UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

United States of America

v.

[redacted]

Case No. 1:26-sw-54

MEMORANDUM OF LAW IN SUPPORT OF THE WASHINGTON POST'S AND HANNAH NATANSON'S MOTION TO INTERVENE AND FOR RETURN OF PROPERTY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTION

RULES, STATUTES, AND REGULATIONS

INTRODUCTION

The federal government's wholesale seizure of a reporter's confidential newsgathering materials violates the Constitution's protections for free speech and a free press and should not be allowed to stand. It is a prior restraint and a violation of the reporter's privilege that flouts the First Amendment and ignores federal statutory safeguards for journalists. The seizure chills speech, cripples reporting, and inflicts irreparable harm every day the government keeps its hands on protected materials. The government cannot meet its heavy burden to justify this intrusion, and it has ignored narrower, lawful alternatives. The Court should order the immediate return of all seized materials. Anything less would license future newsroom raids and normalize censorship by search warrant.

In the early morning before dawn on Wednesday, January 14, the government executed a search warrant at the home of Washington Post reporter Hannah Natanson because of her newsgathering activities. It seized a massive volume of her electronic data, capturing years of her newsgathering materials across hundreds of stories, including communications with confidential sources. Natanson is an award-winning investigative journalist who covers a wide range of news about the federal government. Three weeks before the FBI's raid, she published an article about her more than 1,100 sources within the federal government who have helped The Post break dozens of stories in the last year.[1]

The search warrant says that it seeks records relating to a defense contractor named Aurelio Luis Perez-Lugones, who was arrested roughly a week earlier. But the FBI seized Natanson's newsgathering materials, stored on devices including her Post-issued laptop and cellphone, that

[1] Hannah Natanson, *I am The Post's 'federal government whisperer.' It's been brutal*, Wash. Post, Dec. 24, 2025, https://wapo.st/3LSRR1i.

contain years of information about past and current confidential sources and other unpublished newsgathering materials, including those she was using for current reporting. Almost none of the seized data is even potentially responsive to the warrant, which seeks only records received from or relating to a single government contractor. The seized data is core First Amendment-protected material, and some is protected by the attorney-client privilege.

Pursuant to the First Amendment and Rule 41(g) of the Federal Rules of Criminal Procedure, WP Company LLC d/b/a The Washington Post ("The Post") and Natanson seek return of the seized newsgathering materials because the seizure was an unconstitutional prior restraint, which is "the most serious and the least tolerable infringement on First Amendment rights." *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). The seizure had the practical effect of suppressing The Post and Natanson's current and future journalism, including because the seizure has prevented her from communicating with her more than 1,100 sources, who run the gamut of federal officials from more than 120 agencies or subagencies, and who overwhelmingly and self-evidently have nothing to do with the warrant. Nor are Natanson's confidential sources likely to work with her again, if the government is permitted to rummage through her files unchecked.

At the very least, The Post and Natanson seek return of the non-responsive data and judicial oversight of the return process as a reasonable condition "to protect access to the property and its use in later proceedings." Fed. R. Crim. P. 41(g). In other cases involving the seizure of constitutionally protected or privileged information, courts require such judicial oversight. *See, e.g.*, *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 181 (4th Cir. 2019) (holding that either "the magistrate judge (or an appointed special master)—rather than the Filter Team—must perform the privilege review of the seized materials").

BACKGROUND

I. The Government Arrests Perez-Lugones.

On January 8, 2026, the government arrested Aurelio Luis Perez-Lugones, alleging that he had unlawfully retained national defense information in violation of 18 U.S.C. § 793(e). *See* Latcovich Decl., Ex. C (Perez-Lugones Complaint and Affidavit). The affidavit in support of the criminal complaint alleges that Perez-Lugones was a government contractor with a Top Secret security clearance. *See id.* at ¶ 8. It further alleges that since October 2025 (i) he copied information from a classified report and attachment to a single Microsoft Word document, which he then printed; (ii) he took possession of four pages from a yellow notepad (or pads) that may or may not contain notes about classified information; and (iii) a search of his residence and vehicle identified two documents marked secret. *Id.* ¶¶ 16, 32, 35-36, 38-39.

The criminal complaint thus alleges that Perez-Lugones possessed a small number of documents that potentially contain classified information—three documents and four yellow notepad pages.

