UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

In the Matter of the Search of the Real Property and Premises of Hannah Natanson,	No. 1:26-sw-00054-WBP

OBJECTIONS TO MAGISTRATE JUDGE'S MEMORANDUM OPINION AND ORDER ON THE MOTION FOR RETURN OF PROPERTY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Rules

Regulations

Other Authorities

INTRODUCTION

The magistrate judge erred when, in an order partially granting a motion for return of property under Federal Criminal Rule 41(g), he took the position that the magistrate judge—rather than the Executive Branch—should search the devices of Ms. Hannah Natanson, a reporter for the Washington Post. *See* ECF No. 62 (Op.). The magistrate judge's approach violates the Constitution and Supreme Court precedent, and it creates a series of logistical and security concerns. A court's role in reviewing a search warrant application is to be a "neutral[] and detach[ed] . . . judicial officer," and not "a member, if not the leader, of the search party which [is] essentially a police operation." *Lo-Ji Sales, Inc. v. New* York, 442 U.S. 319, 327 (1979). Moreover, when classified information is at risk of further dissemination, as it is here, the search of the devices must be executed by an authority with the "necessary expertise" in identifying classified material and "protecting" this compelling government interest. *Dep't of the Navy v. Egan*, 484 U.S. 518, 529 (1988). That authority and expertise belong to the Executive Branch, not the Judiciary. *Id.* at 527–29.

The Court should overrule the magistrate judge's decision, deny the underlying motion in full, and authorize the Government to search the seized devices used a filter protocol, a search and seizure that was authorized by a valid search warrant signed by the magistrate judge. The execution of a search warrant and the conduct of the subsequent search is a quintessential function of the Executive and, in a unique case like this, must be conducted by professionals with expertise in identifying and handling classified information. With respect, the magistrate judge lacks that ability. Moreover, the Government's contemplated search of the devices is lawful. The Government sought a search warrant that, under controlling precedent, was sufficiently particular with respect to the property to be searched and the items to be seized. The Government, then, was the one to execute that warrant and conduct that search. The First Amendment implications of this

case do not counsel otherwise. As a reporter, Ms. Natanson is subject like any other citizen to a legitimate use of criminal legal process in a criminal investigation, such as this search warrant. *See Branzburg v. Hayes*, 408 U.S. 665, 682–83 (1972). The magistrate judge's path forward instead creates a reporter-specific search procedure that binding precedent clearly rejects and that is unjustified by Ms. Natanson's First Amendment activities.

This Court should adopt the Government's original proposal to the magistrate judge by allowing a filter team to review the seized devices for materials that are potentially privileged or protected by the First Amendment and/or the Privacy Protection Act (PPA). That solution is routine and complies with circuit precedent.

BACKGROUND

I. Arrest of Aurelio Perez-Lugones and Execution of The Search Warrant

On October 31, 2025, the Post published an article containing classified information from a Government intelligence report. *See* ECF No. 35-1, Decl. of Roman Rozhavsky ¶¶ 6, 12. The intelligence report was classified at one of the highest levels: TOP SECRET//SCI//NOFORN. *See id.* ¶ 11.[1] Ms. Natanson co-authored that article. *See id.* ¶ 12. The Federal Bureau of Investigation (FBI) then began to investigate the unauthorized disclosure of the classified material. *See id.* ¶ 5.

A government contractor named Aurelio Perez-Lugones became a suspect. He 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-

[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 "SCI" marking indicates that it relates to intelligence sources, methods, and analytical processes. The "NOFORN" marking indicates that information is not releasable to foreign nationals and can be disseminated only to U.S. nationals.

Lugones had allegedly viewed the intelligence report on which the Post 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.* The Post's article omitted the same portion of the intelligence report that was rendered illegible in the screenshot. *See id.* ¶ 12.

This pattern repeated multiple times—classified information would appear in the Post after 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, which the application had placed there for tracking purposes. *See id.* ¶ 18. And in another instance, he allegedly made handwritten notes while viewing classified reports on his work computer and then removed those notes from the SCIF, the specially equipped environment for storing, reviewing, and discussing 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 Post 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, and with his consent, the FBI reviewed messages exchanged between him and Ms. Natanson via

[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." *Id.* § 3a.11(a)(3).

Signal, *see id.*, a messaging application 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 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. That review also revealed that Perez-Lugones had sent photographs of the documents that had been the source of classified material in the articles as well as audio messages about those documents. *See id.* ¶¶ 19–20. Around this time, and pursuant to a court-authorized search, the FBI located in Perez-Lugones's lunchbox a hard copy printout of a SECRET//NOFORN document. *See id.* ¶ 21. The classification header had been removed from that printout, and agents later found the excised header in a trash can at Perez-Lugones' workplace. *See id.* ¶¶ 21–22. A 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), the Espionage Act. *See* ECF No. 25, *United States v. Perez-Lugones*, No. 26-cr-30 (D. Md. Jan. 22, 2026) (Indictment).

Days after Perez-Lugones's arrest, the Government sought warrants in this District to search Ms. Natanson's person, vehicle, and residence to recover electronic devices the Government had probable cause to believe contained classified material sent by Perez-Lugones. *See* Nos. 26-sw-52 (vehicle), 26-sw-53 (person), 26-sw-54 (residence). Magistrate Judge William Porter found that the Government had established probable cause, and he issued those search warrants. Attachment B to the warrant for Ms. Natanson's residence authorized seizure of "[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 (Att. B) at 5 (footnotes omitted).[3] The items authorized to be seized were "limited to all records and information, including classified and/or national defense information, from the time period October 1, 2025, to the [date of the warrant]," constituting "records received from or relating to Aurelio Luis Perez-Lugones, as evidence of violations of 18 U.S.C. § 793." *Id.* Attachment B also authorized 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. The warrant further authorized investigators to compel Ms. Natanson to use biometrics—such as facial recognition or her fingerprint—to unlock the devices. *Id.* at 7.

