UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

In the Matter of the Search of the Real Property and Premises of Hannah Natanson,	No. 1:25-sw-00054-WBP

OPPOSITION OF THE UNITED STATES TO THE MOTION TO INTERVENE AND FOR RETURN OF PROPERTY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Regulations

Other Authorities

INTRODUCTION

Earlier this month, the Government seized devices from Ms. Hannah Natanson that it has probable cause to believe contain evidence of crimes committed by a government contractor named Aurelio Perez-Lugones. That evidence includes government secrets of the most sensitive type—information that cannot be disseminated without risking exceptionally grave harm to the United States. Ms. Natanson and her employer, the Washington Post, claim the Government's seizure of this evidence violated the First Amendment and that it must be returned to them. They are wrong. Under the reasonableness standard of Federal Rule of Criminal Procedure 41(g), the Government is entitled to maintain this evidence because it is relevant to an ongoing investigation and prosecution. In addition, the Government cannot be reasonably required to hand over to Movants devices that the Government has probable cause to believe contain its own highly classified information.

Movants invite the Court to reimagine the First Amendment as a journalist's exception to search warrants. That is not the law, and the Government did not impose an unconstitutional prior restraint on Movants by executing the search warrant. "It is clear that the First Amendment does not invalidate every incidental burdening of the press that may result from the enforcement of civil or criminal statutes of general applicability." *Branzburg v. Hayes*, 408 U.S. 665, 682 (1972). "[O]therwise valid laws serving substantial public interests may be enforced against the press as against others, despite the possible burden that may be imposed." *Id.* at 682-83.

Movants' fallback position that the Court should take on responsibility for segregating evidence and classified information also misses the mark. That task must be performed by experts trained in identifying national security information. And because of the sensitivity of the classified information at issue, access to it must be limited to the maximum extent. The Government has developed an appropriate protocol for a filter team that will work to protect applicable privileges

as well as Movants' confidentiality interests. The Court should deny the Rule 41(g) motion, dissolve the Standstill Order, and permit the Government to review the seized devices as it prepares for Mr. Perez-Lugones's trial.

BACKGROUND

I. Investigation, Arrest, and Indictment of Aurelio Perez-Lugones

On October 31, 2025, the Washington Post published an article containing classified information from an intelligence report. *See* Ex. 1, Decl. of Roman Rozhavsky ¶¶ 6, 12. Ms. Natanson co-authored the article. *See id.* ¶ 12. The intelligence report was classified at one of the highest levels; TOP SECRET//SCI//NOFORN. *See id.* ¶ 11.[1] The Federal Bureau of Investigation (FBI) began to investigate the dissemination of the published classified information. *See id.* ¶ 5.

A government contractor named Aurelio Perez-Lugones became a suspect. Mr. Perez-Lugones is a former member of the U.S. Navy and had held a security clearance since at least 1995. *See id.* ¶ 7. As a government contractor, Mr. Perez-Lugones had access to classified systems and networks, and he worked inside a Sensitive Compartmented Information Facility (SCIF). *See id.* ¶ 8. The FBI learned that, on or around October 28, 2025, Mr. Perez-Lugones had allegedly viewed the Top Secret intelligence report on which Ms. Natanson reported days later. *See id.* ¶¶ 11–12. He allegedly took screenshots of that report and of one of its attachments and pasted those screenshots into a Microsoft Word document. *See id.* ¶ 11. The cropping of one screenshot rendered a portion of the intelligence report unreadable. *See id.* Ms. Natanson's article omitted

[1] Documents containing classified information are marked with headers to indicate the classification of the information and any restrictions on it. Information is classified as Top Secret when its unauthorized disclosure "could reasonably be expected to cause exceptionally grave damage to the national security." 18 C.F.R. § 3a.11(a)(1). The "NOFORN" marking indicates that information is not releasable to foreign nationals and can be disseminated only to U.S. nationals.

the same portion of the intelligence report that was rendered illegible in the screenshot. *See id.* ¶ 12.

This pattern unfortunately repeated multiple times—classified information would appear in the Washington Post after Mr. Perez-Lugones allegedly accessed it. *See id.* ¶¶ 13–18, 22. In most instances, he allegedly took screenshots of that information and pasted them into another application (typically Microsoft Word) before printing and removing the document containing the screenshots. *See id.* ¶¶ 13–14. In one instance, he allegedly cut off header information from the printed document, thereby removing his name, *see id.* ¶ 18, which the application had placed there for tracking purposes. And in another instance, he allegedly made handwritten notes while viewing classified intelligence reports on his work computer and removed those notes from the SCIF, the specially equipped environment for storing such materials. *See id.* ¶ 16. The documents he accessed were marked by headers, including SECRET//NOFORN and CONFIDENTIAL//NOFORN.[2] *See id.* ¶¶ 13, 14, 16, 18. And days after Perez-Lugones accessed classified information from those documents, that information appeared in the Washington Post as part of articles coauthored by Ms. Natanson. *See id.* ¶¶ 13, 15, 17, 22.

The FBI arrested Perez-Lugones on January 8, 2026. *See id.* ¶ 19. Prior to his arrest, the FBI consensually reviewed messages between Mr. Perez-Lugones and Ms. Natanson sent via Signal on or around January 7 and 8, 2026. *See id.* Signal is a messaging app that provides end-to-end encryption and allows users to create a custom timeframe in which messages "disappear" or "delete." *Id.* ¶ 40. The messages discussed the classification level of certain documents, set

[2] Information is classified as Secret when its disclosure "could reasonably be expected to cause serious damage to the national security." 18 C.F.R. § 3a.11(a)(2). Information classified as Confidential is information the unauthorized disclosure of which "could reasonably be expected to cause damage to the national security." 18 C.F.R. § 3a.11(a)(3).

forth details about which U.S. government agencies had produced different reports, and explained how certain documents would be referenced in forthcoming news articles. *See id.* ¶19. The review of his device also revealed that Perez-Lugones had sent audio messages to Natanson providing additional details about the information that he had transmitted and photographs of the documents that had been the source of the classified information in the Washington Post. *See id.* ¶¶ 19–20. After transmitting one such document, Perez-Lugones wrote, "I'm going quiet for a bit . . . just to see if anyone starts asking questions." *See id.* ¶ 20. Around this same time, the FBI located, pursuant to a court-authorized search, a hard copy printout of a SECRET//NOFORN document in Perez-Lugones's lunchbox. *See id.* ¶ 21. The header was removed from that printout, but agents later found it in a trash can at Perez-Lugones' workplace. *See id.* ¶¶ 21–22.