II. The Government Raids a Washington Post Journalist's Home and Seizes a Trove of Newsgathering Materials That Are Protected by the First Amendment and Materials Protected by the Attorney-Client Privilege.

On Wednesday, January 14, 2026, at approximately 6:00 AM, FBI agents executed a search warrant at the residence of Washington Post reporter Hannah Natanson, seeking records received from or relating to Perez-Lugones. *See* Latcovich Decl., Ex. A (Search and Seizure Warrant); Natanson Decl. ¶ 11.

Natanson is an award-winning investigative journalist who covers the Trump administration's transformation of the federal government. *See* Natanson Decl. ¶¶ 2-4. She won a Peabody Award in 2024 and was part of a team of Post journalists who won the Pulitzer Prize for Public Service in 2022. *See id.* ¶ 3. Over the past year on this beat, Natanson gained 1,169

confidential sources—federal employees from more than 120 agencies or subagencies who requested anonymity because they "fear retribution from the government due to their disclosures." *Id.* ¶¶ 5-6, 39. These sources' contributions resulted in Natanson writing or co-writing "more than 200 articles across roughly twenty news desks." *Id.* ¶ 7.

The search warrant authorized the seizure of "[a]ll digital devices, or other electronic storage media, or components of either identified during the searches that are reasonably believed to be used by Natanson." Latcovich Decl., Ex. A (Search and Seizure Warrant). The FBI agents ultimately seized the following items from Natanson's residence: (1) a MacBook Pro that is owned by The Post and that Natanson used for work; (2) a second MacBook Pro that Natanson personally owns but also used for work; (3) an iPhone that The Post owns that Natanson used for work; (4) a 1-terabyte portable hard drive; (5) a Garmin watch that Natanson personally owns; and (6) a voice recorder that The Post owns and that Natanson used for her reporting. Latcovich Decl., Ex. B (Property Receipt); Natanson Decl. ¶ 14.

Although the government seized only six devices, those devices are capable of storing multiple terabytes of data. To put this in perspective, ten terabytes could hold the entire Library of Congress's printed collection. Natanson's devices contain essentially her entire professional universe: more than 30,000 Post emails from the last year alone, confidential information from and about sources (including her sources and her colleagues' sources), recordings of interviews, notes on story concepts and ideas, drafts of potential stories, communications with colleagues about sources and stories, and The Post's content management system that houses all articles in progress. Natanson Decl. ¶¶ 8, 16-35. The devices also housed Natanson's encrypted Signal messaging platform that she used to communicate with her more than 1,100 sources. *Id.* ¶ 43. Without her devices, she "literally cannot contact" these sources. *Id.* ¶ 43. Prior to the seizure,

she would receive somewhere between dozens and over 100 tips from her sources via Signal *per day*. *Id.* ¶ 39. In short, the devices are critical to her ability both to function as a journalist and to collaborate with her colleagues in the newsroom. *Id.* ¶¶ 40-41. These devices also reflect the details of her personal life, "including medical information, financial information, and even information about [her] wedding planning." *Id.* ¶ 25.

The government seized this proverbial haystack in an attempt to locate a needle. The search warrant orders that the government's search of the seized data "must be limited to all records and information . . . from the time period October 1, 2025, to the present, which constitute records received from or relating to Aurelio Luis Perez-Lugones." Latcovich Decl., Ex. A (Search and Seizure Warrant). Even the government cannot expect to find many records responsive to the warrant in this ocean of data because its criminal complaint alleges that Perez-Lugones possessed only a small number of documents potentially containing classified or secret information, which he only began collecting three months ago. Meanwhile, Natanson has thousands of communications across her more than 1,100 sources. *See* Natanson Decl. ¶ 39. And her devices contain years of data about past and current confidential sources and other unpublished materials. *See id.* ¶¶ 17-18, 20, 32-33, 35; Roberson Decl. ¶¶ 7-9, 11. At best, the government has a legitimate interest in only an infinitesimal fraction of the data it has seized. *See* Natanson Decl. ¶ 38.