FBI agents announced themselves at Ms. Natanson's house and executed the warrant on January 14, 2026. *See* Rozhavsky Decl. ¶¶ 24–25. They located a 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. The iPhone's display noted that it 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. They then discovered another MacBook Pro ("Work MacBook Pro"), *see id.* ¶ 29, which they were able to unlock using Ms. Natanson's fingerprint, *see id.* ¶ 31, even though she had previously said she did not use biometrics to open any of her devices, *see id.* ¶ 25.

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 items would need to be reviewed by a filter team of personnel who would not be part of the team investigating Perez-Lugones to scope the material under Attachment B and to protect against disclosure to the investigation team of not only privileged materials but also First Amendment

[3] All pincites to Attachment B are to the ECF pagination.

material not within the warrant's scope. *See id.* ¶ 34. The processing of all electronic devices that occurred immediately after their seizure was thus conducted by analysts and agents who were not (and will never be) associated with the investigation team. *See id.* The FBI's Computer Analysis Response Team (CART) was able to process the recorder and portable drive in full, *see id.* ¶ 37, and to create a limited partial image of the Work MacBook Pro, *see id.* ¶ 38. However, the other computer is password-protected and encrypted and therefore could not be imaged, *see id.* ¶ 36, and because the iPhone was in Lockdown mode, CART could not extract that device either, *see id.* ¶ 35.

II. The Rule 41(g) Motion and The Magistrate Judge's Decision

Around this time, the Post and Ms. Natanson (collectively, Movants) moved to intervene in the search warrant case and for return of the items under Federal Criminal Rule 41(g), which allows a "person aggrieved by an unlawful search and seizure of property or by the deprivation of property" to "move for the property's return." The Rule 41(g) motion sought return of all materials on the theory that the seizure was an impermissible prior restraint on Ms. Natanson's First Amendment activity. *See* ECF No. 9 at 12–17. The motion alternatively argued that, in the event the magistrate judge did not order return of all materials, it should supervise the process of returning those materials not within the scope of the warrant. *See id.* at 17–25. Movants also contended that the filter-team approach proposed by the Government to review the seized devices was inappropriate. *See id.* at 24–25. According to Movants, the devices should be returned so that Movants themselves could identify material responsive to the warrant and produce it to the Government. *See* ECF No. 40 at 7.

Movants simultaneously sought a separate "standstill order" to prevent the "review of any seized materials" pending adjudication of the Rule 41(g) motion. ECF No. 10-1 at 1. The magistrate judge entered an order directing that the Government "must preserve but must not

review any" of the seized materials. ECF No. 18 at 1. Out of an abundance of caution, the Government ceased all preservation efforts after entry of that order, including further imaging of the devices. *See* Rozhavsky Decl. ¶ 50. No other preservation efforts have occurred since.

The parties then briefed the Rule 41(g) motion. The Government argued that the issuance of a valid warrant conferred authority consistent with the Fourth Amendment to search the seized devices for evidence and further argued that the Government needed to conduct that review given the likely presence of classified material. *See* ECF No. 35 at 8–14. The Government also argued that the seizure did not constitute a prior restraint and that neither the First Amendment nor the Privacy Protection Act (PPA), 42 U.S.C. § 2000aa, required Movants to review the seized devices in the first instance. *See id.* at 14–19, 22–23. Finally, the Government proposed that its review should occur through a filter team. *See id.* at 19–21. The magistrate judge heard argument on the motion, and after that argument the Government filed a proposed filter team protocol under seal and served a redacted version on the Movants. The Government will file the same unredacted protocol under seal to this Court.

On February 24, the magistrate judge issued a memorandum opinion and order granting the motion to intervene and granting in part and denying in part the 41(g) motion. *See* Op. The magistrate judge affirmed that, per the warrant, the Government had "established probable cause to believe Movants possess evidence needed to prosecute" a violation of the Espionage Act. *Id.* at 7. The magistrate judge thus found that the Government had shown two legitimate reasons under Rule 41(g) for retention of the devices: their relevance to the pending prosecution and the likely presence of classified material on the devices. *Id.* at 17–18. The magistrate judge therefore refused to "return all devices and permit Movants to unilaterally identify material responsive to the search warrant." *Id.* at 18.

But the magistrate judge ruled he could not permit the Government to retain more than the information responsive to the warrant, citing the Movants' First Amendment equities. *Id.* at 16. After "[b]alancing Movants' First Amendment rights and newsgathering rights against the [G]overnment's compelling interest in its prosecution," *id.* at 18, the magistrate judge ruled that the filter team could not review "the entirety of a reporter's work product," *id.* at 19. Such a review would, he said, "authorize an unlawful general warrant" that is forbidden by the Fourth Amendment. *Id.* at 20. Rather, the magistrate judge would "conduct the review [him]self." *Id.* at 21. He reached this conclusion by relying on *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159 (4th Cir. 2019) (*Baltimore Criminal Defense Firm*). That decision rejected a filter-team approach where filter team agents themselves would have made decisions about which seized documents were privileged and, therefore, should not reach the investigative team. *See id.* at 172, 176. *Baltimore Criminal Defense Firm* supposedly "mandate[d]" that the magistrate judge perform the search himself. *Id.* at 21.

