702 violates the Fourth Amendment and so the Court must suppress all evidence derived from the § 702 collection in his case. Specifically, al-Jayab contends that § 702 is unconstitutional because it (1) violates the Fourth Amendment's warrant clause; (2) allows surveillance and interception without probable cause, particularity, and specification; (3) authorizes unreasonable surveillance; and (4) requires the FISA Court to participate in the construction of the surveillance program, blurring the separation of the judiciary and executive branches and rendering the FISA Court's opinions advisory. The Court considers these arguments in turn.

1. Warrant Clause

The Fourth Amendment provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. But the warrant clause does not apply in

all cases and "does not apply to searches and seizures by the United States against a non-resident alien in a foreign country." *United States v. Zakharov*, 468 F.3d 1171, 1179 (9th Cir. 2006) (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75, 110 S. Ct. 1056, 108 L. Ed. 2d 222 (1990)). [redacted] *See United States v. Mohamud* (*Mohamud II*), 843 F.3d 420, 439 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 636 (2018). [redacted] the government did not need to obtain a warrant.[30] *Id.* [redacted] *See In re Directives*, 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."); *Hasbajrami*, 2016 WL 1029500, at *9 ("[W]hen the surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful." (footnote omitted)). Although al-Jayab contends that the collection of his communications should be considered intentional and

[30] The fact that the collection may have occurred on United States soil does not matter, as the concern is the location of the target, not where the collection is made. *See Hasbajrami*, 2016 WL 1029500, at *9 n.15 ("The government concedes that information-gathering under Section 702 takes place within the United States. But what matters here is the location of the *target*. The mere fact that Section 702 surveillance originated from within the United States, or that the communications obtained through such surveillance originated from or terminated within the United States, is not enough to trigger the warrant requirement." (citations omitted)); *United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir. 1983) (noting that "the Fourth Amendment protects people, not places," meaning that the location of the recording equipment makes no difference in the Fourth Amendment analysis (quoting *Katz v. United States*, 389 U.S. 347, 351, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967))).

targeted and not incidental, particularly considering the volume of the incidental collection of communications of U.S. persons or persons in the United States under § 702, these arguments play into the reasonableness determination and not into whether the government needed a warrant to make the collection lawful. *See Mohamud II*, 843 F.3d at 440 (finding that the government did not need to obtain a search warrant for incidental collection, noting that "the mere fact that more communications are being collected does not make it unconstitutional to apply the same approach [of Title III and traditional FISA interceptions] to § 702 collection, though it does increase the importance of minimization procedures once the communications are collected").

2. Probable Cause, Particularity, and Specification Requirements

Al-Jayab also argues that § 702 violates the Fourth Amendment because it does not require a determination of probable cause or particularity and specification and instead allows for the approval of broad programs and procedures without specific targets. But because the government did not need to obtain a warrant for the surveillance at issue, the probable cause, particularity, and specification requirements do not come into play. *See Hasbajrami*, 2016 WL 1029500, at *8, 9 n.16 (because warrant requirement did not apply, probable cause, particularity, and specification requirements also were not applicable). Therefore, § 702 is not rendered unconstitutional because it does not require a determination of probable cause or that warrants be issued with particularity and specificity before undertaking § 702 surveillance.

3. Foreign Intelligence Exception

Alternatively, the government argues that a foreign intelligence exception applies to the warrant and probable cause requirements, analogizing to cases where courts have allowed exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the

normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873, 107 S. Ct. 3164, 97 L. Ed. 2d 709 (1987) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 351, 105 S. Ct. 733, 83 L. Ed. 2d 720 (1985) (Blackmun, J., concurring in judgment)); *see, e.g.*, *United States v. Duka*, 671 F.3d 329, 341 (3d Cir. 2011) (collecting cases that "have examined the Fourth Amendment's application to electronic surveillance conducted under the guise of the President's executive authority to collect foreign intelligence information," which have "almost uniformly concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of 'foreign intelligence exception' to the Fourth Amendment's warrant requirement"); *In re Directives*, 551 F.3d at 1012 ("[W]e hold 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."). Al-Jayab contends that the foreign intelligence exception applies narrowly and cannot be extended to § 702 because it only applies where the surveillance in question is directed at a specific foreign agent or foreign power, with the primary purpose of the surveillance to gather foreign intelligence information, and the surveillance has been personally approved by the President or Attorney General. *See United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000) (limiting foreign intelligence exception). According to al-Jayab, § 702 meets none of these requirements because it operates on a much larger scale and allows the government to engage in warrantless surveillance to gather evidence of criminal activity without requiring that its targets be identified foreign powers and agents.

The Court need not reach the foreign intelligence exception, having found that § 702 does not violate the warrant and probable cause requirements. But even so, it would be more inclined to follow those cases that have recognized the applicability of the foreign intelligence exception to § 702 collections. *See United States v. Mohamud* (*Mohamud I*), No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *17–18 (D. Or. June 24, 2014); *[Caption Redacted]*, 2011 WL 10945618, at *24 (FISA Ct. Oct. 3, 2011); *In re Directives*, 551 F.3d at 1012.[31] Section 702 requires that a "significant purpose" of the acquisition consist of obtaining foreign intelligence information, 50 U.S.C. § 1881a(g)(2)(v), which goes beyond "ordinary criminal-law enforcement purposes," *In re Directives*, 551 F.3d at 1011 (noting that, under the PAA, § 702's predecessor, the "prevention or apprehension of terrorism suspects . . . is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection," and that there "is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes"); *see also [Caption Redacted]*, 2011 WL 10945618, at *24 (noting that the collection as a whole under § 702, even with the understanding that "as a result of the transactional nature of the upstream collection, NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood," was still conducted for the purpose of national security). Additionally, "there is 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." *In re Directives*, 551 F.3d at 1011; *see also Mohamud I*, 2014 WL 2866749, at *18 (finding that "[t]he government's need for speed and stealth have not lessened" since the

[31] Although *In re Directives* addressed the PAA, the precursor of § 702, the Court finds its analysis equally applicable to § 702.

FISA Court approved of the foreign intelligence exception's application to § 702 surveillance). Finally, although certain cases, such as the *Bin Laden* case cited by al-Jayab, have required that the foreign intelligence surveillance be directed at a foreign power or agent, *see* 126 F. Supp. 2d at 277, the foreign intelligence exception appears suited to § 702, which, although it does not include a foreign power or agent requirement, 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. This limitation on § 702's targets curtails the bounds of the exception, particularly where these targets are otherwise unprotected by the Fourth Amendment. And while the Attorney General does not personally approve each acquisition under Section 702, the Attorney General and DNI must jointly authorize each broader collection, *see* 50 U.S.C. § 1881a(a), which provides some oversight over the process. Therefore, to the extent the Court's conclusion that § 702 meets the warrant and probable cause requirements proves incorrect, the Court would find that the foreign intelligence exception applies.

4. Reasonableness

Al-Jayab argues that even if the government does not need a warrant to engage in § 702 collection, the Court should find the § 702 collection at issue unreasonable under the Fourth Amendment. *See Maryland v. King*, --- U.S. ----, 133 S. Ct. 1958, 1970, 186 L. Ed. 2d 1 (2013) ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution."); *see also United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1253–54 (D. Colo. 2015) (declining to decide whether foreign intelligence exception applied to § 702 surveillance where "the standard ultimately is one of reasonableness"); *In re Directives*, 551 F.3d at 1012 (noting that even with a foreign intelligence exception, "governmental action intruding on individual privacy interests must comport with the

Fourth Amendment's reasonableness requirement"). In assessing reasonableness, the Court weighs "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Id.* (alteration in original) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300, 119 S. Ct. 1297, 143 L. Ed. 2d 408 (1999)).

a. Government's Interest

The government's national security interest in acquiring foreign intelligence information is "of the highest order of magnitude." *In re Directives*, 551 F.3d at 1012 (addressing governmental interest under the PAA); *see also Holder v. Humanitarian Law Project*, 561 U.S. 1, 28, 130 S. Ct. 2705, 177 L. Ed. 2d 355 (2010) ("Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order."). Additionally, "[t]he government's interest in using intelligence information to detect and prevent criminal acts of terrorism, and ultimately to punish their perpetrators, is a legitimate governmental interest." *Muhtorov*, 187 F. Supp. 3d at 1256.

b. Al-Jayab's Privacy Interest

Al-Jayab does not spend much time addressing his interest in the privacy of his communications, instead focusing generally on the unreasonable nature of § 702 surveillance. As other courts addressing the issue have recognized, however, individuals have a diminished expectation of privacy in communications sent to others, particularly over the internet, and assume the risk that the recipients will share the communications with others.[32] *See Mohamud*

[redacted]