Although the warrant narrowly defines what is within its scope, it does not prescribe a detailed search protocol to locate those items. Instead, the warrant authorizes a non-exhaustive list of review techniques, including opening and reading the substance of files contained on the devices, even those files that relate to newsgathering activity or confidential sources and that have nothing to do with Perez-Lugones. *See* Latcovich Decl., Ex. A (Search and Seizure Warrant). The

government's review of the data thus presents unique issues in this case. Everything included in this massive volume of data is presumptively protected by the First Amendment. The search warrant, however, includes no protocol or safeguards relating to the review of materials protected by the First Amendment. *See* Latcovich Decl., Ex. A (Search and Seizure Warrant). The data also includes privileged communications with Post attorneys. *See* Natanson Decl. ¶ 34; *see also supra* 1 n.1 (explaining that Natanson developed her sourcing system in consultation with "Post lawyers"). The warrant includes no protocol for the review of materials protected from disclosure by the attorney-client privilege, although it does state that if government agents identify documents that they deem, in their own discretion, to be potentially privileged, they are to segregate such documents to prevent further substantive review. *See* Latcovich Decl., Ex. A (Search and Seizure Warrant).

III. The Government Issues an Overlapping Grand Jury Subpoena to The Post.

The same day the FBI raided Natanson's residence, the government issued a grand jury subpoena to The Post seeking substantially the same items as those particularized in the search warrant—records of communications with Perez-Lugones and records received from him. *See* Latcovich Decl., Ex. D (Grand Jury Subpoena). Nothing prevented the government from issuing a subpoena to Natanson instead of executing a search warrant, which is what, historically, would have been mandated by government policy.

IV. The Government Refuses to Return the Protected Materials.

The same day the FBI raided Natanson's residence, undersigned counsel reached out to the government to advise that the seized items contain materials protected by the First Amendment and the attorney-client privilege. *See* Latcovich Decl., Ex. E (Email). Undersigned counsel asked the government to refrain from reviewing the documents pending a discussion. *See id.* On January 15, the parties conferred regarding the seized documents. *See* Latcovich Decl. ¶ 10. No

agreements regarding the handling of the data were reached because government counsel asserted that all issues had to be vetted with more senior government officials. *Id.* The government also represented that it was in the process of extracting data from the devices and preserving data, and that it was not reviewing content. *See id.*

On January 16, the parties conferred twice regarding the seized data. *Id.* ¶ 11. Counsel for The Post proposed a process that would involve the government's copying and preservation of the seized data, returning the seized property, and reviewing only the responsive material, if any, identified by counsel for The Post and Natanson. *See id.* ¶ 11. After conferring with the unnamed, more-senior officials, the government called back and rejected this proposal, but agreed that it would not begin a substantive review of the seized data pending further discussion on January 20. *See id.* ¶ 12. The government asked counsel to provide a list of attorney names on January 20 for the government to use as the basis for screening privileged materials. *See id.* ¶ 12. Counsel for The Post explained that a list of attorney names would be an inadequate basis to screen privileged information because editors at The Post, as opposed to reporters, generally request and receive legal advice from attorneys and then disseminate that advice to reporters. *See id.* ¶ 12; *see also* Natanson Decl. ¶ 34. Counsel for The Post also explained that a list of attorney names would not address the significant First Amendment issues and asked for further time to discuss these complex issues before the government commenced its review. *See* Latcovich Decl. ¶ 13. The government expressed doubt that the unnamed, senior officials would agree to a proposal designed to protect the significant First Amendment interests at stake here. *See id.* ¶ 13.

On January 20, the parties conferred again. Counsel for The Post and Natanson proposed that the government return the seized property and that The Post would treat the devices as covered by the grand jury subpoena served on The Post. *See* Latcovich Decl. ¶ 14. The government

rejected this proposal. Latcovich Decl. ¶ 15. Counsel for The Post and Natanson then informed the government that they intended to seek judicial relief and would file a motion within twenty-four hours, and asked the government to agree to refrain from beginning review until the Court could respond, noting that Judge Rushing on the Fourth Circuit had previously written in a similar Rule 41(g) matter that this was a "sensible procedure." *See* Latcovich Decl. ¶ 16 (quoting *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 184 (2019) (Rushing, J., concurring)). The government stated that it would not refrain from conducting a substantive review of the seized material pending judicial resolution of this dispute, notwithstanding this guidance, and that it was still in the process of preserving data and had not yet started reviewing it. Latcovich Decl. ¶ 17. The government also refused to take a position one way or the other on any protocol to protect either attorney-client privilege or First Amendment privileges, and it would not commit that it intended to undertake any process to protect any applicable First Amendment privileges. Latcovich Decl. ¶¶ 18-19.