The magistrate judge granted the motion to intervene, granted the Rule 41(g) motion as to information outside the scope of the warrant, and denied the motion as to information within that scope. *Id.* at 22. The magistrate judge further ordered that he would "conduct an independent judicial review of the seized materials," and he rescinded the portion of the warrant "authorizing the government to open, access, review or otherwise examine any of Movants' seized data." *Id.* The standstill order remains in effect. *See id.*

The Government hereby objects to the magistrate judge's decision to order a judicial search of the seized material. The Government does not challenge his conclusion that Ms. Natanson and

the Post are not entitled to return of the devices now and that they cannot unilaterally review those devices themselves for responsive information.[4]

LEGAL STANDARD

This Court reviews the magistrate judge's order de novo because the Rule 41(g) motion is "dispositive of a claim or defense," namely Ms. Natanson's claim that the Government should return her property. Fed. R. Civ. P. 72(b)(1), (3), *see* Fed. R. Crim. P. 59(b)(1), (3) (same); *United States v. Hiya*, 2025 WL 2416733, at *3 (S.D.N.Y. Aug. 21, 2025) (reviewing de novo a Rule 41(g) motion related to a search warrant); *United States v. Collins*, 2012 WL 3537814, at *6 (N.D. Cal. Mar. 16, 2012) (treating a Rule 41(g) motion as dispositive for purposes of magistrate-judge jurisdiction).

Under Rule 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). "Rule 41(g) motions are treated as civil motions in equity." *United States v. Jones*, 2016 WL 8933629, at *2 (E.D. Va. July 26, 2016). Thus, they are "governed by equitable principles." *United States v. Johnson*, 2014 WL 2215854, at *6 (D. Md. May 28, 2014). Those include whether the Government has displayed a callous disregard for the constitutional rights of the movant. *See In re Hoover's Residence*, 2010 WL 7351761, at *2 (N.D. W. Va. Dec. 30, 2010). "[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). 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).

[4] The Government also does not object to the magistrate judge's decision to grant the motion to intervene.

ARGUMENT

I. The Magistrate Judge Erred When He Ordered a Judicial Search of the Devices.

The magistrate judge erred when he decided to supplant investigators and search the devices himself.[5] When investigators conduct a search under a warrant, the Government searches the property for items within the warrant's scope. The magistrate judge provided no valid reason to depart from that practice. And although he referred to his task as a "review" rather than a search, he clearly intends to look through the seized devices for evidence in the scope of the warrant. Op. 21. That is a search typically performed by the Government, as it should be here.

A. The Proposed Judicial Search of the Seized Material Is Inconsistent with the Separation of Powers, Including the Executive's Duty to Protect Classified Material, and Is Unworkable.

1. A Judicial Search Is Inconsistent with the Separation of Powers.

Once the Government obtained the signature of a magistrate judge regarding probable cause, the Government was authorized to search the devices for evidence within the warrant's scope. That is the process that should have commenced once the Government obtained the signature of this magistrate judge, but he took on the search duties himself.

The Supreme Court has specifically rebuked judges for participating in searches in this manner. In *Lo-Ji Sales*, a judge accompanied town investigators when they executed a search warrant on an adult bookstore. While there, the judge cursorily reviewed films and books and, "[w]hen he was satisfied that probable cause existed," he ordered investigators to seize the offending items. 442 U.S. at 323. Although the town argued that the judge's presence "ensured that no items would be seized absent probable cause," the Supreme Court held that the judge had

[5] The details of the magistrate judge's search protocol and procedure have not been determined, despite a hearing between the parties on that subject since his decision. *See* ECF No. 73. Notwithstanding these objections, the Government reserves all rights with respect to those details, once they are made available.

not "manifest[ed] that neutrality and detachment demanded of a judicial officer when presented with a warrant application for a search and seizure." *Id.* at 326. Instead, the judge had "allowed himself to become a member, if not the leader, of the search party which was essentially a police operation." *Id.* at 327.

This magistrate judge fell into the same trap when he decided to conduct a search himself to balance the Government's need to obtain evidence with the subject's First Amendment rights (in *Lo*-Ji, to sell allegedly obscene materials and, here, to write articles). The Constitution does not countenance this blending of Judicial and Executive powers. Rather, under Supreme Court precedent, it protects property owners "by interposing, *ex ante*" to a search, "the deliberate impartial judgment of a judicial officer" and "by providing, *ex post*, a right to suppress evidence improperly obtained and a cause of action for damages." *United States v. Grubbs*, 547 U.S. 90, 99 (2006) (citation omitted). The Fourth Amendment does not require or allow further judicial involvement during a warranted search by law enforcement for evidence of a criminal offense.

Moreover, his decision deprived the Government of its Executive power to determine how to investigate criminal wrongdoing. *See Cmty. for Creative Non-Violence v. Pierce*, 786 F.2d 1199, 1201 (D.C. Cir. 1986) (The "power to decide when to investigate, and when to prosecute, lies at the core of the Executive's duty to see to the faithful execution of the laws."). Not only that, but because the magistrate judge will be the only one that can establish the chain of custody for any evidence he identifies, he will need to testify about that evidence in any trial of Perez-Lugones. Given the difficulties associated with preparing a magistrate judge for testimony and cross-examining him, this Court should overrule the magistrate judge's decision now.

2. A Judicial Search Intrudes on the Executive's Duty to Protect Classified Information.

A judicial search is highly improper and impracticable in the context of crimes involving highly classified information. As the magistrate judge recognized, "no governmental interest is more compelling than the security of the Nation," and thus unauthorized disclosure of classified material must not occur. Op. 18 (quoting *United States v. Sterling*, 724 F.3d 482, 509 (4th Cir. 2013)). Disclosure of that material can be "reasonably expected to cause exceptionally grave damage" and/or "serious damage" to national security. 18 C.F.R. § 3a.11(a)(1), (2) (definitions of Top Secret and Secret). And some of the material involved is Sensitive Compartmented Information, meaning it relates to intelligence sources, methods, and analytical processes such that it cannot be housed or handled outside a SCIF. *See* 28 C.F.R. § 17.18(a). Disclosure of that material "could cause irreparable injury to the United States." *Sensitive Compartmented Information Nondisclosure Agreement*, Form 4414 (Rev. 12-2013), at 1. Moreover, classified material is the Government's property. *See United States v. Fowler*, 932 F.2d 306, 309–10 (4th Cir. 1991); *see also Wiebe v. National Sec. Agency*, 2012 WL 4069746, at *6 (D. Md. Sept. 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)."), *report and recommendation adopted*, ECF No. 78, No. 11-cv-3245 (D. Md. Mar. 27, 2013).