II, 843 F.3d at 442; *Hasbajrami*, 2016 WL 1029500, at *10–11; *Muhtorov*, 187 F. Supp. 2d at 1255. This includes not only physical letters but also email and other communications over the internet.[33] *See United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) ("A person's reasonable expectation of privacy may be diminished in 'transmissions over the Internet or e-mail that have already arrived at the recipient.'" (quoting *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004))); *[Caption Redacted]*, 2011 WL 10945618, at *26 ("Whether they are transmitted by letter, telephone or e-mail, a person's private communications are akin to personal papers."). But at the same time, "this diminished expectation of privacy in email communications does not mean the government can search every email with impunity just because the email sender communicated with a foreign person abroad." *Hasbajrami*, 2016 WL 1029500, at *10; *see also Muhtorov*, 187 F. Supp. 2d at 1255 (refusing to adopt government's view that defendants have diminished expectations of privacy in communications with non-U.S. persons "based simply on the fact that those persons could be targets for surveillance," but

[redacted]

[33] The Supreme Court recently declined to extend this third-party principle to cell phone location records in *Carpenter v. United States*, No. 16-402, slip op. at 11 (June 22, 2018) ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]."). [redacted] Additionally, the Supreme Court made clear that its *Carpenter* decision was a "narrow one" and "does not consider other collection techniques involving foreign affairs or national security." *Id.*, slip op. at 17–18. Thus, *Carpenter* does not affect this Court's analysis.

finding that "expectations of privacy are diminished the more information one puts out into the ether, especially the ether of the global telecommunications network").

c. Balancing the Interests

Al-Jayab argues that § 702 does not adequately protect his privacy interests because it abandons the "core requirements of the warrant clause—individualized suspicion, prior judicial review, and particularity" and thus "eliminates the primary protections against general surveillance." Doc. 48 at 46. He compares the protections provided by FISA and Title III to those in § 702 and argues that § 702 is unreasonable because it does not include the basic safeguards incorporated into FISA and Title III, such as identification of targets, demonstration of individualized suspicion to a court, and imposition of strict limits on the communications that may be monitored and the duration of surveillance. Al-Jayab argues that the government's targeting and minimization procedures under § 702 are defective because they do not meaningfully constrain the selection of foreign targets and do not impose an affirmative obligation to identify and purge U.S. persons' communications once obtained, meaning that the government has monitored countless U.S. persons' communications without a warrant. Al-Jayab also argues that § 702 is unreasonable because the FISA Court does not have authority to supervise the intelligence agencies' compliance with minimization procedures during the course of acquisitions and agencies need not seek judicial approval before analyzing, retaining, or disseminating domestic communications.

The government responds that § 702's targeting and minimization procedures sufficiently ensure that collections are appropriately targeted at non-U.S. persons located outside the United States for foreign intelligence purposes and that the privacy interests of individuals located in the United States whose communications are incidentally collected are protected. The government

takes issue with al-Jayab's characterization of § 702 collection as "dragnet" or "bulk" surveillance, contending instead that, although the general certifications do not include specific targets, each specific collection is aimed at a particular target after an individualized determination is made using the targeting procedures. *See* PCLOB Report at 111 ("[T]he Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made."); *August 26, 2014 FISA Ct. Op.*, slip. op. at 26 ("While in absolute terms, the scope of acquisitions under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner. Rather, they are effected through [redacted] discrete targeting decisions for individual facilities.").

The § 702 application in this case included the required certification and accompanying documents, which detail the targeting and minimization procedures in place to protect the privacy of both U.S. and non-U.S. persons located in the United States. *See* Sealed Exs. 13–22; 50 U.S.C. § 1881a(a), (g), (i). The FISA Court reviewed the certification and approved it, finding that it met the statutory requirements and was consistent with the Fourth Amendment. *See* Sealed Ex. 27. This approval process by the FISA Court is not just a rubber stamp; the FISA Court subjects the proposed procedures to scrutiny and considers prior implementation in coming to its conclusions. *Cf. [Caption Redacted]*, 2011 WL 10945618, at *23–28 (finding that targeting and minimization procedures proposed did not satisfy the Fourth Amendment's requirements as applied to upstream collection including multi-communication transactions). The Attorney General and DNI must also periodically submit assessments of the government's compliance with the approved minimization and targeting procedures to both the FISA Court and congressional oversight committees. 50 U.S.C. § 1881(a)(l). This oversight, although not the

same as that in the traditional FISA context, does support finding that the § 702 surveillance here was reasonable. *See Clapper*, 133 S. Ct. at 1144 ("Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment."); *Hasbajrami*, 2016 WL 1029500, at *11 (finding that oversight provided by FISA Court, executive branch, and Congress worked together to safeguard the Fourth Amendment). *But see Mohamud II*, 843 F.3d at 443–44 (noting that "where the only judicial review comes in the form of the FISC reviewing the adequacy of procedures, this type of internal oversight does not provide a robust safeguard").

Although al-Jayab complains that § 702 lacks a particularity requirement, the Court does not find this fatal. *See [Caption Redacted]*, 2011 WL 10945618, at *6 (targeting and minimization procedures for to/from communications comply with § 702 and the Fourth Amendment). Generally, § 702's targeting procedures ensure that, with each target, the government assesses whether the potential target is a non-U.S. person and possesses and/or is likely to communicate or receive foreign intelligence information. *See* PCLOB Report at 41–42; Sealed Exs. 18, 20. [redacted] The use of such "'[s]trong selectors, such as email addresses, weed out innocent or inadvertent communications '[b]ecause of the small set of people with knowledge of the email address or phone number of a subject of foreign intelligence interest.'" *Hasbajrami*, 2016 WL 1029500, at *12 (second alteration in original) (quoting Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection after Snowden*, 66 Hastings L.J. 1, 47 (Dec. 2014)). Consequently,

the Court cannot find the government's use of the targeting procedures unreasonable in this instance.

Section 702's minimization procedures also "serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons." *In re Directives*, 551 F.3d at 1015. But al-Jayab contends that the minimization procedures are not adequate because the FISA Court does not supervise compliance and agencies need not seek judicial approval before searching the collected communications of U.S. persons or persons living in the United States, allowing for expansive "backdoor searches" of this information that invade individuals' privacy interests. Section 702 requires regular reports to the FISA Court concerning implementation of the minimization procedures, 50 U.S.C. § 1881(l), and the government must also report all instances of non-compliance to the FISA Court, *see* FISA Court R. 13(b).[34] The FISA Court also may take proactive action in instances of noncompliance, such as "seek additional information, issue orders to the government to take specific action to address an incident of noncompliance, or (if deemed necessary) issue[ ] orders to the government to cease an action that the court assesses to be non-compliant." PCLOB Report at 76.

Al-Jayab also argues that the government's ability to conduct "backdoor searches" (*i.e.*, the querying of already collected information pursuant to § 702 for law enforcement purposes) makes § 702 unreasonable. [redacted]

[34] Although al-Jayab highlights instances of non-compliance with minimization procedures as reasons to find § 702 surveillance unreasonable, reasonableness does not demand "perfection," and so "[g]iven the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made." *November 6, 2015 FISA Ct. Op.*, slip op. at 45–46; *see also In re Directives*, 551 F.3d at 1016 (finding surveillance at issue satisfied reasonableness requirement where "the risks of error and abuse are within acceptable limits and effective minimization procedures are in place").

[redacted] *See Mohamud II*, 843 F.3d at 438, 440 n.24 (refusing to address querying of incidentally collected information, where case involved only the targeting of a foreign national, through which defendant's communications were incidentally collected). [redacted] Because al-Jayab was not aggrieved by any backdoor searches, the Court need not consider the issue further.

Going a step further, however, § 702's minimization procedures generally sufficiently protect against unbridled searches of the communications of U.S. persons and individuals located in the United States. *See November 6, 2015 FISA Ct. Op.*, slip op. at 39–45 (addressing FBI's minimization procedures allowing use of U.S. person information to query § 702 acquired information to find evidence of crimes unrelated to foreign intelligence and finding the minimization procedures "strike a reasonable balance" between the government's national security interests and individuals' privacy interests, making the procedures reasonable under the Fourth Amendment); *[Caption Redacted]*, 2011 WL 10945618, at *7 (approving querying provision allowing for searches using U.S. person identifiers, noting that FISA Court has approved similar applications for information acquired under Titles I and III of FISA, and that the NSA's minimization procedures for § 702 collection "should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons"). Moreover, "[a]ccessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information," so no warrant is needed. *Muhtorov*, 187

F. Supp. 3d at 1256; *Mohamud I*, 2014 WL 2866749, at *26 ("[S]ubsequent querying of a § 702 collection, even if U.S. identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment."). The government must review information collected pursuant to § 702, including that concerning U.S. persons or those located in the United States, to determine whether to retain or disseminate it under its minimization procedures. The additional intrusion upon an individual's privacy in searching that information using a U.S. person identifier is not significant and, in light of the minimization procedures already in place, does not render § 702 unreasonable. *See Hasbajrami*, 2016 WL 1029500, at *12 n.20; *Mohamud I*, 2014 WL 2866749, at *26.