Perez-Lugones was charged by complaint with unlawful retention of national defense information in violation of 18 U.S.C. § 793(e). *See id.* ¶ 23. And on January 22, a federal grand jury in the District of Maryland indicted Perez-Lugones for five counts of unlawfully transmitting, and one count of unlawfully retaining, national defense information in violation of 18 U.S.C. § 793(e). *See* ECF No. 25, *United States v. Perez-Lugones*, No. 26-cr-30 (D. Md., Jan. 22, 2026) (Indictment).

II. The Search Warrant

Days after Perez-Lugones's arrest, the Government sought search warrants in this District for Ms. Natanson's person, vehicle, and residence to recover electronic devices the Government had probable cause to believe contained classified information sent by Perez-Lugones. *See* Nos. 26-sw-52 (vehicle), 26-sw-53 (person), 26-sw-54 (residence). This Court issued those search warrants. Attachment B to the warrant for Ms. Natanson's residence authorized investigators to seize "[a]ll digital devices, other electronic storage media, or components of either identified during the searches" that "are reasonably believed to be used by Natanson," including her mobile

phone. ECF No. 9-5 at 5 (ECF pagination) (footnotes omitted). Those authorized searches were "limited to all records and information, including classified and/or national defense information," constituting "records received from or relating to Aurelio Luis Perez-Lugones, as evidence of violations of 18 U.S.C. § 793." *Id.*

The warrant also directed the investigators to use reasonable methods and procedures to locate information responsive to the warrant "while minimizing the review of information not within the list of items to be seized . . . , to the extent reasonably practicable." *Id.* at 6. These methods and procedures, however, should still "permit[] government examination of all the data necessary to determine whether that data falls within the items to be seized." *Id.* The warrant further authorized investigators to "press or swipe" Ms. Natanson's fingers "to the fingerprint scanner of the device" and to "hold a device found during the search in front of [her] face" to activate any facial recognition feature "for the purpose of attempting to unlock" that particular device. *Id.* at 7.

The FBI executed the warrant on January 14. *See* Rozhavsky Decl. ¶ 24. Prior to entering the premises, the agents announced themselves. *See id.* ¶ 25. They asked Ms. Natanson what electronics she had and advised her that, though she was not compelled to provide her passcodes, the FBI could use her biometrics to open any devices. *See id.* She stated that she had only a laptop and a cell phone upstairs and that she did not use biometrics on her devices. *See id.* In the upstairs of the house, investigators located a powered-off silver MacBook Pro with a black case, an Apple iPhone 13, a Handy branded audio recording device, and a Seagate portable hard drive. *See id.* ¶ 26. Investigators seized these devices. The iPhone was found powered on and charging, and its display noted that the phone was in "Lockdown" mode. *See id.* ¶ 27. Investigators also seized Ms. Natanson's Garmin watch as an electronic device covered by the search warrant. *See id.* ¶ 28.

Investigators then discovered another silver MacBook Pro (this time without a case) inside a red backpack in the kitchen. *See id.* ¶ 29. Once opened, the laptop asked for a Touch Id or a Password. *See id.* When investigators later presented the laptop to Ms. Natanson, she reiterated she does not use biometrics for her devices. *See id.* ¶ 31. Investigators told her to try nevertheless, and when she applied her index finger to the fingerprint reader, the laptop unlocked. *See id.* ¶ 32. This computer is referred to as the Work MacBook Pro.

Investigators checked the seized devices into evidence at the FBI's Washington Field Office. *See id.* ¶ 33. That afternoon, the Department of Justice informed the FBI that the seized items would need to undergo a scoping process to comply with Attachment B and review by a filter team to protect against disclosure of privileged materials to the investigation team. *See id.* ¶ 34. The processing of all electronic devices was thus conducted by filter Agents who were not (and will never be) associated with the case team responsible for the Perez-Lugones investigation. *See id.*

The Computer Analysis Response Team (CART) began processing each device to preserve the information therein. The Handy recorder and the Seagate portable drive have been processed, but no review has occurred. *See id.* ¶ 37. Because the iPhone was in Lockdown mode, CART could not extract that device. *See id.* ¶ 35. Similarly, the personal MacBook Pro could not be imaged yet. *See id.* ¶ 36. The Garmin watch was not processed before this Cout's Standstill Order, and no further processing will occur until further order of the Court. *See id.* ¶ 37.

As for the Work MacBook Pro, the FBI has not yet been able to obtain a full physical image of the device. *See id.* ¶ 38. A limited partial live logical image was made but not reviewed. *See id.* Agents also began taking photographs and, where necessary, audio recordings of the various conversations in the laptop's Signal application as the only option to preserve the information. *See*

id. ¶ 41. Investigators noticed that several of Ms. Natanson's Signal chat messages were set for auto-deletion. *See id.* ¶ 40. Agents thus worked in a reverse chronological order to take pictures of the Signal conversations for only those conversations in which the display date of the last message, attachment, notification, conversation setting change, etc. was on or after October 1, 2025, consistent with Attachment B. *See id.* ¶ 45. Once the conversations were photographed in their entirety, as they appeared on screen, agents then attempted to manually click on and open every attachment and file contained within each conversation, again solely to preserve the information. *See id.* ¶ 47. For audio messages that they discovered, investigators captured those by using the video recording function on a camera. *See id.* ¶ 48. This process took up five memory cards that investigators subsequently transferred to a staging drive for storage. *See id.* ¶ 49. These actions were taken only for preservation purposes and no substantive review has occurred. *See id.* ¶ 50.