All parties to this dispute acknowledge that the seized devices likely contain classified material. Indeed, the warrant itself authorized seizure of records relating to Perez-Lugones "including classified and/or national defense information." Att. B at 5. That classified material is not only the Government's property regardless of form, *see Fowler*, 932 F.2d at 309–10, but 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," *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980). "The authority to protect such information falls on the President as head of the Executive Branch and as Commander in Chief." *Egan*, 484 U.S. at 527. That authority carries with it a "necessary expertise" in identifying classified material and "protecting" it. *Id.* at 529.

With respect, the magistrate judge does not possess that expertise nor the authority to determine what material is classified. He is not designated as an original classification authority under the relevant rules, *see* Exec. Order No. 13,526 § 1.3(a), and thus cannot be presumed to identify classified material. Nor will he have access to original classification authorities who could determine whether the devices contain unmarked classified material or national defense information. Those facts should legally foreclose his review here, particularly given allegations that Perez-Lugones deliberately obfuscated the classified nature of the information he disclosed, including by pasting classified material into Word documents and removing classified headers. *See* Indictment ¶¶ 14, 16, 18, 22. So, at least in this search, classified material likely will not have any markings. And even if the Government were to provide the magistrate judge some classified contextual information about the material in question beyond the classified filing already lodged with the magistrate judge (which the Government to be clear is not offering now), there will likely be other documents relating to Perez-Lugones that mention or excerpt snippets of classified material, such as notes about an oral conversation between him and Ms. Natanson. There is thus a serious risk that the magistrate judge would not recognize, identify, or discern when such documents partially contain classified material and would order return of classified material back to Movants when the magistrate judge concludes his review. *See* ECF No. 73 (Status Conf. Tr.) at 11:21-12:5 (raising this issue to the magistrate judge). Indeed, the magistrate judge might

perpetuate unauthorized disclosure of classified material that is not within the warrant's scope but is otherwise present and seizable under the plain-view doctrine. *See id.* at 20:21-25.

Government review would protect any such material. That is why, when the Government executes a search warrant, "it is left to the [G]overnment to determine . . . whether or not there is classified material." *Search Warrant for the Person of John F. Gill*, 2014 WL 1331013, at *2 (E.D.N.C. Mar. 31, 2014). That procedure will avoid the above issues and ensure protection of *all* classified material located on the devices.

Moreover, review by the magistrate judge and other court personnel creates the chance for unauthorized and unintended dissemination of classified material. That is not meant as a "slight" on the magistrate judge's reliability but rather as a recognition that, as the Fourth Circuit has acknowledged, each additional disclosure carries risks. *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1369 (4th Cir. 1975). Those risks should be managed by the Executive, which is constitutionally charged to make "[p]redictive judgment[s]" about the potential disclosure of classified material. *Egan*, 484 U.S. at 529; *see also CIA v. Sims*, 471 U.S. 159, 180 (1985) ("It is the responsibility of the [Executive], not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk."). Courts have "traditionally shown the utmost deference to Presidential responsibilities" in this area. *Egan*, 484 U.S. at 530 (citation omitted). Yet the magistrate judge's process would supplant the Executive's constitutional responsibility for reviewing for classified material.

It also is no answer that the magistrate judge and judicial staff possess security clearances. "[P]ossession of a security clearance alone is insufficient to access classified information." *United States v. Kotey*, 545 F. Supp. 3d 331, 337 (E.D. Va. 2021). Rules promulgated by the President require that individuals with an appropriate clearance can access classified material only if they

have a "need-to-know" that information. Exec. Order No. 13,526 § 4.1(a)(3). And those rules define "need-to-know" as "a determination *within the executive branch* . . . that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." *Id.* § 6.1(dd) (emphasis added). Here, "no agency has determined that [the Court may] have access to" this classified material, so they cannot access it as part of a review. *Wiebe*, 2012 WL 4069746, at *6.

This need-to-know requirement is significant. As multiple courts including the Fourth Circuit have recognized, disclosure of material to those without access to it "give[s] rise to added opportunity for leaked information." *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005). "It is not to slight judges, lawyers or anyone else to suggest that any such disclosure carries with it serious risk that highly sensitive information may be compromised." *Knopf*, 509 F.2d at 1369. That is precisely why the "need to know" requirement exists: to limit the disclosure of classified material only to those individuals who need to know it. "Disclosure to one more person," even one that is generally reliable and trustworthy, "may seem of no great moment, but information may be compromised inadvertently as well as deliberately." *Colby v. Halperin*, 656 F.2d 70, 72 (4th Cir. 1981).

3. A Judicial Search Is Logistically Unworkable.

In addition to the legal issues catalogued to this point, the magistrate judge's approach raises numerous logistical difficulties that could be obviated by Government review in the first instance, as discussed at a recent status conference. For example, the parties must determine the best place, platform, and technology for review given the classified material on the devices. *See* Status Conf. Tr. 11:1-4 (Government suggesting review at an FBI office in Manassas, Virginia); *id.* at 16:3-9 (magistrate judge suggesting review at the courthouse SCIF); *id.* at 16:10-21 (Movants suggesting review at DOJ's Litigation Security Group). Court personnel beyond the magistrate

judge will need security clearances before they begin the review and personal accounts on the review platform to ensure that investigators can track and identify for chain-of-custody purposes who accessed evidence, including classified material. *See id.* at 10:1-14.