Having examined the totality of the circumstances, and in light of the protections provided by § 702's targeting and minimization procedures, the Court concludes that the government's interest in protecting national security outweighs the intrusion into [redacted] The Court therefore finds [redacted] as applied to al-Jayab, reasonable under the Fourth Amendment.

5. Separation of Powers

Finally, al-Jayab argues that § 702 is unconstitutional because the FISA Court does not issue a warrant based on probable cause but rather authorizes and certifies general procedures, which means it essentially renders advisory opinions on whether the proposed targeting and minimization procedures comply with the statute and Constitution instead of looking at particularized facts or context. *See Chafin v. Chafin*, 568 U.S. 165, 172, 133 S. Ct. 1017, 185 L. Ed. 2d 1 (2013) ("Federal courts may not . . . give 'opinion[s] advising what the law would be upon a hypothetical state of facts.'" (alteration in original) (quoting *Lewis v. Cont'l Bank Corp.*, 494 U.S. 472, 477, 110 S. Ct. 1249, 108 L. Ed. 2d 400 (1990))). According to al-Jayab, when

the FISA Court considers § 702 requests, it does not function as the neutral and detached judge required by the Fourth Amendment. *See Steagald v. United States*, 451 U.S. 204, 212, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981) (noting that "[t]he purpose of a warrant is to allow a neutral judicial officer to assess whether the police have probable cause to make an arrest or conduct a search," with the judge acting as a "checkpoint between the Government and the citizen").

But courts faced with this argument have rejected it, and this Court sees no reason to deviate from those rulings. *See Mohamud I*, 2014 WL 2866749, *aff'd*, *Mohamud II*, 843 F.3d 420; *Muhtorov*, 187 F. Supp. 3d 1240. In *Mohamud I*, the district court rejected the idea that the FISA Court only provides advisory opinions or assists in designing § 702 procedures, concluding that the FISA Court's "review of § 702 surveillance submissions provides prior review by a neutral and detached magistrate." 2014 WL 2866749, at *11. The Ninth Circuit agreed that § 702 survived separation of powers and non-delegation challenges, finding that the FISA Court's review of the surveillance applications was "similar to the review of search warrants and wiretap applications" and was not advisory because the FISA Court either approved or denied the applications. *Mohamud II*, 843 F.3d at 444 n.28. In *Muhtorov*, although the court took a different view from *Mohamud* in finding that the FISA Court's "role in approving the surveilling of individual foreign powers or agents under traditional FISA is qualitatively different from its role in approving the surveillance and incidental acquisition of strangers' communications under the FAA," the court nonetheless found that for purposes of the case before it, that role did not offend Article III so as to invalidate § 702 as a foreign intelligence gathering tool. 187 F. Supp. 3d at 1251–52. The Court similarly finds that, although differences do exist between traditional warrant applications and those made under § 702 to the FISA Court, the role played by the FISA Court in approving § 702 applications does not improperly blur constitutional separation of

powers so as to render § 702 unconstitutional. Therefore, the Court finds that § 702 is constitutional as applied to al-Jayab.[35]

C. Acquisition of § 702 Materials in this Case

Having concluded that § 702 is constitutional as applied to al-Jayab, the Court must still consider whether the government lawfully acquired the § 702 information in this case and conducted the acquisitions in conformity with the orders of authorization. Al-Jayab briefly raises this issue, arguing that the acquisition may have violated the statute by, for example, intentionally targeting a person known at the time of acquisition to be located in the United States or a U.S. person believed to be outside the United States, that the acquisition was not made pursuant to the necessary certifications, or that the targeting and minimization procedures did not comply with 50 U.S.C. § 1881a(d) and (e). Although undeveloped, the Court finds these bases unfounded. Instead, based on its *in camera* and *ex parte* review of the § 702 materials, the Court concludes that the § 702 acquisition in this case was lawfully authorized and conducted, as set forth below. [redacted]

1. Section 702 Authorizations and Procedures

a. Certification

[redacted] The Attorney General and the DNI made

[35] Because the Court concludes that § 702 passes constitutional muster, it need not consider the government's argument that the good faith exception to the exclusionary rule provides an independent basis for denying al-Jayab's motion to suppress.

the certification under oath, and it was accompanied by the applicable targeting and minimization procedures and supported by the required affidavits. *See* 50 U.S.C. § 1881a(g);

[redacted] And the FISA Court found that the amended minimization procedures complied with the requirements of both § 702 and the Fourth Amendment. *Id.* Similarly, the Court's review of the certification and amended submissions indicates that they complied with all statutory and constitutional requirements.

b. Targeting and Minimization Procedures

The Court next examines the targeting and minimization procedures to ensure they complied with the statutory requirements. The pertinent targeting and minimization procedures here are: [redacted] Although these procedures differ in some ways from the current procedures in place, the government represents that the differences are not relevant.

To comply with the statute, targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized [by § 702] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of

[redacted]

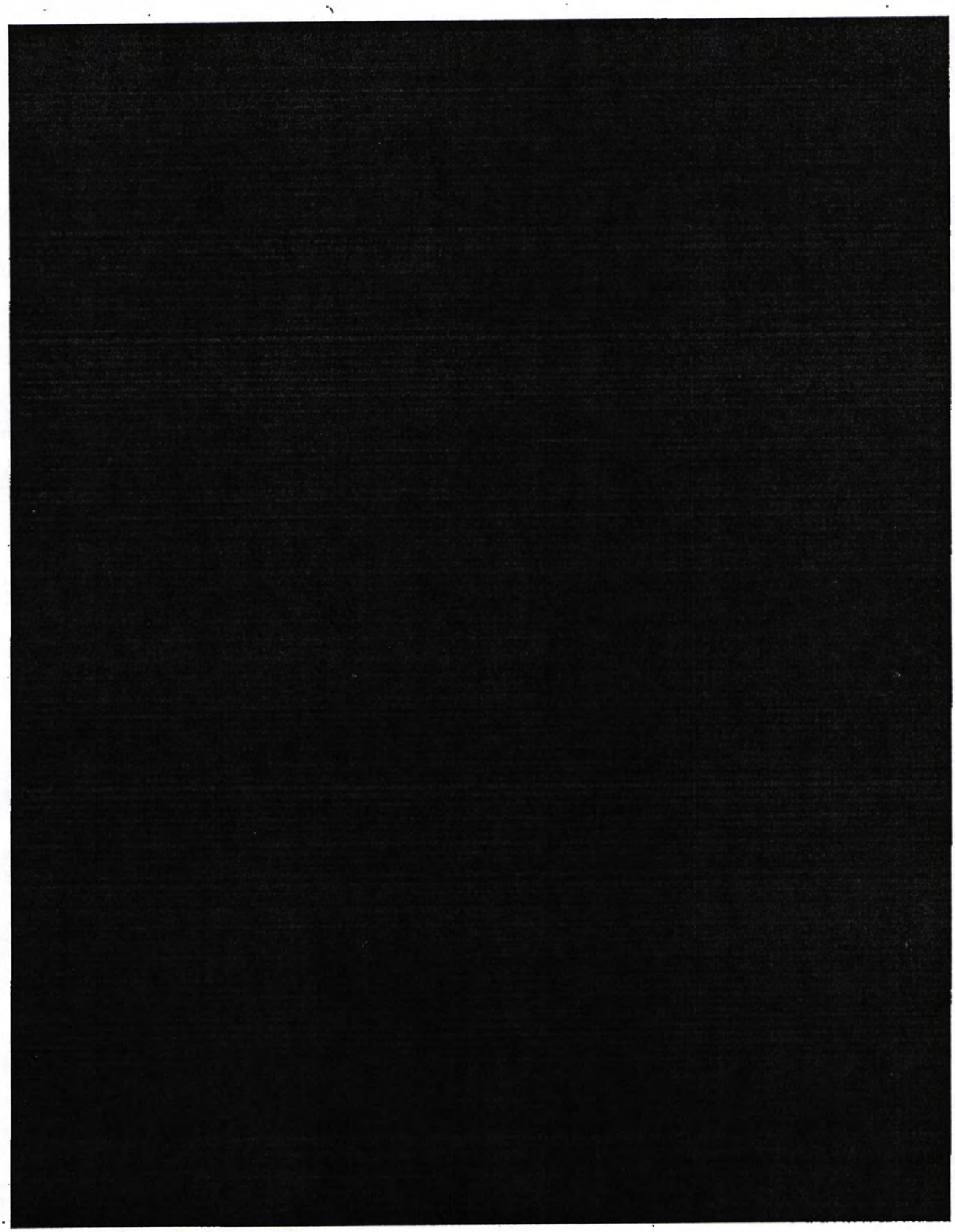
the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). The NSA's targeting procedures require NSA analysts to examine the totality of the circumstances in determining whether an individual is a non-U.S. person reasonably believed to be located outside the United States, searching lead information, NSA databases and other available information, and conducting technical analyses of the facilities at issue to determine or verify the information about the person's location. A target is tasked only after internal approval. Various checks are built into the tasking determination, both pre- and post-targeting, to ensure that a person has not entered the United States since targeting and prevent the targeting of individuals within the United States. Like the FISA Court, the Court finds these targeting procedures satisfy the statutory requirements.