III. The Pending Motion

On January 21, the Washington Post and Ms. Natanson (collectively, Movants) filed a combined motion for return of Ms. Natanson's property under Federal Rule of Criminal Procedure 41(g) and for the Post to intervene, along with a memorandum of reasons supporting that motion. *See* Mot. to Intervene and for Return of Property, ECF No. 8; Mem. of Law In Supp. Of Mot. to Intervene and for Return of Property, ECF No. 9 (Mot.). Movants also requested, via separate motion, a "standstill order to preserve the status quo and an expedited schedule for briefing and hearing" on the Rule 41(g) motion. *See* ECF No. 10.

This Court granted that motion and entered an order directing the Government to "preserve but [] not review any of the materials that law enforcement seized pursuant to" the search warrants. ECF No. 18 at 1. The Government is complying with that order. *See* Rozhavksy Decl. ¶ 50. The Court also set a briefing schedule and oral argument on the Rule 41(g) motion. *See* ECF No. 18.

After a consent motion to modify that schedule by one business day, the Court entered a new scheduling order. *See* ECF No. 33.

ARGUMENT

I. Movants Fail to Establish Entitlement to the Return of Property Because The Government Has a Reasonable Need for It.

Under Fed. R. Crim. P. 41(g), "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Fed. R. Crim. P. 41(g). "[D]uring the pendency of an ongoing criminal investigation or proceeding, the [movant] bears the burden of demonstrating that the government's retention of the seized property is unreasonable." *Allen v. Grist Mill Cap. LLC*, 88 F.4th 383, 396 (2d Cir. 2023); *see also United States v. Chambers*, 192 F.3d 374, 377 (3d Cir. 1999). "No standard is set forth in the rule to govern the determination of whether property should be returned to a person aggrieved either by an unlawful seizure or by deprivation of the property." Fed. R. Crim. P. 41 advisory committee's note to 1989 amendment. "[R]easonableness under all of the circumstances must be the test when a person seeks to obtain the return of property." *Id.* In general, "the Government may retain the property if it has a legitimate reason for doing so." *Lavin v. United States*, 299 F.3d 123, 127–28 (2d Cir. 2002).

A. Movants fall far short of establishing the reasonableness of a court-ordered return of the seized property for multiple reasons. *First*, the Government must retain the devices because they contain evidence that may be used in the Government's prosecution of Mr. Perez-Lugones. "The United States' retention of the property generally is reasonable if it has a need for the property in an investigation or prosecution." *Ramsden v. United States*, 2 F.3d 322, 326 (9th Cir. 1993); *see also United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("[A] Rule 41(g) motion is properly denied if . . . the government's need for the property as evidence continues." (citation omitted));

United States v. Garcon, 406 F. App'x 366, 370 (11th Cir. 2010) ("[T]he government was not obligated to return . . . items . . . needed as evidence in the event that Garcon[] . . . is able to obtain a new trial.").

This rule is consistent with the general principle that the Government's retention of property is reasonable if the Government needs the property for an ongoing investigation or prosecution. *See Krimstock v. Kelly*, 464 F.3d 246, 251–52 (2d Cir. 2006) (noting that the Government's need to retain evidence should be evaluated for reasonableness and that the Government may have a continuing need to hold evidence); *United States v. Christie*, 717 F.3d 1156, 1167 (10th Cir. 2013) (holding that after the Government found incriminating evidence on a computer pursuant to a search warrant, it was "presumptively entitled" to retain the computer until the criminal proceedings terminated); *see also* Fed. R. Crim. P. 41 advisory committee's note to 1989 amendment ("If the United States has a need for the property in an investigation or prosecution, its retention of the property generally is reasonable.").

The Government has probable cause to believe that the devices contain evidence of Mr. Perez-Lugones's alleged offenses. Those devices therefore "may hold evidentiary value to the [G]overnment" as they prosecute him. *United States v. Figueroa*, 2022 WL 2873226, at *3 (S.D.N.Y. July 21, 2022). Indeed, the entry of a warrant constitutes a "judicial determination" that the devices "contain relevant information, or are relevant themselves," to the investigation and prosecution of Mr. Perez-Lugones. *Id.*

It is also reasonable and lawful for the Government to search the entirety of the devices while identifying evidence. As with most information seized in search warrants, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen v. Maryland*, 427 U.S. 463,

482 n.11 (1976); *see also United States v. Crouch*, 648 F.2d 932, 933–34 (4th Cir. 1981) (acknowledging that officers may conduct "some cursory reading" of documents discovered during a search to determine their relevance to the crime providing the basis for the search). The same is true when a warrant authorizes the search of a computer for responsive information. Investigators cannot be expected to predict "where on the computer the evidence will be found." *United States v. Kamara*, 2023 WL 8357946, at *8 (E.D. Va. Dec. 1, 2023) (citation omitted). After all, the responsive information does not come labeled, as the Fourth Circuit noted when it said that the owner of a computer who is engaged in criminal conduct "will not label his files to indicate their criminality." *United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010); *accord United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006) ("Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.").

No one disputes that investigators had probable cause to believe that Ms. Natanson's devices contained evidence, including in the form of classified information. But those investigators "had no way of knowing when they applied for the warrant exactly . . . *where* [she] had placed the evidence on her computer." *United States v. Cobb*, 970 F.3d 319, 329 (4th Cir. 2019). "[B]ecause the designation or labeling of files on a computer can easily be manipulated to hide their substance," *Williams*, 592 F.3d at 522, the valid warrant here "impliedly authorize[s] officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file falls within the scope of the warrant's authorization"—*i.e.*, whether it related to Perez-Lugones's violations, *Cobb*, 970 F.3d at 329 (quoting *Williams*, 592 F.3d at 521–22). Thus, well-established Fourth Amendment principles make clear that the Government has a legitimate interest in the entirety of Ms. Natanson's seized devices.