At this time, investigators have not imaged multiple devices due to the magistrate judge's standstill order. *See id.* at 14:9-15:2. But even assuming the magistrate judge lifts that order, the process to image all remaining devices could take a matter of weeks, and then investigators will need to package those images onto a review platform suitable for classified material.[6] *See id.* at 30:12-21. And there remains some question over who the magistrate judge might order to do the forensic processing and chain-of-custody activities given Movants' concern with further FBI involvement, *see id.* at 36:21-22, even though the FBI's CART team is capable of ensuring retrieval and storage of electronic evidence in a forensically sound manner, *see id.* at 40:22-41:5. And of course review by the magistrate judge will take an unspecified amount of time while the underlying criminal indictment and investigation ticks forward.

Review by the Government obviates these serious practical problems. FBI personnel would be able to image the devices and package the resulting data for the filter team much more quickly than under the magistrate judge's process because those personnel already have the requisite expertise in how to image devices, extract data, and preserve it in a forensically sound manner, all while keeping an unbroken chain of custody. Indeed, these efficiencies are yet another reason why seized material is typically reviewed by the Government.

[6] It could take even longer depending on whether Ms. Natanson agrees to cooperate with investigators to grant access to some of the devices, notably the phone currently in Lock Down Mode. *See* Status Conf. Tr. at 31:21-32:2.

B. The Government's Seizure and Proposed Search of the Devices Comported with the Fourth Amendment.

The magistrate judge reached his determination, at least in part, to protect against what he conceived of as an "unlawful general warrant." Op. 20. According to him, the Government had "established probable cause to obtain only a small fraction of the material it seized" from Ms. Natanson and "acknowledge[d]" as much. *Id.* at 19. For that reason, according to the magistrate judge, "[a]llowing the government to search through the entirety of a reporter's work product—when probable cause exists for only a narrow subset—would authorize an unlawful general warrant." *Id.* at 19–20.

This conclusion was incorrect. The magistrate judge's opinion confused the place to be searched with items to be seized under the warrant. A warrant must "particularly describ[e] the place to be searched and the persons or things to be seized." *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (quoting U.S. Const. amend. IV). A warrant meets the latter requirement by "identifying the items to be seized by reference to a suspected criminal offense" or "describing them in a manner that allows an executing officer to know precisely what he has been authorized to search for and seize." *Id.* at 863. The Fourth Circuit has applied these principles to computer searches, recognizing that the complexity of electronic devices and the large amount of information contained therein may require searches that will expose all or most of a computer's content to some sort of review to identify items subject to seizure under the warrant. *See United States v. Williams,* 592 F.3d 511, 521 (4th Cir. 2010) ("[T]he warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."); *United States v. Cobb*, 970 F.3d 319, 331–32 (4th Cir. 2020) (same). It is therefore important to maintain the "distinction between what may be searched and can be seized." *United States v. Zelaya-Veliz*, 94 F.4th 321, 337 (4th Cir.

2024). A warrant for a digital device can specifically identify and authorize a *search* of property that contains both evidence of a crime and innocuous material. *See, e.g.*, *Williams*, 592 F.3d at 522. If that device contains "a wide swath of personal information" outside the warrant's scope, the warrant is still sufficiently particularized where "the scope of the seizure it authorized was limited to evidence of enumerated offenses," *Zelaya-Veliz*, 94 F.4th at 337.

The warrant here is therefore sufficiently particular. It identifies Ms. Natanson's devices as the property to be searched and limits any seizure to evidence of Perez-Lugones's crimes from within a particular date range. *See* Att. B at 5. The warrant thus appropriately "confined the executing officers' discretion," *Cobb*, 970 F.3d at 328, by permitting them to seize only "the fruits, evidence, or instrumentalities of violations of enumerated federal statutes," *Zelaya-Veliz*, 94 F.4th at 337. That is not a general warrant according to binding precedent.

The magistrate judge's opinion did not address that precedent, even though the Government raised some of it before him. *See* ECF No. 35 at 10. The cases make clear that when the Government establishes probable cause to believe that an electronic device contains evidence of a crime, the Government can conduct a reasonable search for that evidence. As for the Government's "acknowledg[ment]" that it "established probable cause to obtain only a small fraction of the material it seized," Op. 19, that is necessary when there is no other way to search for the evidence contained on these devices. *See* Fed. R. Crim. P. 41(e)(2)(B) (authorizing physical seizure of devices to search for information that is subject to seizure). Indeed, the magistrate judge's focus on the harms from a Government search of "the entirety of a reporter's work product," implies that, but for that First Amendment consideration, this would not be a general warrant. Op. 19. And the magistrate judge tacitly recognized the propriety of this warrant. If it were a general warrant when he signed it, his unilateral and unrestrained search would do nothing to cure that

unconstitutionality. *See Marron v. United States*, 275 U.S. 192, 195–96 (1927) ("The effect of the 4th Amendment is to put *the courts of the United States* and federal officials . . . under limitations and restraints as to the exercise of [their] power and authority[.]" (emphasis added and citation omitted)).

In any event, the magistrate judge also mischaracterized the Government's proposed review. Far from searching "the entirety of [Ms. Natanson's] work product," Op. 19, the Government's proposed filter team would provide the investigatory team only information falling within the date range specified by the warrant and would use search terms to identify responsive information. And although not all information within the scope of Attachment B can be located by keyword searches, the Government proposes using reasonable measures to identify that other information.[7] The warrant itself authorizes the use of such "reasonable efforts to use methods and procedures that will locate" responsive documents. Att. B at 6. In short, the Government does not intend to "rummage through [the devices] in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014); *accord* 28 C.F.R. § 50.10(d)(4) (directing investigators to "use search protocols designed to minimize intrusion into potentially protected materials or newsgathering activities"). Rather, the Government will engage in the standard practice for searching seized electronic devices and will search based on the specific terms of the warrant. Any other suggestion ignores the terms under which the Government proposes that the filter team should operate.