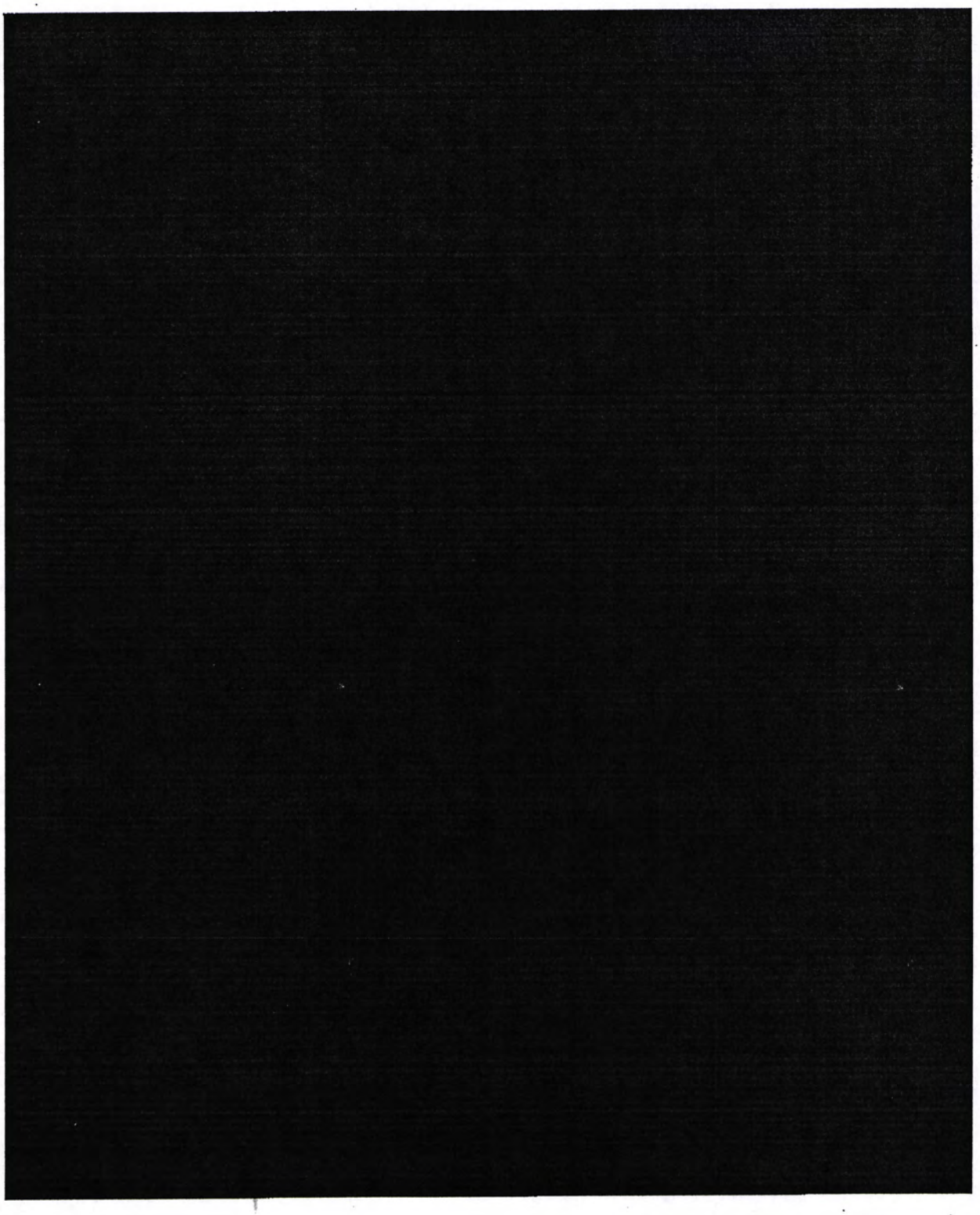
According to the statute, minimization procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance" to minimize the acquisition and retention of non-publicly available information of non-consenting U.S. persons, and prohibit the dissemination of such information that is acquired, consistent with the need to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. §§ 1801(h)(1)-(3), 1881a(e)(1). Initially, the government notes that the FISA Court has found that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained." *In re DNI/AG Certification 2008-A Op.*, Sealed Ex. 10 at 23 (FISA Ct. Sept. 4, 2008). The minimization procedures at issue here provide further protection in line with the statutory requirements. [redacted] provide that disseminations based on communications involving a U.S. person are

authorized only if they meet certain criteria;[37] otherwise, the identity of the U.S. person was to be replaced with a generic term or symbol. *See* Sealed Ex. 31 at 11. The amended FBI minimization procedures contained similar provisions. *See also* Sealed Ex. 32 at 26–32. The FBI's minimization procedures do allow properly-trained personnel to conduct searches of unminimized § 702 acquired information, including searches using terms with U.S. person information, as long as they are reasonably designed to "find and extract" either "foreign intelligence information" or "evidence of a crime." *See id.* at 11, 24–25. But the Court does not find that these U.S. person queries violate the statutory minimization requirements. *See [Caption Redacted]*, 2011 WL 10945618, at *7.

2. Acquisition in this Case

[37] The name of the person could be disseminated if, for example, the information was "necessary to understand foreign intelligence information" or if "the communication or information indicate[d] that the United States person may be engaging in international terrorist activities." Sealed Ex. 31 at 11–12.





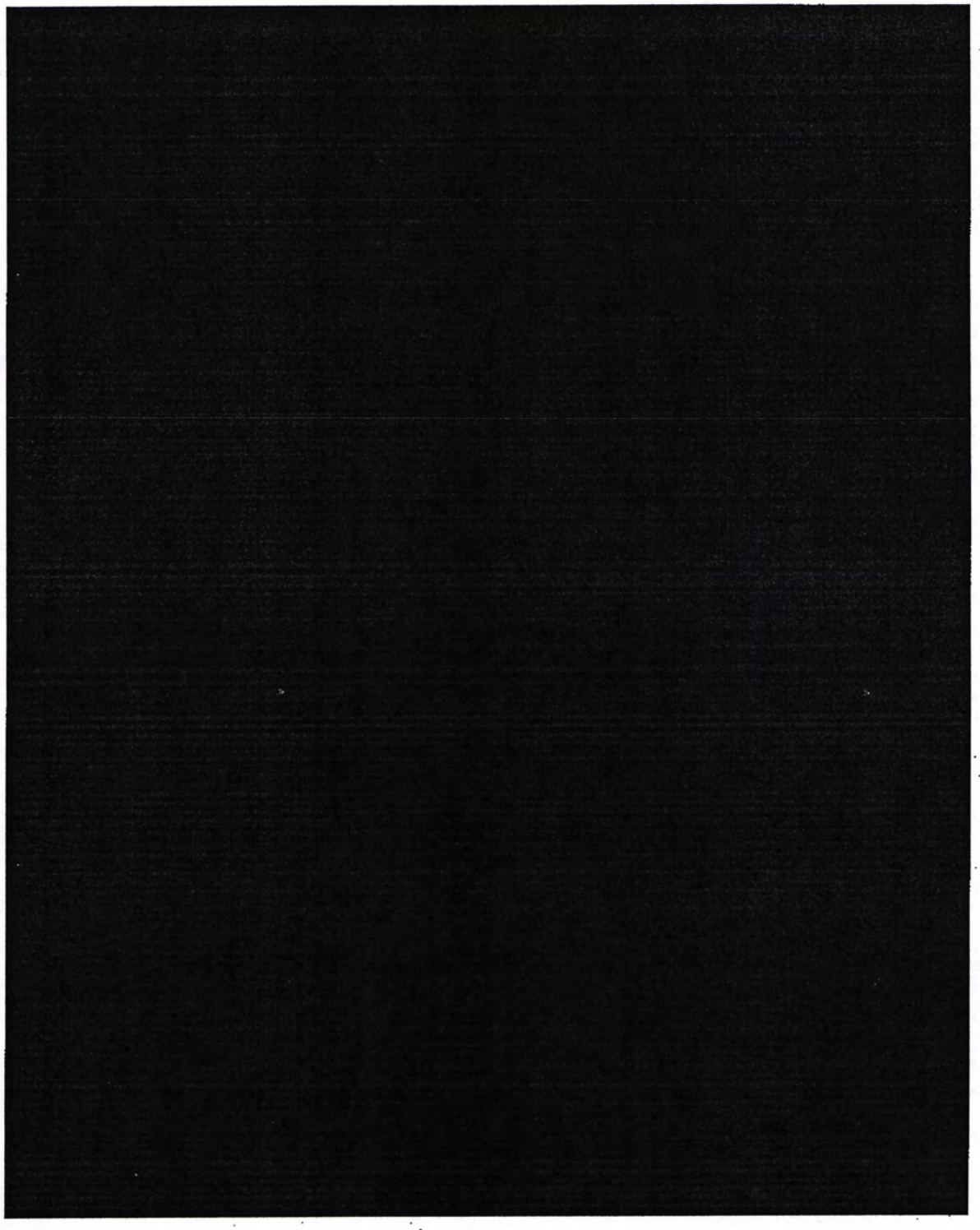
[redacted] The Court again finds that the FBI took all steps required by its minimization procedures in connection with the acquired communications.