Second, the Government has probable cause to believe these devices contain classified information that cannot be returned to Movants, and it is therefore reasonable not to return those devices now. The Government has an obvious and compelling interest in protecting classified information—national security depends upon it. *See United States v. Sterling*, 724 F.3d 483, 508 (4th Cir. 2013) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (quoting *Haig v. Agee*, 453 U.S. 280, 307 (1981)). The Government therefore has "broad discretion to determine who may have access to" classified information and an obligation to protect against unauthorized disclosure. *Dep't of Navy v. Egan*, 484 U.S. 518, 529 (1988). "The Government . . . may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it." *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cit. 1984), *vacated on other grounds*, 780 F.2d 1102 (4th Cir. 1985). That unique interest in classified information provides more than a legitimate reason to retain the devices until the Government can review them. *See Egan*, 484 U.S. at 527 ("This Court has recognized the Government's compelling interest in withholding national security information from unauthorized persons in the course of executive business." (citation omitted)).

Movants do not have the same unique interest in classified information given they are not the entity constitutionally designated to classify "information bearing on national security," *Egan*, 484 U.S. at 527. Nor can the Court presume that Movants can identify classified information given the allegations here that Perez-Lugones allegedly pasted classified information into Microsoft Word documents and removed classified headers from various classified documents before doing so. *See* Indictment ¶¶ 14, 16, 18, 22; *see also* ECF No. 9-7 ¶ 17. The Government has also alleged some of his screenshots altered certain portions of the classified information that he sent to Ms. Natanson. *See* Indictment ¶¶ 14–15. It does not matter if Movants' counsel have security

clearances, they lack the requisite "need to know the information." Exec. Order 13,526 § 4.1(a)(3); *see also United States v. Daoud*, 755 F.3d 479, 484 (7th Cir. 2014) (rejecting argument "that any concerns about disclosure were dissolved by defense counsel's security clearances . . . as if disclosing state secrets to cleared lawyers could not harm national security. Not true."); *Egan*, 484 U.S. at 529 ("Predictive judgment of this kind must be made by those with the necessary expertise in protecting classified information.").

"Generally, a Rule 41[(g)] motion is properly denied if the defendant is not entitled to lawful possession of the seized property [or] the property is contraband or subject to forfeiture . . . ." *Chambers*, 192 F.3d at 377 (citation omitted); *see also Hill v. United States*, 296 F.R.D. 411, 414 (E.D. Va. 2013). "[C]lassified information . . . is considered contraband." *Search Warrant for the Person of John F. Gill and the Premises Located at 28 West Side Drive*, 2014 WL 1331013, at *2 (E.D.N.C. Mar. 31, 2014). Thus, "a defendant is not entitled to the return of property that has classified information stored on it." *United States v. Montgomery*, 2021 WL 615401, at *5 (S.D. Ohio Feb. 17, 2021).

Courts have repeatedly denied Rule 41(g) motions where they seek the return of classified materials. *See, e.g.*, *John F. Gill*, 2014 WL 1331013, at *3 ("Because the government has established that the iPhone contains classified information and that the iPhone cannot be returned to petitioner because of the level of classified information found on the iPhone and the government's regulations requiring disposal of such a contaminated item, this court denies petitioner's motion for return of his property with prejudice."); *Montgomery*, 2021 WL 615401, at *6 ("[T]he items on Exhibit D contain classified/secret information and therefore belong to the United States, not Mr. Montgomery."). As a district judge on this Court recognized, returning

property of a "classified nature" to a person under Rule 41(g) "would pose potential security risks." *United States v. Hoffman*, 2018 WL 5973763, at *2 (E.D. Va. Nov. 14, 2018)

As an example, in December 2005, the New York Times published a series of articles describing alleged NSA activities including warrantless wiretaps. *See Roark v. United States*, 2015 WL 2085193, at *1 (D. Or. May 4, 2015). The Department of Justice investigated to identify the sources responsible for the disclosure of classified information contained in the articles. *See id.* A former congressional staffer named Diane Roark was identified as a subject of the investigation. *See id.* The Government obtained a search warrant for Roark's residence and seized computers, hard drives, and other electronic items. *See id.* Three other individuals later admitted to being the sources of the leaked information, and Roark sought the return of her media. *See id.* at *1–2. The district court denied Roark's Rule 41(g) motion. The Government submitted a declaration establishing that Roark's devices contained classified information. *See id.* at *3. The court thus refused to compel the Government to provide it to her. *See id.* Roark proposed that her own expert should use software to redact other sensitive information from her electronic devices. *See id.* at *6. The court declined to order this as well, recognizing that "the government has no obligation to cede classification authority to a third party, and this Court is in no position to compel the government to do so." *Id.*

The Government's interests in confidentiality are especially significant for Top Secret and Secret information of the type Mr. Perez-Lugones is accused of stealing from the Government, the disclosure of which could be reasonably expected to cause "exceptionally grave damage" and/or "serious damage" to national security. 18 C.F.R. § 3a.11(a)(1), (2). And some of the information stolen by Perez-Lugones is Sensitive Compartmented Information, meaning it relates to intelligence sources, methods, and analytical processes that cannot be disclosed outside of a SCIF.

See Sensitive Compartmented Information Facilities, Intelligence Community Directive 705 (Feb. 20, 2024), https://www.dni.gov/files/documents/ICD/ICD-705-SCIFs.pdf. Disclosure of that information "could cause irreparable harm to the United States." *Sensitive Compartmented Information Nondisclosure Agreement*, Form 4414, at 1; *see also* 28 C.F.R. § 17.18(a) (Sensitive Compartmented Information "is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods."). Should the Court need further detail, the Government's classified, *ex parte* declaration describes how continued proliferation of the information removed by Mr. Perez-Lugones harms national security.

B. Movants admit that "the test is one of 'reasonableness under all of the circumstances." Mot. 11 (quoting Fed. R. Crim. P. 41 advisory committee's note to 1989 amendment). Yet, they never connect their argument to Rule 41(g)'s reasonableness standard. Movants instead focus on attempting to demonstrate the alleged unlawfulness of the search and seizure. The Government's execution of the warrant was lawful, but even if there were a defect, that fact would not permit the Court to grant the motion. "[T]he judge . . . does not have to decide the legality of the seizure in cases involving contraband which, even if seized illegally, is not to be returned." Fed. R. Crim. P. 41 advisory committee's note to 1972 amendment. Regardless of Movants' First Amendment assertions, the Government cannot hand over devices that it has probable cause to believe contain government secrets of the most sensitive sort.