C. The First Amendment Allows Review by the Government.

The magistrate judge also foreclosed Government review of the devices because the seizure "constitutes a restraint on the exercise of First Amendment rights." Op. 16. And after

[7] The details are available in the filter protocol that will be submitted under seal as soon as a judge is assigned to this motion.

"[b]alancing" that restraint "against the [G]overnment's compelling interest in its prosecution," the Court decided to undertake a judicial search for only information responsive to the search warrant. *Id.* at 18. That is wrong at every turn. Reporters are subject to lawful searches and seizures just like everyone else.

1. The Magistrate Judge Improperly Imposed First Amendment-Specific Procedures on a Search Authorized by a Valid Warrant.

The magistrate judge's balancing would improperly upend traditional practice when a valid search warrant is executed. Once the Government establishes probable cause to find evidence of a crime and obtains a search warrant that complies with the Fourth Amendment, the Government is authorized to search for that evidence. Movants have never disputed that the Government has probable cause to believe that Ms. Natanson's devices contain evidence of a crime, nor have they argued that those devices are free of that evidence. Those facts alone provide ample reason for the Government to have authority to review the seized devices for material responsive to the warrant.

The magistrate judge's decision to the contrary imposes a new requirement on the standard review process for material seized under a valid warrant where those materials implicate First Amendment activity. That is contrary to precedent. The Supreme Court has long held 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*, 408 U.S. at 682; *see also Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 704 (1986) (same and collecting authorities). "[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." *Branzburg*, 408 U.S. at 682–83. In other words, "the *Branzburg* Court declined to treat reporters differently from all other citizens who are compelled to give evidence of criminal activity, and refused to require a 'compelling interest' or other special showing simply because it is a reporter who is in possession of the

evidence." *Sterling*, 724 F.3d at 493. Similarly, the Supreme Court has rejected any effort to require heightened procedures that alter the requirements of the Fourth Amendment's Warrant Clause or prevent searches when the Government seeks a warrant to search journalistic premises. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978). And the Fourth Circuit has twice held that reporters "have no privilege different from that of any other citizen" when asked to provide evidence of crimes to the Government. *In re Shain*, 978 F.2d 850, 852 (4th Cir. 1992); *see Sterling*, 724 F.3d at 497.

Yet the magistrate judge's decision places reporters (or other persons with First Amendment interests) on a different constitutional footing than other subjects of a search warrant. Under his framework, the warrant requirements and standard review procedure—in which the Government searches material seized under a search warrant—are thoroughly altered because the subject is a reporter. *See* Op. 16, 18 (justifying a judicial search procedure based on the effect on Ms. Natanson's "work product" and "newsgathering rights"). The First Amendment as interpreted by the *Branzburg* Court and the Fourth Circuit in *Shain* and *Sterling* does not require such a reporter-specific procedure. *See 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.").

Neither does *Zurcher*. That case suggested that judges apply the requirements of the Fourth Amendment "with scrupulous exactitude" whenever "the materials sought to be seized may be protected by the First Amendment." 436 U.S. at 563 (citation omitted). The magistrate judge here read that directive to require an initial judicial search. *See* Op. 16. But *Zurcher* simply instructs rigorous application of the Fourth Amendment's standard rules when a warrant is requested, *i.e.*, to ensure the warrant is reasonable in its particular context. It does not require special procedures

for the search process such as judicial participation. *See* 436 U.S. at 565 (explaining that the relevant precedents "do no more than insist that the courts apply the warrant requirements with particular exactitude"). As the Supreme Court said, "the preconditions for a warrant . . . should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices." *Id.*

The magistrate judge here had the opportunity to apply those preconditions when the Government sought this search warrant. And based on his opinion, he did so with the "scrupulous exactitude" required by *Zurcher*. As he explained, the Government presented "successive versions of the proposed warrant" until the magistrate judge ultimately approved the final version. Op. 4. Throughout, he expressed "concern[s] about both the scope of the proposed search warrant and the government's apparent attempt to collect information about Ms. Natanson's confidential sources." *Id.* In other words, he knew that the warrant would implicate First Amendment activity and worked to ensure that the resulting warrant "properly applied, policed, and observed" the requirements for all warrants under the Fourth Amendment. *Zurcher*, 436 U.S. at 566. The Government also did not seek the warrant attempting to collect information on any other source of Ms. Natanson's. Indeed, the warrant allows the Government to seize only evidence from a limited date range and relating to a specific individual. Once the magistrate judge signed that warrant after rounds of review, he fulfilled the directive from *Zurcher* regarding scrupulous exactitude. Nothing in that decision authorizes him to deviate from the standard Government-first review of materials seized pursuant to a valid search warrant.

The presence of material potentially protected by the First Amendment also does not support the magistrate judge's rescission of authority to search the devices. *See* Op. 22. As an initial matter—and as made clear by *Sterling*, which the magistrate judge did not address—that

material is not "privileged" and insulated from review in the face of a valid search warrant. Op. 19. The Fourth Circuit has rejected a reporter's privilege in criminal cases when a subpoena "is issued in good faith and is based on a legitimate need of law enforcement[.]" *Sterling*, 724 F.3d at 496. The logic applies to search warrants, which are animated by the same "compelling public interest in effective criminal investigation and prosecution" as a criminal subpoena, *id.* at 498, and are issued after only a determination by a neutral magistrate judge (which is not required for a subpoena). Here, the search warrant was based on a legitimate need of law enforcement to seize evidence of a crime and was sought in good faith to obtain that evidence. That the search of those devices involves some review of First Amendment material beyond the scope of the search warrant does not provide a basis for the magistrate judge's drastic departure from authority governing searches of electronic devices.