Therefore, having thoroughly reviewed the § 702 materials at issue, the Court finds that the acquisition was lawfully authorized and conducted. The Court denies al-Jayab's motion to suppress the evidence obtained or derived from the [redacted]

III. Traditional FISA Collection

In its response to al-Jayab's various motions, the government also argues that the Court should find that the physical search conducted pursuant to traditional FISA authorities complied with the statutory requirements and that the Court should not suppress the information obtained from the search. Al-Jayab did not make a formal motion to suppress information obtained pursuant to traditional FISA authorities so as to trigger *ex parte* and *in camera* review of that information. *See* 50 U.S.C. § 1825(f)-(g). But because the government has provided this information to the Court, and given al-Jayab's belated assertion of such a motion in his reply, *see* Doc. 69 at 13, the Court considers the legality of the traditional FISA physical search that occurred in this case.

As with the § 702 collection, § 1825(g) provides for an *in camera*, *ex parte* review of FISA materials to determine whether the physical search was lawfully authorized and conducted where the Attorney General has filed an affidavit indicating that disclosure or any adversary hearing would harm the national security of the United States. 50 U.S.C. § 1825(g). The Court may only disclose materials to the defense after undertaking this review if the Court concludes "disclosure is necessary to make an accurate determination of the legality of the physical search." *Id.*

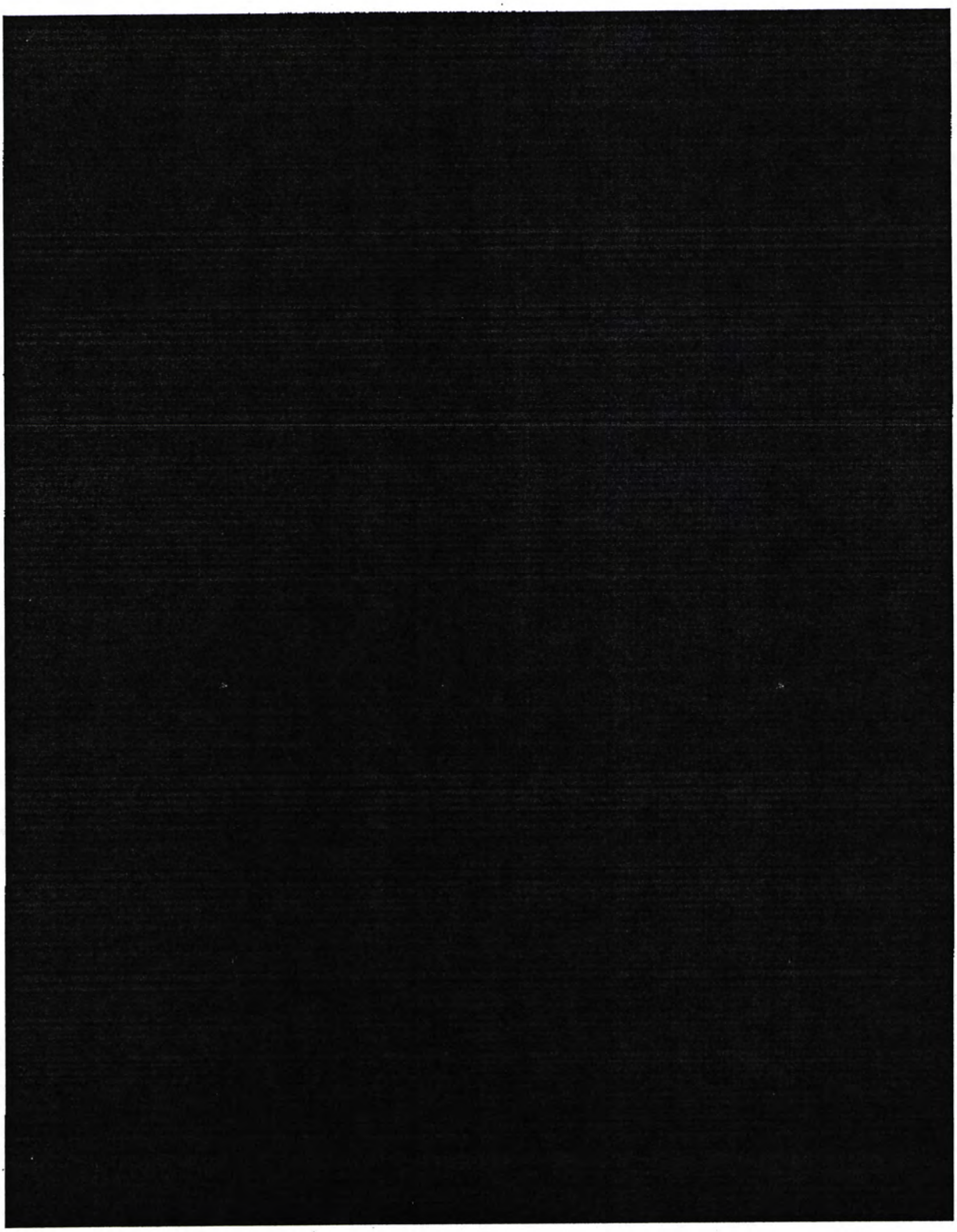


[redacted] In undertaking its review of the traditional FISA collection, the Court addresses (1) whether the certification submitted in support of the FISA application was properly made, (2) whether the FISA Court properly found probable cause, and (3) whether the FISA collection was properly minimized. *United States v. Turner*, 840 F.3d 336, 338 (7th Cir. 2016); 50 U.S.C. §§ 1823(a), 1824(a). The Court reviews the propriety of the FISA Court orders *de novo*, conducting the same review as the FISA Court. *Turner*, 840 F.3d at 340. This *de novo* review extends to consideration of the FISA Court's probable cause determinations. *Id.*

A. Probable Cause

FISA requires the government to establish probable cause that the target "is a foreign power or an agent of a foreign power" and that "the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power." 50 U.S.C. § 1824(a)(2). FISA defines "foreign power" to include "a group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. § 1801(a)(4). An "agent of a foreign power" includes a non-U.S. person who "engages in international terrorism or activities in preparation therefore," and any person, including a U.S. person, who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." 50 U.S.C. § 1801(b)(1)(C), (b)(2)(C).

[redacted]

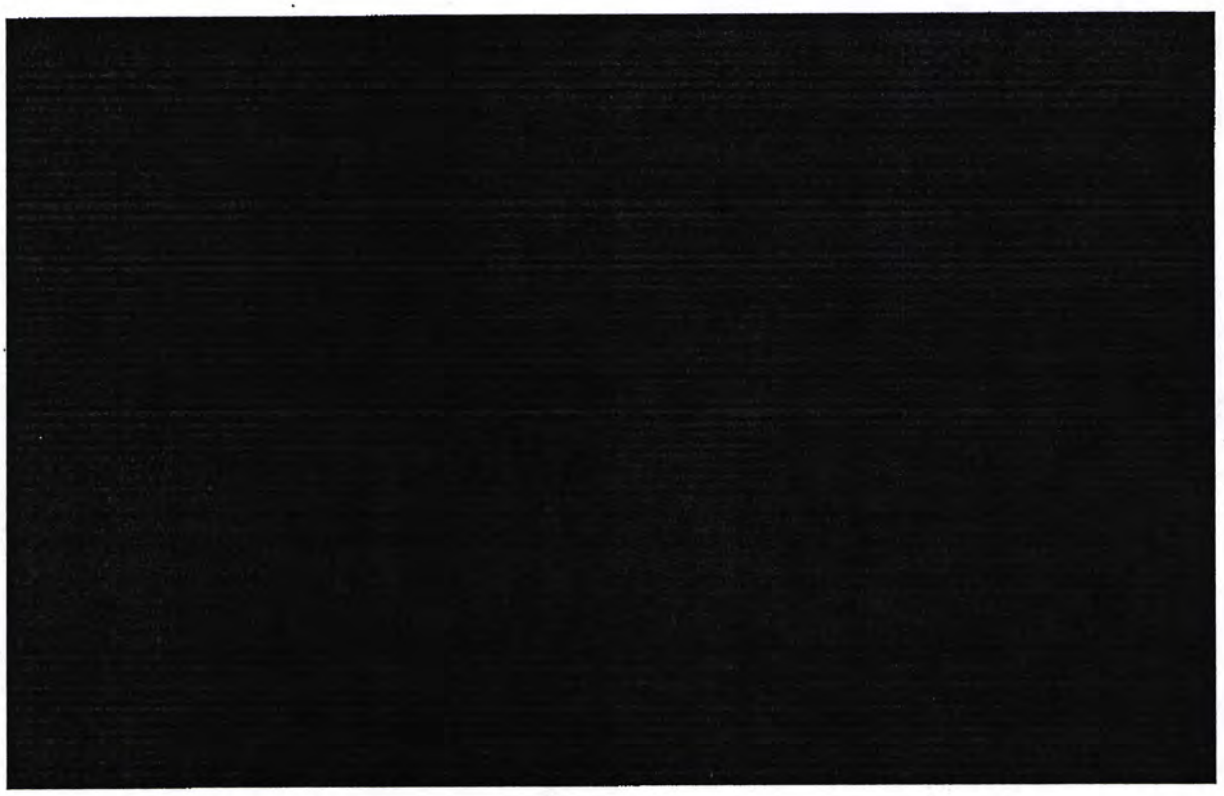


[redacted]