In any event, the search warrant's execution was lawful. The fundamental facts are undisputed: Movants do not argue that the acts Mr. Perez-Lugones has been accused of are not crimes. They do not dispute that Ms. Natanson's communications with Mr. Perez-Lugones are evidence relevant to the Government's prosecution. They do not dispute that there was probable

cause for the warrant executed at Ms. Natanson's residence. And they do not argue that the devices seized are free from classified material.

Movants instead rest on a limitless theory of the First Amendment that insulates journalists from lawful search warrants, even though the Supreme Court has rejected that anything more than the usual "preconditions for a warrant" are needed to protect "against the harms that are assertedly threatened by warrants for searching newspaper offices." *Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978). According to Movants, the Government's seizure of electronic devices containing journalistic communications and work product is a prior restraint on the exercise of a First Amendment right. But prior restraints are actions "*forbidding* certain communications when issued *in advance* of the time that such communications are to occur." *Alexander v. United States*, 509 U.S. 544, 550 (1993) (quoting M. Nimmer, Nimmer on Freedom of Speech § 4.03 (1984) (second emphasis added)). For example, a judicial order that prohibits local news outlets from future reporting about events in an open courtroom is a prior restraint because it imposes "an immediate and irreversible sanction" that "freezes" speech, rather than simply chilling it. *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 545 (1976). In other words, a prior restraint occurs when a law, regulation, or judicial order blocks speech "in advance of its actual expression." *Citizens United v. Schneiderman*, 882 F.3d 374, 386 (2d Cir. 2018) (citation omitted); *see also Ward v. Rock Against Racism*, 491 U.S. 781, 795 n.5 (1989) (prior restraint when regulations that "authorize[] suppression of speech *in advance of* its expression").

Movants claim the execution of the search warrant resulted in a prior restraint because it "commandeered Natanson's reporting records and tools, thereby preventing her" from contacting sources and "impairing her ability to publish the stories she otherwise would." Mot. 12; *see also id.* at 12–17. Their claim is factually and legally wrong. No court has entered an order prohibiting

Ms. Natanson "from engaging in any expressive activities in the future," nor has the Government "require[d] [her] to obtain prior approval for any expressive activities." *Alexander*, 509 U.S. at 550–51. If she wishes to publish a story tomorrow, nothing stops her from doing so. She can also continue conversations with her current sources without any advance prohibition by the Government. *See Hill v. Colorado*, 530 U.S. 703, 734 (2000) (rejecting prior-restraint challenge where "absolutely no channel of communication is foreclosed. No speaker is silenced. And no message is prohibited"). Movants assert that "[w]ithout her devices," Ms. Natanson "literally cannot contact" her sources, and that since her devices were seized, her Signal account's messages "ha[ve] dropped to zero." Mot. 4, 14. But they neglect to note that Ms. Natanson's X and Bluesky accounts broadcast her email address and "NEW SIGNAL @HannahNatanson.2026." Hannah Natanson, Bluesky, https://bsky.app/profile/hannahnatanson.bsky.social (last accessed Jan. 30, 2026); Hannah Natanson, X, https://x.com/hannah_natanson?lang=en (last accessed Jan. 30, 2026).

Alexander also shows that despite Movants' suggestion that Ms. Natanson cannot publish without her devices, this does not amount to a prior restraint. In *Alexander*, the Supreme Court held that an order directing forfeiture of an adult bookstore owner's "specific assets that were found to be related to" previous wrongdoing was not a prior restraint. *Alexander*, 509 U.S. at 551. Nothing about the forfeiture order imposed a "legal impediment to" the owner's ability to "engage in any expressive activity he cho[se]." *Id.* He could open a new store, for example; he just could not finance that enterprise with certain assets. *See id.* So too here—Ms. Natanson has been deprived under a valid warrant of certain assets that the Government has probable cause to believe contain evidence of a crime. But the Government has not blocked her future publication. She remains free to do that.

Movants suggest otherwise by likening Ms. Natanson's situation to police seizures of cameras that bystanders used to film police activity. *See* Mot. 12–13. Those cases are inapposite because those seizures were directed at the content of the expression at issue. In *Channel 10, Inc. v. Gunnarson*, officers seized a camera and refused to return it until the officer could check "whether the film contained information detrimental to the prosecution." 337 F. Supp. 634, 636 (D. Minn. 1972). Similarly, the officer in *Garcia v. Montgomery County* seized film of police activities "for the purpose of preventing the dissemination of the information on the recording"—*i.e.*, because of what the recording showed. 145 F. Supp. 3d 492, 510 (D. Md. 2015).

That is not the case here. The Government did not seize Ms. Natanson's devices because of the content of her future expression, but rather to recover "all records and information, including classified and/or national defense information" that the Government had probable cause to believe were in her possession and "relat[ed] to Aurelio Perez-Lugones, as evidence of violations of 18 U.S.C. § 793." ECF No. 9-5 at 5. The Government seeks only to obtain evidence in a criminal case, evidence that because of its classified nature is the Government's property. *See United States v. Fowler*, 932 F.2d 306, 309–10 (4th Cir. 1991). This case is therefore unlike cases where a prohibition *based on the content of the expression* was unlawful. *See Neb. Press Ass'n*, 427 U.S. at 542 (lower-court order enjoined reporting because its content would "tend to prevent a fair trial"); *Citizens United*, 882 F.3d at 386 (prior restraints occur when action suppresses speech "on the basis of the speech's content" (citation omitted)).