Moreover, the probable cause standard for warrants implicating First Amendment material is the same as it is for all other warrants. *See New York v. P.J. Video, Inc.*, 475 U.S. 868, 875 (1986); *see also United States v. Giberson*, 527 F.3d 882, 889 (9th Cir. 2008). Rescinding search authority for First Amendment material simply because it is First Amendment material imposes enhanced warrant requirements that the Fourth Circuit has rejected in cases involving electronic evidence. *See Cobb*, 970 F.3d at 329; *Zelaya-Veliz*, 94 F.4th at 337–38. And although courts sometimes impose safeguards when the state seeks large-scale seizures of First Amendment material "for the sole purpose of their destruction," there is no risk of that here. The Government seeks evidence of a crime, not destruction of Ms. Natanson's materials. The magistrate judge's observation that "a seizure reasonable as to one type of material in one setting may be unreasonable in a different setting" does not entitle him to fundamentally alter the standard search-and-seizure procedures provided by law. Op. 16 (quoting *Zurcher*, 436 U.S. at 564).

2. There Is No Prior Restraint Here.

Notwithstanding the above, the magistrate judge appeared to order a judicial search procedure based to some extent on the nature of the perceived restraint placed on Ms. Natanson. While the magistrate judge recited the general prohibition against *prior* restraints, he never said that the "restraint" imposed against Ms. Natanson qualifies as a prior restraint. *See* Op. 15–16. That is a meaningful distinction—a restraint on First Amendment activity is not automatically a presumptively unlawful *prior* restraint. *See Schenck v. Pro-Choice Network*, 519 U.S. 357, 374 n.6 (1997) (declining to evaluate an injunction restricting abortion protests to certain areas as a prior restraint); *Madsen v. Women's Health Ctr., Inc.*, 512 U.S. 753, 763 n.2 (1994) (same). But to the extent that the magistrate judge did view the seizure as a prior restraint, that conclusion was erroneous.

Prior restraints are a particular type of restriction on First Amendment activity. The Supreme Court has described them as 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 Melville B. Nimmer, *Nimmer on Freedom of Speech* § 4.03 at 4–14 (1984)); *see also Ward v. Rock Against Racism*, 491 U.S. 781, 795 n.5 (1989) ("[T]he regulations we have found invalid as prior restraints have had this in common: they gave public officials the power to deny use of a forum in advance of actual expression." (citation omitted)). Not all governmental actions that "may incidentally affect expression" are prior restraints. *Madsen*, 512 U.S. at 763 n.2. When "absolutely no channel of communication is foreclosed," a prior restraint does not exist. *Hill v. Colorado*, 530 U.S. 703, 734 (2000). And when the state burdens speech "not because of the content" of that expression, there is no prior restraint. *Madsen*, 512 U.S. at 763 n.2.

This seizure does not constitute a prior restraint. No court order or government action prohibits Ms. Natanson "from engaging in any expressive activities in the future," nor does she need to "obtain prior approval for any expressive activities" she wishes to undertake. *Alexander*, 509 U.S. at 550–51. Indeed, she did not need Government approval to set up a new Signal account, presumably so that she can continue to cultivate sources for her reporting. *See* Hannah Natanson [@hannah_natanson], X, https://x.com/hannah_natanson?lang=en (announcing her Signal as @HannahNatanson.2026). And contrary to the magistrate judge's suggestion, *see* Op. 2–3, 21–22, the Government has not seized these devices to burden Ms. Natanson's reporting based on its content. It seized them because there is probable cause to believe that they contain evidence of a crime, a conclusion with which the magistrate judge agreed when he signed the warrant and with which he still agrees, *see* Op. 7.

The magistrate judge responds that she cannot publish without her devices, which contain her confidential sources and her work product, thus creating a prior restraint. But there is a difference between an action forbidding future expressive activities and an order depriving someone of "specific assets that were found to be related" to previous wrongdoing. *Alexander*, 509 U.S. at 551. The latter is not a prior restraint because it imposes "no legal impediment to . . . [the] ability to engage in any expressive activity." *Id.* Here, a valid warrant deprived Ms. Natanson of assets which the Government had probable cause to believe held evidence of a crime. That is not a prior restraint given that she is not forbidden from further First Amendment activities. And although the magistrate judge labeled it "unjust and unreasonable" to expect Ms. Natanson to buy new devices for her reporting, Op. 21, it is also unreasonable and unjust to prevent the Government from searching devices that all agree contain evidence of federal crimes. The Government does not dispute that reporters like Ms. Natanson engage in First Amendment-

protected conduct and speech. *Contra id.* at 15. But that is true of many persons who may have devices seized pursuant to a valid search warrant, such as people of faith, political activists, and social media users. The presence of First Amendment-protected content on a device does not immunize that device from standard search warrant practices.

In short, a seizure is not a prior restraint simply because it encompasses journalistic or work product communications.[8] The Supreme Court and Fourth Circuit rejected any contrary notion when they required journalists to give evidence of criminal wrongdoing in response to legitimate exercises of law enforcement, even when that evidence might implicate source relationships. *See Branzburg*, 408 U.S. at 691–92; *Sterling*, 724 F.3d at 494. To the extent that the magistrate judge ordered a judicial search based on the purported presence of a prior restraint, that was erroneous.

II. The Use of a Filter Team Is Appropriate Here and Consistent With Fourth Circuit Precedent.

The Government should be the one reviewing the seized material. And to account for any privilege or First Amendment interests applicable to some of that material, the Government is prepared to proceed via a filter team of reviewers and attorneys that are walled-off from the team prosecuting Perez-Lugones. The use of a filter team is common, *see In re Search of Elec. Commc'ns*, 802 F.3d 516, 530 (3d Cir. 2015), and multiple circuits have approved the use of a

[8] To accept otherwise risks alarming consequences. In recent years, investigators have seized devices from multiple reporters based on probable cause that those devices contained child pornography. *See* U.S. Atty's Off. of D.C., *Award-Winning Journalist Arrested and Charged with Possession of Child Pornography* (Jun. 27, 2025), https://www.justice.gov/usao-dc/pr/award-winning-journalist-arrested-and-charged-possession-child-pornography; U.S. Atty's Off. of E. Dist. of Va., *Former Journalist Sentenced For Possessing Child Sexual Abuse Material* (Sep. 29, 2023), https://www.justice.gov/usao-edva/pr/former-journalist-sentenced-possessing-child-sexual-abuse-material. It cannot be the case that these seizures, undertaken to locate critical evidence of serious crimes, would constitute prior restraints merely because the seized devices also contained the reporters' journalistic work product.

walled-off filter team to review seized documents for privilege, *see In re Sealed Search Warrant*, 11 F.4th 1235, 1249 (11th Cir. 2021) (collecting authorities).