B. Certification

The Court must also ensure that the certification submitted by the government complied with all the statutory requirements. This means that it "contains all statements and certifications required by section 1823 of this title, and, if the target is a United States person, the certification or certifications are not clearly erroneous." 50 U.S.C. § 1824(a)(4). The certification must include information that (1) "the certifying official deems the information sought to be foreign intelligence information," (2) "a significant purpose of the search is to obtain foreign intelligence information," and (3) the "information cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1823(a)(6)(A)-(C). The Court's role "is not to second-guess the executive branch official's certifications." *In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 205 (7th Cir. 2003). Al-Jayab does not challenge any specific factor set forth in § 1823(a).

[redacted]



C. Minimization

After the FISA Court approves FISA surveillance, the government must comply with specific minimization procedures, as described in its application. These minimization procedures provide protections for the communications and information of U.S. persons and must be "reasonably designed . . . 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." *See* 50 U.S.C. § 1821(4).

"The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information." *United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005). The procedures "are subject to a rule of reason," *United States v. Rosen*, 447 F. Supp. 2d 538, 553

(E.D. Va. 2006), with "nominal failure to abide by the minimization procedures" not intended "to undercut entire investigations," *United States v. Aziz*, 228 F. Supp. 3d 363, 378 (M.D. Penn. 2017) (citing S. Rep. No. 95-701, at 21–22).

[redacted]

[redacted] The SMPs govern the acquisition, retention, and dissemination of non-publicly available information concerning non-consenting U.S. persons acquired by the FBI pursuant to FISA. They do not apply to information concerning non-U.S. persons except for provisions concerning attorney-client communications, use of FISA-acquired information in criminal proceedings in both the United States and foreign countries, and the dissemination of raw FISA-acquired information to other agencies. *See* Sealed Ex. 39, SMP § I.B.

[redacted]

Having reviewed the traditional FISA material, the Court finds the [redacted] was properly authorized and conducted. Thus, the Court will not suppress the information obtained or derived from tha[redacted].

IV. Al-Jayab's Request for Disclosure of FISA Materials

In his reply brief addressing § 702 and FISA surveillance, al-Jayab requests the disclosure of all § 702 and FISA related materials and objects to any *ex parte* and *in camera* proceedings under 50 U.S.C. § 1806(f) and § 1825(g) to determine whether any electronic or physical searches were lawfully conducted.[40] But these statutes provide that, upon the filing of an affidavit by the Attorney General that disclosure or an adversary hearing of the materials relating to the § 702 or FISA surveillance would harm the national security of the United States, the Court shall conduct an *in camera* and *ex parte* review of the materials to determine whether the surveillance was lawfully authorized and conducted. 50 U.S.C. §§ 1806(f), 1825(g). Only after undertaking this review may the Court order disclosure of the materials to the defense, and it may do so only where "necessary to make an accurate determination of the legality of the

[40] In his opening brief concerning § 702 surveillance, al-Jayab did include a request that the Court order the government to disclose all § 702 material *to the Court*, but he did not ask for such disclosure to his own counsel. *See* Doc. 48 at 48.

surveillance" or "the physical search" 50 U.S.C. § 1806(f), 1825(g); *see Daoud*, 755 F.3d at 484 ("Unless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction.").

Al-Jayab contends that disclosure would substantially promote the Court's understanding of the legality of the surveillance here, particularly in light of al-Jayab's complicated factual background and the need to ensure the accuracy of translations and attributions in the materials at issue. Although the Court agrees with al-Jayab that "the legality of the surveillance and search would be better tested through the adversarial process," that is not the relevant inquiry. *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130 (D. Mass. 2007) ("The question under the statute, however, is not how to optimize the legal review of the surveillance and search, but whether disclosure is 'necessary' in order to make that determination.").

Al-Jayab also argues that disclosure is necessary to provide a basis for any potential suppression motion pursuant to *Franks v. Delaware*, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978). The Court acknowledges the difficulty al-Jayab faces in making the required preliminary showing that statements in the FISA or § 702 applications were false to be entitled to a hearing without access to the underlying materials. But the Court cannot provide access to materials "simply to ensure against the possibility of a *Franks* violation" without such a preliminary showing. *Mubayyid*, 521 F. Supp. 2d at 130–31; *see also Mohamud I*, 2014 WL 2866749, at *31 (denying *Franks* hearing where defendant only speculated about false statements or omissions and relied on unrelated cases to suggest errors in his case, collecting cases); *United States v. Medunjanin*, No. 10 CR 19 1 (RJD), 2012 WL 526428, at *10 (E.D.N.Y.

Feb. 16, 2012) ("Defense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA[.]"). Here, al-Jayab has given the Court no basis to suspect a *Franks* violation. But the Court has kept the difficulties inherent in making a preliminary showing in mind in undertaking its careful, independent review of the FISA record. *See Daoud*, 755 F.3d at 484 (noting the difficulties for a defendant in mounting a *Franks* challenge without access to classified materials, but stating that "[t]he drafters of the Foreign Intelligence Surveillance Act devised a solution: the judge makes the additional determination, based on full access to all classified materials and the defense's proffer of its version of events, of whether it's possible to determine the validity of the *Franks* challenge without disclosure of any of the classified materials to the defense"); *Aziz*, 228 F. Supp. 3d at 371 ("In recognition [of the "all but insurmountable" preliminary burden a defendant faces in the FISA context], Congress mandated careful *ex parte* and *in camera* judicial review of the FISA record. In essence, the court's independent review may supplant that of defense counsel."). *But see Daoud*, 755 F.3d at 486–496 (Rovner, J., concurring) (addressing the difficulties in reconciling *Franks* with FISA proceedings where defendants do not have access to the FISA applications). Having reviewed the materials, the Court finds no evidence or indication of a material misstatement or omission so as to warrant a *Franks* hearing. The Court has also found it possible to determine the legality of the investigations from the FISA materials without disclosure to the defense. *See Daoud*, 755 F.3d at 484–85 (where the judge is "capable" of "making an accurate determination without disclosing any classified materials to defense counsel . . . disclosure was not 'necessary' under any definition of that word"); *Hasbajrami*, 2016 WL 1029500, at *14 (finding that court could "evaluate the legality of the challenged surveillance without concluding that due process first

warranted disclosure"); *Mohamud I*, 2014 WL 2866749, at *32 (finding "necessary" to "be much closer to 'essential' than to 'helpful'" and that the court could make an accurate determination of the legality of the surveillance without disclosure to the defense).

Al-Jayab also argues that disclosure is necessary as a matter of due process, relying on the balancing test set forth in *Mathews v. Eldridge*, 424 U.S. 319, 335, 96 S. Ct. 893, 47 L. Ed. 2d 18 (1976). The government contends that the *Mathews* balancing test does not apply in criminal cases. *See Medina v. California*, 505 U.S. 437, 444–45, 112 S. Ct. 2572, 120 L. Ed. 2d 353 (1992) (questioning the applicability of *Mathews* to resolving due process claims in criminal cases); *United States v. Warsame*, 547 F. Supp. 2d 982, 988 (D. Minn. 2008) ("The Court is therefore not convinced that the *Mathews* balancing test supplies an appropriate framework for evaluating FISA procedures in this case."). But even those courts to have considered the *Mathews* framework in the FISA context have all found that FISA's *in camera, ex parte* review process complies with due process. *See United States v. El-Mezain*, 664 F.3d 467, 567–68 (5th Cir. 2011) (concluding after engaging in balancing test that due process did not require disclosure of FISA materials); *United States v. Elshinawy*, No. ELH-16-0009, 2017 WL 1048210, at *8–9 (D. Md. Mar. 20, 2017) (collecting cases); *Aziz*, 228 F. Supp. 3d at 369 (finding that FISA's "system of legislative, executive, and judicial supervision adequately guards a defendant's constitutional rights"). Al-Jayab does not raise any arguments that would compel the Court to deviate from these well-reasoned opinions. Following these opinions, then, the Court similarly finds that due process does not require disclosure of the FISA materials to defense counsel.