V. The Federal Government Historically Has Prohibited the Search and Seizure of Materials from Journalists.

Searches and seizures of journalists' newsgathering materials by the federal government are nearly unprecedented. And, even by local authorities, such actions are exceedingly rare and have been subject to public and legal repudiation.[2] Against that backdrop, the search and seizure

[2] *See* Katherine Jacobsen, *"This Kind of Behavior Cannot Be Tolerated": Police Raid on Kansas Newspaper Alarms Media, Press Freedom Groups*, Comm. to Protect Journalists (Aug. 14, 2023), https://tinyurl.com/yc35d5as ("The use of search warrants against journalists remains rare in the United States."). After local police raided a Kansas newsroom in 2023, the county ultimately agreed to pay $3 million for the wrongful search and seizure. Caitlin Vogus, *Kansas County Pays $3M for Forgetting the First Amendment*, Freedom of the Press Found. (Nov. 12, 2025), https://tinyurl.com/4ruufb7z. On the rare occasions when similar searches have occurred, opposition has been swift and bipartisan. *See Justice Search Warrant Relied on "Probable Cause" of Criminal Conduct by Fox News Journalist*, Reps. Comm. for Freedom of the Press (May 22, 2013), https://tinyurl.com/yw95etvz (describing DOJ search warrant for Fox News reporter's personal email in North Korea leak probe as "downright chilling" and "appalling"); *Zurcher v.*

of devices from Natanson's home stands alone. "This is the first time the U.S. Justice Department has raided a journalist's home in connection with a national security leak investigation." Chris Young & Emily Vespa, *The FBI Search of a Washington Post Reporter's Home: What We Know and Why it Matters*, Reps. Comm. for Freedom of the Press (Jan. 16, 2026), https://tinyurl.com/4wfs62db. That lack of precedent reflects that the Framers' drafting of the Fourth Amendment was informed by "a history of conflict between the Crown and the press." *Stanford v. State of Tex.*, 379 U.S. 476, 482 (1965).[3]

The virtually unprecedented search of Natanson's home and the seizure of The Post's devices coincide with a rise in federal government attacks against the independence of the press. *See* Jess Bidgood, *Trump Sharpens Attacks on a Favorite Foe: The News Media*, N.Y. Times (July 21, 2025), https://tinyurl.com/23c45uwv; Luke Broadwater, *Trump Says Critical Coverage of Him Is 'Really Illegal'*, N.Y. Times (Sept. 19, 2025), https://tinyurl.com/bddwuwaj. This includes an earlier unprecedented move by the Defense Department—effectively evicting the Pentagon press corps for rejecting demands to pledge to refrain from seeking or publishing information that is not officially approved. *See* David Bauder, *Journalists Turn in Access Badges, Exit Pentagon Rather than Agree to New Reporting Rules*, AP News (Oct. 15, 2025), https://tinyurl.com/mu2symvh.

Stanford Daily, 436 U.S. 547, 551 (1978) (raid of Stanford student newspaper); Privacy Protection Act of 1980 Statement on Signing S. 1790 Into Law, The Am. Presidency Project, https://tinyurl.com/pjtsvd9t (decrying raids like the one at Stanford for their "chilling effect on the ability to develop sources and pursue stories.").

[3] In April 2025, the Attorney General rescinded the previous administration's strict protections against issuing compulsory process against the news media. *See* April 25, 2025 Atty. Gen. Mem., https://tinyurl.com/mrb42msw; 28 C.F.R. § 50.10. But even in the memorandum announcing the change, the Attorney General acknowledged that "investigative techniques relating to newsgathering are an extraordinary measure to be deployed as a last resort when essential to a successful investigation or prosecution." *Id.* The government's action here flouted even that principle—it chose to execute a search warrant on a journalist's home as a first resort, and apparently refuses to do anything post-seizure to protect the First Amendment interests at stake.

At a time when journalists are already under attack, this raid "is not just about one reporter, one newsroom, or one investigation," but "about whether journalists can promise confidentiality to sources without fear that federal agents will show up at their door." Press Release, Soc'y of Pro. Journalists, *SPJ Condemns FBI Search of Washington Post Reporter's Home as a Grave Threat to Press Freedom* (Jan. 14, 2026) (available online at https://tinyurl.com/5amvsdf7); *see also* Press Release, Investigative Reps. and Eds., *IRE Statement on FBI Raid of Hannah Natanson's Home*, (available online at https://tinyurl.com/4fzvj4kv) (describing the search as "an unconscionable attack on a free press").