Movants likewise misplace their reliance on *Zurcher*. There, the Supreme Court observed that materials "presumptively protected" by the First Amendment "are not necessarily immune from seizure under warrant." 436 U.S. at 567. In fact, the Court said, "[n]ot every such seizure, *and not even most*, will impose a prior restraint." *Id.* Movants argue that this search warrant is

different from the one in *Zurcher* on various factual grounds, including the more limited disruption to newsgathering activities in *Zurcher* and the notice provided by Movants' counsel in the immediate aftermath of this seizure. *See* Mot. 13–14. But those details are not salient to *Zurcher*'s holding, which is that members of the press do not receive a special constitutional exemption from the demands of a valid search warrant and that, therefore, executing a valid warrant to seize newsgathering materials does not create a prior restraint. Here, the Government had a valid warrant, and there is no order or other action expressly forbidding Movants from future publication. Thus, there is no prior restraint.

Movants assert that the solution is a subpoena instead of a search warrant. *See* Mot. 11. That suggestion ignores the obvious risk that evidence could be lost either through a failure to preserve expiring Signal messages or bad faith conduct. The claim that the Government should have trusted Movants to preserve their documents and allowed them to segregate classified information and other evidence of Mr. Perez-Longones's crimes is difficult to square with the record. As the Rozhavsky Declaration explains, Ms. Natanson misled investigators about the devices that were seized. She misrepresented to officers that the devices could not be unlocked with biometrics, possibly in order to prevent the Government from reviewing materials within the scope of the search warrant. *See* Rozhavsky Decl. ¶¶ 25, 31, 32. The record confirms the correctness of the Government's choice to proceed with a search warrant.

At bottom, Movants seek a rule that places journalists outside the jurisdiction of search warrants because a seized device contains journalistic work product or communications. If accepted, the consequences are alarming. Just last year, a different Washington Post journalist had a search warrant executed at his home and his work computer seized. *See* Dep't of Just., *Award-Winning Journalist Arrested and Charged with Possession of Child Pornography* (June 27, 2025),

https://www.justice.gov/usao-dc/pr/award-winning-journalist-arrested-and-charged-possession-child-pornography. That journalist's work computer contained 11 videos depicting child sexual abuse material. *Id.* Movants would likely deem the execution of that search warrant no less a prior restraint to the extent that work computer also contained journalistic communications and draft work product.

That is not the law. The Supreme Court held long ago that the First Amendment does not exempt journalists "from the ordinary duty of all other citizens to furnish relevant information to a grand jury performing an important public function." *Branzburg v. Hayes*, 408 U.S. 665, 697 (1972); *see also Zurcher*, 436 U.S. at 565 (noting that the Framers "did not forbid warrants where the press was involved" despite being aware of historical struggles between the Government and the press). The Court also specifically rejected the notion that "the First Amendment protects a newsman's agreement to conceal the criminal conduct of his source." *Id.* at 692. And "the Supreme Court refused to recognize a reporter's privilege not to testify in criminal prosecutions about relevant evidence known to the reporter, regardless of whether the information was obtained during newsgathering." *In re Shain*, 978 F.2d 850, 852 (4th Cir. 1992) (citing *Branzburg*, 408 U.S. at 690); *see also Reps. Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1056 (D.C. Cir. 1978) ("[T]he First Amendment affords no procedural or substantive protection beyond that afforded by the Fourth and Fifth Amendments."). This Court should reject Movants' demand to return lawfully seized devices that the Government has probable cause to believe contain classified material as evidence of Mr. Perez-Longones's alleged crimes.

II. The Standstill Order Should Be Dissolved, and the Government Should Be Permitted to Review Evidence With a Filter Team.

As a fallback to their extraordinary request for the return of devices containing government secrets, Movants ask the Court to forbid the Government from reviewing all materials contained

in the seized devices. They would have this Court instead search for and review highly classified information and determine each document's relevance to Mr. Perez-Lugones's prosecution. That approach is unwarranted as the Government intends to design a filter protocol to ensure that privileged materials are shielded while also protecting classified information and segregating materials within the scope of the warrant.

Filter teams are a well-accepted practice that is "respectful of, rather than injurious to, the protection of privilege." *United States v. Avenatti*, 559 F. Supp. 3d 274, 282 (S.D.N.Y. 2021) (citation omitted). This is particularly true when, as here, the information is "already in the government's possession." *Id.* (citation omitted). In reviewing the information seized through this search warrant, the Government intends to: (1) segregate information covered by the attorney-client and work product privileges; (2) maximize the privacy of Ms. Natanson's First Amendment-related information; (3) avoid violating the Privacy Protection Act; and (4) otherwise ensure that the team prosecuting Mr. Perez-Lugones sees only non-privileged information that falls within the scope of Attachment B. This filter protocol is overinclusive. Although the Government is not required to segregate First Amendment- and PPA-related information at this time, it has decided to do so.

Under the Government's plan, the filter team—consisting of an Assistant U.S. Attorney and multiple FBI agents—would review information from October 1, 2025, to January 14, 2026, that includes Mr. Perez-Lugones's name and information sent to or received from him. The filter team will take reasonable measures to determine whether a file contains information regarding Perez-Lugones, including opening files to scan for the name or information. Information within the scope of Attachment B would be saved separately from information on the remainder of the devices. The review and segregation process will be memorialized afterwards in a memo from the

filter team to the prosecution team, along with the number of files reviewed, the number of files sent to the prosecution team, and the number of files segregated from the prosecution team.

The protocol would direct the filter agents doing the search to formulate a list of keyword terms to expedite the search, including known identifiers associated with Mr. Perez-Lugones, a list of terms known to have been used in communications between him and Ms. Natanson, and language from the classified reports that he purloined and that were published. Information found within the scope of Attachment B would be segregated as potentially responsive, subject to any privilege.

The filter team would then review the responsive documents for attorney-client and work product privilege using a list of search terms across the seized material to isolate potentially privileged materials. That list would include search terms provided by Movants' counsel before the Court entered its Standstill Order. Information containing one of those search terms or hard copy materials there were either to or from an attorney would be segregated. All other materials would be considered "clean," *i.e.* within the scope of Attachment B and not subject to a valid privilege. At that time, the filter AUSA would review the "clean" information for anything that might be related to the First Amendment or subject to the PPA. Any information considered protected under either would be placed in the segregated materials.