Next, al-Jayab argues that *Brady v. Maryland*, 373 U.S. 83, requires disclosure of the FISA materials, contending that the government's application to the FISA Court and the FISA

Court order authorizing the electronic and physical searches in this case would be helpful to the defense in preparing the motions to suppress the § 702 and FISA-derived evidence. But having reviewed the FISA documents, the Court concludes that these documents include no exculpatory material that must be disclosed under *Brady*.

Finally, in a supplemental filing, al-Jayab argues that the declassification and release in February 2018 of two House Select Committee on Intelligence memoranda that summarize portions of a FISA application demonstrate that "it is possible to discuss publicly the merits of a FISA application without damaging national security" and warrant disclosure of the FISA materials in this case to cleared defense counsel. Doc. 99-1 at 5. In the case of the House Select Committee on Intelligence memoranda, however, the President made an executive decision to declassify the information, having determined that "the public interest in disclosure outweighs any need to protect the information." Doc. 99-1 at 10. The limited declassification of FISA materials in those memoranda does not suggest that all FISA materials should now be made available to defense counsel or the public, where each FISA application must be evaluated individually to determine whether its disclosure would harm national security. Here, the executive branch maintains that disclosure of the FISA information would harm national security. The Court defers to the executive branch's certifications on such issues, *see In re Grand Jury Proceedings*, 347 F.3d at 205, and may only disclose the FISA materials to defense counsel if it finds it cannot make an accurate determination of the legality of the surveillance *in camera* and *ex parte*, *see Daoud*, 755 F.3d at 484. The recent disclosure of select FISA materials does not affect this standard of review. As the Court has found disclosure unnecessary under this standard, the Court denies al-Jayab's request for disclosure and his objection to the conduct of *ex parte* and *in camera* proceedings with respect to the FISA materials.

V. Al-Jayab's Motion for Notice of Surveillance Techniques Used During the Course of the Investigation [52]

Al-Jayab also requests an order compelling notice and discovery of (1) each surveillance program or technique the government used to obtain information about al-Jayab's communications or activities during its investigation, (2) the legal authority relied on, and (3) the warrants, orders, directives, and court applications that supported the surveillance used.[41] Specifically, al-Jayab requests disclosure concerning the following surveillance techniques: (1) FISA §§ 703-705 (50 U.S.C. § 1881b-d); (2) 50 U.S.C. § 1861 (§ 215 of the Patriot Act); and (3) National Security Letters (specifically, 18 U.S.C. § 2709). He claims disclosure is required by the Fourth and Fifth Amendments, 18 U.S.C. § 3504, FISA, and Federal Rules of Criminal Procedure 12 and 16.

A. Surveillance Techniques at Issue

As for surveillance under FISA §§ 703-705, al-Jayab contends that although these sections target U.S. persons located overseas, they may be relevant because intelligence agencies could have intercepted al-Jayab's communications with U.S. persons located overseas and also appear to have intercepted his communications when he was allegedly overseas from late 2013 through early 2014. The government is expressly required to give notice of its intent to enter into evidence or otherwise use or disclose information obtained or derived from § 703 surveillance. 50 U.S.C. §§ 1806(c), 1881e(b). This notice requirement does not apply to surveillance derived from § 704 or §.705.

Section 215 of the Patriot Act allows for the production of "any tangible things" in connection with investigations to obtain foreign intelligence information not concerning U.S.

[41] Al-Jayab's counsel also made this request of the government in a June 30, 2016 discovery letter.

persons or to protect against international terrorism. 50 U.S.C. § 1861(a)(1). The government previously used § 215 to support the bulk collection of call records, but the Second Circuit found in 2015 that § 215 did not allow for such collection. *See ACLU v. Clapper*, 785 F.3d 787, 810–821 (2d Cir. 2015). Al-Jayab argues that because much of the surveillance in this case predated *Clapper* and Congress' subsequent modification of § 215 to expressly prohibit the bulk collection of call records, the government may have relied on § 215 to collect his call records. He also contends that the government could have used this section to obtain his internet browsing records, travel records, and financial records, including the international money transfers mentioned in the criminal complaint in the case pending against him in the Eastern District of California.

Finally, al-Jayab posits that the government may have used national security letters to obtain his unique IP addresses, account information across various online communication services, and his internet browsing records. 18 U.S.C. § 2709 provides that the FBI may compel wire or electronic communication service providers to disclose subscriber information and electronic communication transactional records when an FBI senior official certifies that such records are relevant to authorized investigations to protect against international terrorism.

B. Alleged Bases for Requiring Notice of Surveillance Techniques

1. Fourth and Fifth Amendments

First, al-Jayab contends that the Fourth and Fifth Amendments require the government to disclose its use of surveillance methods so as to allow him to challenge the legality of these methods and seek suppression of the derivative evidence. Essentially, al-Jayab argues that without knowing the methods of the government's surveillance of him, he cannot determine if anything the government intends to introduce against him at trial is derived from unlawful

surveillance, *i.e.*, if it is the fruit of a potentially poisonous tree. The government represents that it has complied with its notice and discovery obligations and so has no further obligation to inform al-Jayab of which, if any, additional surveillance techniques it used. But al-Jayab argues that the government should not be entitled to make these determinations on its own and that he is entitled to know if the evidence the government intends to use, even if obtained through lawful means, derived from unlawful surveillance. Al-Jayab cites *Alderman v. United States*, 394 U.S. 165, 89 S. Ct. 961, 22 L. Ed. 2d 176 (1969), to argue that the Court cannot allow the government to unilaterally decide the relevance and legality of the evidence it has gathered. In *Alderman*, the Supreme Court required an adversarial hearing because unlawful surveillance had admittedly occurred, *id.* at 180–82, in contrast to the situation here, where al-Jayab seeks to first learn of the surveillance techniques used so as to determine whether any illegal surveillance occurred in the first place. *See United States v. D'Andrea*, 495 F.2d 1170, 1174 (3d Cir. 1974) (distinguishing *Alderman* and approving of *ex parte*, *in camera* hearing to address the threshold question of "whether the alleged illegal surveillance had occurred at all").

2. 18 U.S.C. § 3504

Al-Jayab also argues that he is entitled to notice of electronic surveillance under 18 U.S.C. § 3504. Section 3504 provides that if a party in a proceeding claims that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the government must affirm or deny the occurrence of the alleged unlawful act. 18 U.S.C. § 3504(a)(1). Section 3504 "concerns only *unlawful* surveillance; it does not require affirmance or denial of *all* surveillance." *Aziz*, 228 F. Supp. 3d at 370.

Al-Jayab argues that he need only make a colorable claim of having been subjected to illegal surveillance. *See United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (requiring party claiming to be the victim of illegal surveillance to assert a "cognizable claim," or "a positive statement that illegal surveillance has taken place," and make a prima facie showing that the party was aggrieved by that surveillance, *i.e.*, that he was a party to an intercepted communication, that the government's efforts were directed at him, or that the intercepted communications took place on his premises, which must be based on more than "mere suspicion"). Al-Jayab contends he has done so, positing that the government has collected information about him and his online activities using investigative tools and lawful search warrants without providing details regarding their collection while also providing notice that it intends to use materials collected pursuant to the FAA. [redacted]

[redacted]

The government contends that al-Jayab has not made a sufficient claim of being subjected to illegal surveillance by making only conclusory allegations related to his own case. supported by citations to sources about unrelated problematic foreign intelligence collections. *See United States v. Aref*, 285 F. App'x 784, 793 (2d Cir. 2008) (defendant's showing of statements by unnamed sources in a newspaper article and prosecutor's pattern of objections not sufficient to show unlawful surveillance so as to trigger § 3504); *United States v. Londono-Cardona*, No. 05-10304-GAO, 2008 WL 313473, at *2 (D. Mass. Feb. 1, 2008) (requiring aggrieved person to make "some showing of basis for suspecting illegal action" because otherwise "the statute would have to be understood to require automatic disclosure simply on the

making of an unsupported suggestion that there had been some unlawful intercept, which is not what Congress apparently intended" (citing *United States v. Doe*, 460 F.2d 328, 336 (1st Cir. 1972)). But in the Seventh Circuit, even where the defendant has made an allegation of electronic surveillance that is unsupported by affidavit or otherwise unverified, the government must still respond, although an affidavit based on the investigating prosecutor's personal knowledge suffices. *In re Grand Jury Proceedings of Aug., 1984*, 757 F.2d 108, 114 (7th Cir. 1984). Based on this precedent, then, although al-Jayab's allegations of unlawful surveillance are unsupported, the Court requires the government to respond by affidavit affirming or denying the alleged surveillance. *See id.*; *In re DeMonte*, 667 F.2d 590, 595 (7th Cir. 1981).