Such an environment not only harms journalists but also chills the whistleblowers and other sources on whom journalists rely to shine light on stories that would otherwise remain in the shadows. Disclosures by confidential government sources have resulted in some of the most consequential investigative journalism in history. Military analyst Daniel Ellsberg leaked portions of the Pentagon Papers to the *New York Times* and The Post, enabling the newspapers to reveal government lies "of a generational scale" about the Vietnam War. Elizabeth Becker, *The Secrets and Lies of the Vietnam War, Exposed in One Epic Document*, N.Y. Times (June 9, 2021), https://tinyurl.com/5b4rphmj; Christopher B. Daly, *Fifty years ago the Pentagon Papers shocked America — and they still matter today*, Wash. Post (June 13, 2021), https://tinyurl.com/2pxx2b8m. And a source by the name Deep Throat, a high-ranking FBI official, "knew he was taking a monumental risk" by secretly assisting Bob Woodward and Carl Bernstein in uncovering the Watergate scandal. David Von Drehle, *FBI's No. 2 Was 'Deep Throat': Mark Felt Ends 30-Year Mystery of The Post's Watergate Source*, Wash. Post (June 1, 2005), https://tinyurl.com/4hn6azu2. Raids like these threaten to gravely chill future whistleblowers, potentially keeping them and their stories in the shadows.

ARGUMENT

Federal Rule of Criminal Procedure 41(g) permits any "person aggrieved by an unlawful search and seizure of property or by the deprivation of property" to "move for the property's return." Fed. R. Crim. P. 41(g). The rule does not set forth a standard "to govern the determination of whether property should be returned," but the test is one of "reasonableness under all of the circumstances." Fed. R. Crim. P. 41 advisory committee's note to 1989 amendment. "[I]f the United States' *legitimate interests* can be satisfied even if the property is returned, continued retention of the property would become unreasonable." *United States v. Rayburn House Office Bldg.*, 497 F.3d 654, 663 (D.C. Cir. 2007) (quoting Fed. R. Crim. P. 41 advisory committee's note to 1989 amendment) (emphasis in *Rayburn*). Once the need for retaining property has passed, a district court "has both the jurisdiction and the duty to return the contested property . . . regardless and independently of the validity or invalidity of the underlying search and seizure." *United States v. Wilson*, 540 F.2d 1100, 1103-04 (D.C. Cir. 1976).

The Post and Natanson request that the Court order return of all seized materials and allow the government to maintain, but not review, the preservation copies under seal until this matter is resolved. The government's legitimate interests can be satisfied by issuing a subpoena to Natanson and/or The Post for the same items sought by the warrant—communications with Perez-Lugones, or records allegedly received from him. This is the appropriate remedy because the seizure in this case was an unconstitutional prior restraint that seized materials related to more than 1,100 completely unrelated sources, and suppressed The Post and Natanson's ability to publish stories on completely unrelated topics.

At a minimum, The Post and Natanson request that the Court order return of the non-responsive data with judicial oversight of the return process as a reasonable condition "to protect access to the property and its use in later proceedings." Fed. R. Crim. P. 41(g). In other cases

involving the seizure of constitutionally-protected or privileged information, courts require such judicial oversight. *See, e.g.*, *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 181 (4th Cir. 2019) (holding that either "the magistrate judge (or an appointed special master) — rather than the Filter Team — must perform the privilege review of the seized materials").

I. All the Materials Should Be Returned Because the Seizure Was an Unconstitutional Prior Restraint and Any Government Interest Can Be Protected by a Subpoena or Other Less Invasive Legal Process.

The First Amendment to the U.S. Constitution prohibits the government from "abridging the freedom of speech, or of the press." U.S. Const. amend. I. All of the materials that the government seized should be returned because the search and seizure of Natanson's reporting materials was an unconstitutional prior restraint—government action that blocks expressive activity before it can occur. Here, the government has commandeered Natanson's reporting records and tools, thereby preventing her from contacting her more than 1,100 sources and receiving their tips, and generally impairing her ability to publish the stories she otherwise would have published but for the raid.