Once the agents have completed their initial review, the Assistant U.S. Attorney on the filter team would then comprehensively review both sets of information. Once this review ends, clean information would be sent to the prosecution team. Segregated information would not be made available to the prosecution team. Otherwise, all information not deemed "clean" would be sealed and maintained in a way that the prosecution team cannot access them.

Movants' proposal that this Court should review the seized material in the first instance ignores the sensitivity of the classified information that has been seized. After executing a search warrant, "it is left to the government to determine . . . whether or not there is classified material." *John F. Gill*, 2014 WL 1331013, at *2. As explained *supra*, the Government must be the first to review the devices because only it has the expertise necessary to identify classified information. No less than the Movants, the Court is not the entity constitutionally designated to classify "information bearing on national security," *Egan*, 484 U.S. at 527, and it cannot be presumed to identify classified information given the allegations that Mr. Perez-Lugones pasted classified information into Microsoft Word documents and removed classified headers from various classified documents before doing so and that his screenshots altered classified information before he sent it to Ms. Natanson. *See* Indictment ¶¶ 14, 16, 18, 22; *see also* ECF No. 9-7 ¶ 17; *see also Egan*, 484 U.S. at 529 ("Predictive judgment of this kind must be made by those with the necessary expertise in protecting classified information.").

Movants' proposal is also unworkable. They highlight the potentially enormous quantity of information seized, suggesting the volume of documents might approach that of the entire Library of Congress's printed collection. *See* Mot. 4. For the Government, time is of the essence. Mr. Perez-Lugones is now detained, and his trial must occur quickly pursuant to the Speedy Trial Act. *See* 18 U.S.C. § 3161(c)(1). The Government is therefore on the clock to obtain and review all evidence relevant to that trial so that it can protect Mr. Perez-Lugones's rights in the underlying criminal case.

Movants' invocations of a qualified reporter's privilege, the Privacy Protection Act, and attorney-client privilege do not require a continuation of the Standstill Order. The Fourth Circuit has held that there is no so-called "reporter's privilege" in criminal cases. *Sterling*, 724 F.3d at

492–99. Movants say that there is still a privilege over "material that is irrelevant to the prosecution." Mot. 21. But that assumes the result of the Government's review: It is still too early to know what information on the devices is truly irrelevant. As discussed above, the Government is entitled to search the devices in their entirety for information (subject to Attachment B), and return should not be ordered until it can make that determination. But, in any event, the Fourth Circuit has rejected a reporter's privilege in criminal cases "so long as the subpoena is issued in good faith and is based on a legitimate need of law enforcement." *Sterling*, 724 F.3d at 496. That logic applies to search warrants, which are driven by the same "compelling public interest in effective criminal investigation and prosecution" as a criminal subpoena. *Id.* at 498. Here, the Government had probable cause to believe the devices contained evidence of a crime, and it sought (and was granted) a valid search warrant on that basis. The warrant was not sought for harassment purposes or to seek information "implicat[ing] confidential source relationship[s] without a legitimate need of law enforcement." *Branzburg*, 408 U.S. at 710 (Powell, J., concurring). The Government has a need to locate evidence, and it sought a "legitimate, good faith" search warrant to that effect. *Sterling*, 724 F.3d at 499.

Similarly, the Privacy Protection Act does not provide a basis to return the devices now (or ever). Most fundamentally, the PPA authorizes only "a civil cause of action for damages" against the Government. 42 U.S.C. § 2000aa-6(a). That remedy is "exclusive," meaning Movants cannot invoke the PPA to compel return of the devices. *Id.* § 2000aa-6(d). And, in any event, it is premature to invoke that statute. In a case cited by Movants, the Sixth Circuit has acknowledged that "when police execute a search warrant for documents on a computer, it will often be difficult or impossible . . . to separate the offending materials from other 'innocent' material on the computer." *Guest v. Leis*, 255 F.3d 325, 341–42 (6th Cir. 2001). Accordingly, "when protected

materials are commingled" with criminal evidence, courts should "not find liability under the PPA for seizure of the PPA-protected materials." *Id.* at 342. So too here—even if the PPA may authorize returning the devices, it is premature to do so under that statute.

Movants primarily rely on *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159 (4th Cir. 2019) (*Baltimore Criminal Defense Firm*). There, a magistrate judge issued a warrant authorizing a search for a lawyer's records concerning one specific client. *See id.* at 166. Government agents seized all 37,000 emails in the lawyer's inbox, including his correspondence with clients whose materials were not authorized to be seized. *See id.* at 166–67. Notably as well, some of those other clients were being investigated by the same United States Attorney's Office for unrelated crimes. *See id.* at 167. Simultaneously, the magistrate judge authorized *ex parte* a filter protocol under which a filter team would determine in the first instance whether materials were privileged under the attorney-client or work product privileges. *See id.* at 165–66. Materials deemed nonprivileged could be transmitted to the investigating team immediately, without a court order or consent from the lawyer. *See id.* at 166.

The Fourth Circuit held that the filter protocol was legally flawed. The Circuit objected first to the protocol's delegation to the Executive—"that is, the Filter Team—to make decisions on attorney-client privilege and the work-product doctrine." *Id.* at 177. According to the court, the resolution of such disputes "is a judicial function" that could only be performed by judicial officers. *Id.* at 176, 178. The Fourth Circuit also concluded that the magistrate should not have authorized the filter protocol *ex parte* before knowing what the Government had seized. *See id.* at 178–79. Had he conducted "adversarial proceedings" after knowing those details, including the sheer number of attorney-client correspondence seized, he could have been "fully informed of what was seized" and could have tailored the filter protocol accordingly. *Id.* at 178. "In these

circumstances," the Fourth Circuit ruled that the magistrate judge or a special master should have performed the privilege review of the seized materials. *Id.* at 181.