But the Court agrees with the government that the extent of this § 3504 inquiry does not encompass FISA surveillance. As one district court has stated, although without citation or analysis, "FISA's particularized notice, disclosure, and suppression procedures supplant the requirements of § 3504." *Aziz*, 228 F. Supp. 3d at 370. FISA's notice provisions, adopted after § 3504, are more specific and control over § 3504's general disclosure requirement. *See Gozlon-Peretz v. United States*, 498 U.S. 395, 407, 111 S. Ct. 840, 112 L. Ed. 2d 919 (1991) ("A specific provision controls over one of more general application."); *Bhd. of Maint. of Way Emps. v. CSX Transp., Inc.*, 478 F.3d 814, 817 (7th Cir. 2007) ("In looking at two statutes which might be said to deal with the same subject matter, we must apply certain principles. A specific statute takes precedence over a more general statute, and a later enacted statute may limit the scope of an earlier statute."). To the extent that al-Jayab seeks notice of other electronic surveillance not covered by FISA, however, the government must comply with § 3504 as set forth above.

3. FISA

To the extent that al-Jayab contends that he is entitled to notice under FISA, the government represents that it has provided al-Jayab with all the notice to which he is entitled. As the Court has already found, FISA's notice provisions comply with due process and so the Court finds no further need for disclosure on this ground. *See Aziz*, 228 F. Supp. 3d at 369 (finding "no constitutional deficiency in FISA's notice and disclosure provisions").

4. Federal Rules of Criminal Procedure 12 and 16

Finally, al-Jayab argues that Federal Rules of Criminal Procedure 12 and 16 require notice and disclosure of the government's surveillance techniques. With respect to FISA surveillance, FISA's statutory disclosure provisions displaced these rules. *See id.* at 370 ("Congress intentionally replaced these discovery rules with FISA's disclosure framework. . . . Federal Rules 12 and 16 do not, and cannot, supersede FISA's statutory prohibition on disclosure."); *United States v. Thomson*, 752 F. Supp. 75, 82 (W.D.N.Y. 1990) ("FISA rendered Rule 16 and other existing laws inapplicable to discovery of FISA surveillance information[.]"). Otherwise, the government represents that it has complied with Rule 12 and 16's disclosure requirements. To the extent events ultimately prove otherwise, the Court will address such violations as they arise.

VI. Al-Jayab's Motion for Discovery Regarding Intelligence Agencies' Surveillance Pursuant to Executive Order 12333 [51]

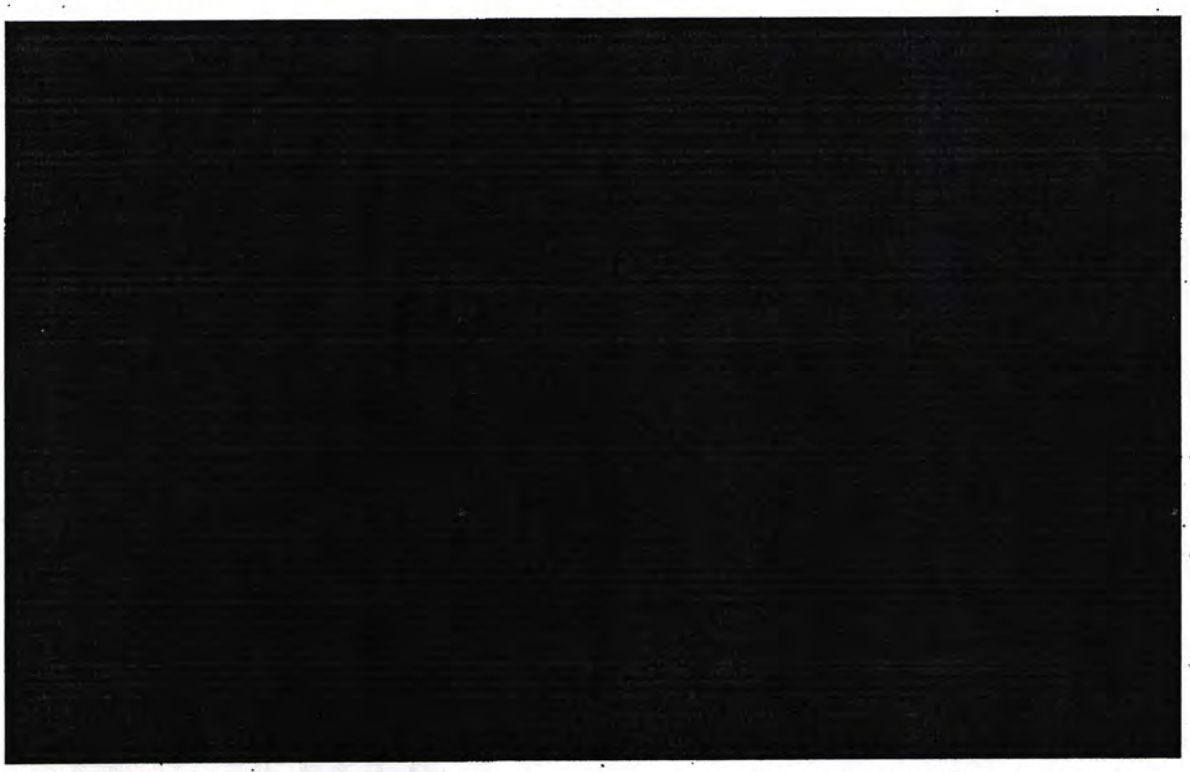
Finally, in a related motion, al-Jayab seeks the production of any material concerning the intelligence agencies' use of surveillance pursuant to Executive Order 12333 ("EO 12333"). He asks not only for production of additional materials but also that the government identify previously disclosed materials acquired under the authority of EO 12333. Additionally, al-Jayab

seeks all materials reflecting the use of EO 123333 during the investigation into al-Jayab's communications and activities.

EO 12333 provides that the intelligence community shall conduct intelligence activities "necessary for the conduct of foreign relations and the protection of the national security of the United States." EO 12333 § 1.4. This includes the "[c]ollection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist . . . activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents." EO 12333 § 1.4(c). EO 12333 authorizes collection of information "constituting foreign intelligence or counterintelligence," provided that no foreign intelligence collection by agencies of the intelligence community "be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons." EO 12333 § 2.3(b). The collection procedures used should "protect constitutional and other legal rights and limit use of such information to lawful governmental purposes." EO 12333 § 2.4. EO 12333 allows the use of techniques that typically require a warrant if the Attorney General determines there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power, even if the technique is being used in the United States or against a U.S. person abroad. EO 12333 § 2.5.

Al-Jayab contends he is entitled to notice of the use of EO 12333 for several reasons: (1) to allow him to potentially mount a challenge to the legality of the surveillance and seek suppression of any derivative evidence, (2) to ensure production of exculpatory material pursuant to *Brady v. Maryland*, 373 U.S. 83, and (3) because counsel is entitled to all of al-Jayab's statements in the government's possession, custody, or control pursuant to Federal Rule of Criminal Procedure 16(a)(1)(B). Alternatively, al-Jayab argues that, at a minimum, 18 U.S.C.

§ 3504 entitles him to notice of surveillance conducted pursuant to EO 12333. Al-Jayab claims that based on discovery showing his online communications with individuals located overseas, including in Syria, Iraq, and Turkey, there is a colorable basis to believe that the government's case is obtained or derived from EO 12333 surveillance, requiring the government to affirm or deny the use of surveillance pursuant to EO 12333.



[redacted] The Court thus denies al-Jayab's motion for discovery regarding surveillance pursuant to EO 12333.

CONCLUSION

For the foregoing reasons, the Court grants in part and denies in part the government's motion for a protective order pursuant to Section 4 of CIPA [55]. The government may withhold from discovery all but the two [redacted] –pursuant to CIPA § 4. [redacted]

[redacted]

The Court grants in part and denies in part al-Jayab's motion for notice of surveillance techniques used during the course of the investigation [52]. The government must provide al-Jayab with an affidavit in compliance with 18 U.S.C. § 3504. The Court denies al-Jayab's motion to suppress evidence obtained or derived from warrantless surveillance under Section 702 of the FISA Amendments Act [47], motion for disclosure to cleared counsel and objection to secret *ex parte* CIPA litigation of Fourth Amendment suppression issue [50], and motion for discovery regarding the intelligence agencies' surveillance pursuant to Executive Order 12333 [51]. The Court also denies al-Jayab's motion to suppress evidence obtained or derived from the physical surveillance conducted pursuant to FISA and al-Jayab's motion for disclosure of the underlying FISA and § 702 materials.

Dated: June 28, 2018

SARA L. ELLIS
United States District Judge