The Government has proposed a filter protocol that would require filter investigators to review information within the date range specified in the warrant. They would then take reasonable measures to locate information that is within the scope of the warrant. Responsive information would then be reviewed for attorney-client privilege and work-product protection as well as for anything that might be subject to the PPA or to the First Amendment.[9] The filter team would segregate information that is outside the warrant's scope, privileged, or otherwise protected and would send all other information within the scope of the warrant to the prosecution team. Further details can be found in the Government's sealed submission.

Baltimore Criminal Defense Firm is readily distinguishable. *Contra* Op. 19–21. There, a magistrate judge issued a warrant authorizing a search for a lawyer's records concerning one specific client. *See* 942 F.3d 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. Some of those other clients were under investigation by the same U.S. 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. The Fourth Circuit held that the filter protocol was flawed for multiple reasons. The

[9] To be clear, the Government does not concede that the First Amendment provides a privilege over any of the material on the devices or that the PPA prohibits the Government's review of commingled materials. *See supra* at 22–23, *infra* at 29–30. But the Government acknowledges that its review might implicate material related to Ms. Natanson's journalistic activities and/or material that is expressly protected from search by the PPA. A filter team will ensure that, absent other privileges, that material will reach the prosecutorial team only if it is responsive to the warrant.

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," which was a "judicial function" to be performed only by judicial officers. *Id.* at 176, 177. The Fourth Circuit also concluded that the filter protocol was improperly authorized *ex parte*. *See id.* at 178–79. Moreover, the filter team proposed there allowed the Government to "contact the Law Firm's clients *ex parte* and seek waivers of their attorney-client privileges." *Id.* at 180. That demonstrated a "lack of respect for the attorney-client privilege and the Firm's duty of confidentiality to its clients." *Id.* "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.

Several distinctions are immediately plain. The *Baltimore Criminal Defense Firm* filter team was deficient in part because "an adverse party's review of privileged materials seriously injure[d]" 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, and over which the Government has unique equities that, unlike the attorney-client privilege, "can neither be claimed nor waived by a private party," *United States v. Reynolds*, 345 U.S. 1, 7 (1953) (footnotes omitted). In addition, *Baltimore Criminal Defense Firm* emphasized that resolution of attorney-client privilege issues is a "judicial function." 942 F.3d at 176–78. The handling of classified material is not; indeed, it is an Executive function, and Congress has enacted a very specific set of rules for when courts should see classified material. *See* Classified Information Procedures Act, 18a U.S.C. § 1 *et seq.* *Baltimore Criminal Defense Firm* also does not "mandate[]" a review by the magistrate judge of all seized material. Op. 21. That judicial officers must resolve disputes about attorney-client privilege, as the Fourth Circuit

held, does not authorize a far-ranging search by a judicial officer of everything that the Government seized pursuant to a search warrant.

In addition, the Government does not seek *ex parte* approval of a filter procedure nor does it proffer a filter protocol that allows for *ex parte* waivers of the attorney-client privilege, thereby avoiding the ethical issues that concerned the Fourth Circuit. *See* 942 F.3d at 178, 180. Nor is this a case where a U.S. Attorney's Office is filtering out information related to other persons under investigation by the same office, as was the case in *Baltimore Criminal Defense Firm*. *See id.* at 172. Indeed, this Court should read *Baltimore Criminal Defense Firm*'s holding as clearly limited to its specific facts, as Judge Rushing emphasized in her concurrence. *See id.* at 183 (Rushing, J., concurring) ("[T]he unique facts and circumstances of this case preclude this Filter Team operating under this Filter Protocol from reviewing the fruits of this search warrant.").

III. The PPA Does Not Bar the Search or Government Review of the Devices.

The magistrate judge's opinion criticized the Government's search warrant application for omitting any mention of the PPA but admitted that he could not "definitively conclude [he] would not have authorized the warrant" had the application referenced the PPA. *See* Op. 9–13. The opinion does not, however, rely on the PPA as authority for a judicial search. In any event, the PPA does not bar this search, and it gives no reason to prevent the Government from searching Ms. Natanson's devices. The statute prohibits searches or seizures of "work product materials" or "documentary materials," both defined in the statute, when possessed by a journalist. 42 U.S.C. § 2000aa(a)-(b). But the statutory definitions specifically exclude "contraband or the fruits of a crime." *Id.* § 2000aa-7(a), (b). Because the search warrant here was for information that is "evidence of violations of 18 U.S.C. § 793," Att. B at 5, it sought the fruits of Perez-Lugones's crimes.

To be sure, the seized material includes more than just that evidence and almost certainly includes PPA-protected materials. But "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. The PPA also is no reason to grant a Rule 41(g) motion. It authorizes an "exclusive" remedy, which is "a civil cause of action for damages" against the Government, not compelled return of seized property. 42 U.S.C. § 2000aa-6(a), (d). In any event, the proposed filter team mitigates any PPA-related concerns.

CONCLUSION

The Court should vacate the magistrate judge's order, deny the Motion for Return of Property, and permit the Government to review the devices in accordance with a filter protocol.

Dated: March 10, 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