Baltimore Criminal Defense Firm does not control here. For one thing, the Fourth Circuit clearly limited that holding to the specific facts, noting that "[i]n th[ose] circumstances," a judicial officer must review for privilege. *Id.* As Judge Rushing explained in her concurrence, "the *unique* facts and circumstances of *this* case preclude *this* Filter Team operating under *this* Filter Protocol from reviewing the fruits of *this* search warrant." *See id.* at 183 (Rushing, J., concurring) (emphases added). The Fourth Circuit therefore did not establish that judicial officers must, as a general rule, perform a privilege review. *See Avenatti*, 559 F. Supp. 3d at 282 (noting the "unique" facts of *Baltimore Criminal Defense Firm*).

Those facts are not present here. First, this Court has not prematurely authorized a filter protocol *ex parte* before learning the results of the search warrant. Indeed, this Court plans to undergo the "sensible procedure[]" of an adversarial hearing before approving any filter team or protocol. *Baltimore Criminal Defense Firm*, 942 F.3d at 179. Moreover, the filter protocol in *Baltimore Criminal Defense Firm* allowed the Government to seek individual waivers from privilege holders (*i.e.*, clients of the law firm.) *See id.* at 180. The Government's filter protocol here includes no such provision that "demonstrate[s] a lack of respect for the attorney-client privilege." *Id.* at 180. Nor is this a case where a U.S. Attorney's Office is filtering out information related to other persons that the same office is investigating, as was the case in *Baltimore Criminal Defense Firm*. *See id.* at 172. And although Movants will likely argue that this seizure, like in *Baltimore Criminal Defense Firm*, is overinclusive compared to the warrant, that argument ignores the Government's probable cause to believe the devices contain evidence of a crime that, if further disclosed, could cause "exceptionally grave damage" and/or "serious damage" to the national

security. 18 C.F.R. § 3a.11(a)(1), (2) (explaining Top Secret and Secret designations). It is also premature: the Government has not yet been able to review for that evidence. And although *Baltimore Criminal Defense Firm* emphasized that "99.8 percent" of the seized material was unrelated to what the warrant authorized, 942 F.3d at 178, that case did not deal with evidence that might cause similar harm to national security.

Similarly, the interests at issue in this case are different and thus require a different result from *Baltimore Criminal Defense Firm*. That filter team was deficient in part because clients of the law firm held the attorney-client privilege, and "an adverse party's review of privileged materials seriously injure[d]" those privilege holders. *Id.* at 175. In contrast, the filter team here will be searching for, among other things, classified information, which is the property of the Government *See Fowler*, 932 F.2d at 309–10 (affirming charge under 18 U.S.C. § 641 for conversion of classified information because classified information was a "record" or "thing of value of the United States" (citation omitted)); *see also Wiebe v. Nat'l Sec. Agency*, 2012 WL 4069746, at *6 (D. Md. Sep. 14, 2012) ("The Government's interest in its own property that has not been released to the public is sufficient for purposes of Rule 41(g).").

Moreover, the Executive Branch's unique interest in any classified information that might be found is a key difference from the filter protocol in *Baltimore Criminal Defense Firm*. The privileges there were the attorney-client and work product privileges held by the law firm and its clients such that the Government's review would, according to the Fourth Circuit, injure those privilege holders. *See Baltimore Criminal Defense Firm*, 942 F.3d at 175. The same privileges are present here, but in a vastly different context. The Executive Branch has particular equities in classified information that, unlike those privileges, "can neither be claimed nor waived by a private party." *United States v. Reynolds*, 345 U.S. 1, 7 (1953) (footnotes omitted); *see also Wikimedia*

Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., 14 F.4th 276, 295 (4th Cir. 2021) (the Executive Branch can "protect information whose secrecy is necessary to its military and foreign-affairs responsibilities" (citation omitted)). Those equities should allow the Government to use a filter team here to protect its unique interest that no one else can hold. Any other procedure would damage that interest.[3]

The unique nature of this filter team also does not require the court to perform the initial review. In the area of foreign affairs, "courts have traditionally shown the utmost deference to Presidential responsibilities." *Egan*, 484 U.S. at 530 (citation omitted); *see United States v. Zubaydah*, 595 U.S. 195, 205 (2022) ("[I]n assessing the Government's claim that disclosure may harm national security, courts must exercise the traditional reluctance to intrude upon the authority of the Executive in military and national security affairs." (quoting *Egan*, 484 U.S. at 530)). To cut the Executive out of this review for classified information implicating foreign affairs—as Movants suggest—would contradict the Supreme Court's admonition that predictive judgments about the protection of classified information "must be made by those with the necessary expertise" in that subject, *i.e.* the Executive. *Egan*, 484 U.S. at 529. None of these considerations was present in *Baltimore Criminal Defense Firm*, so that decision cannot be a blueprint for this case. In sum, the Government should be permitted to do an initial review for privileges as delineated in the filter protocol.

[3] The presence of this interest also distinguishes this case from the procedures used and rejected in *United States v. Rayburn House Office Building*, 497 F.3d 654 (D.C. Cir. 2007), a decision on which Movants rely. *See* Mot. 25. The procedures there were deemed deficient because they provided no opportunity for a Member of Congress to assert his own legislative privilege. *See Rayburn*, 497 F.3d at 662. In contrast, the Government here would be able to assert in the first instance its own unique interest in the reviewed information.

III. If This Court Grants The Motion, The Government Requests A Stay Pending Appeal.

For all the reasons above, the pending 41(g) motion should be denied. If the Court ultimately rules otherwise, the Government requests that the Court stay that order pending the Government filing objections to it pursuant to 28 U.S.C. § 636(b).

CONCLUSION

The Court should deny the Motion to Intervene and for Return of Property.

Dated: January 30, 2026

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General
Civil Division

JOHN A. EISENBERG
Assistant Attorney General
National Security Division

ERIC J. HAMILTON
Deputy Assistant Attorney General
Civil Division, Federal Programs Branch

/s/ Joseph E. Borson
JOSEPH E. BORSON (Va. Bar No. 85519)
Assistant Branch Director
Civil Division, Federal Programs Branch

CHRISTIAN DIBBLEE
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Washington, D.C. 20005
Tel: (202) 514-1944
Email: Joseph.Borson@usdoj.gov

Counsel for the United States