Prior restraints on speech "are the most serious and the least tolerable infringement on First Amendment rights." *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976); *see also, e.g.*, *N.Y. Times Co. v. United States*, 403 U.S. 713, 717 (1971) (Black, J., concurring) ("Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints."). Any prior restraint must be viewed "with a heavy presumption against its constitutional validity." *Neb. Press Ass'n*, 427 U.S. at 558 (citation omitted).

Government seizure of newsgathering material is a prior restraint because it substantially impairs or prevents future publication of news. Thus, courts have repeatedly held that such seizures are unlawful. *See, e.g.*, *Garcia v. Montgomery County*, 145 F. Supp. 3d 492, 511 (D. Md.

2015) (seizure of reporter's recording of police activity is an unconstitutional prior restraint); *Robinson v. Fetterman*, 378 F. Supp. 2d 534, 541 (E.D. Pa. 2005) ("to the extent that the troopers were restraining [the plaintiff] from making any future videotapes and from publicizing or publishing what he had filmed, the defendants' conduct clearly amounted to an unlawful prior restraint upon his protected speech"); *Channel 10, Inc. v. Gunnarson*, 337 F. Supp. 634, 637 (D. Minn. 1972) ("[I]t is clear to this court that the seizure and holding of the [journalist's] camera and undeveloped film was an unlawful 'prior restraint' whether or not the film was ever reviewed."); *see also, e.g.*, *Meyer v. City of Marion*, 776 F. Supp. 3d 991, 1037 n.22 (D. Kan. 2025) ("[P]laintiffs have stated a plausible claim that defendants violated their First Amendment rights by physically invading the *Record*'s office and interfering with the *Record*'s ability to gather and publish the news.").[4]

Indeed, the Supreme Court acknowledged in *Zurcher v. Stanford Daily* that a police search of newsroom materials could constitute a prior restraint. 436 U.S. 547, 567 (1978) (considering whether the search created a "realistic threat of prior restraint or of any direct restraint whatsoever on the publication of the Daily or on its communication of ideas"). While the Court ultimately determined in that case, which involved only a limited search *and no seizure*, that there was no threat of a prior restraint, *id.* at 567, that threat has unquestionably materialized here.

In *Zurcher*, police conducted a limited search for "news photographs taken in a public place." *Id.* The search did not require them to open any "locked drawers and rooms." *Id.* at 551. And the government was *not* notified of any confidentiality concerns prior to the search. 436 U.S.

[4] *See also Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 63-64 (1989) ("searches for and seizure of First Amendment material" create "risk of prior restraint"); *Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241, 256 (1974) ("Governmental restraint on publishing need not fall into familiar or traditional patterns to be subject to constitutional limitations on governmental powers.").

at 551. In addition, there was no seizure at all in *Zurcher*: "*no materials were removed from the Daily's office*," and the reporters could continue their work. *Id.* at 552 (emphasis added). Given the limited scope of the search and disruption to newsgathering activities, the Court held that the Fourth Amendment adequately protected the newspaper's First Amendment interests.[5]

That is a far cry from what happened in this case. Here, the government seized all of Natanson's reporting materials that it could through the unprecedented execution of a search warrant of her home, seizing devices that were digitally secured. Natanson Decl. ¶ 14. The government, unlike in *Zurcher*, was immediately put on notice by The Post and Natanson that its search and seizure raised substantial privilege and confidentiality concerns. *See supra* pp. 7-9. But it has nonetheless continued the seizure.

By seizing Natanson's communication devices, source and reporting information, interview notes, and unpublished drafts—not to mention internal communications with editors, newsroom colleagues, and Post lawyers—the government has restrained The Post and Natanson's future publications, in multiple respects. First, the seizure has made it impossible for Natanson to publish the several stories she was actively working on at the time of the raid, which have nothing to do with this case. Natanson Decl. ¶ 44. Second, she no longer has access to her communications with her more than 1,100 confidential sources who have nothing to do with this case, which were primarily housed within her Signal app. Natanson Decl. ¶ 43. Prior to the raid, Natanson—a truly prolific reporter—received an average of dozens to over one hundred tips per day from these sources. Natanson Decl. ¶ 39. Since the raid, without access to her Signal account, that number has dropped to zero; she literally is unable to contact the overwhelming majority of her sources.

[5] Notably, there was such widespread criticism of this outcome that Congress subsequently passed the Privacy Protection Act, which generally prohibits such raids. *See infra* section II.B.3.

Natanson Decl. ¶ 39. Third, and relatedly, the government's seizure has severely hampered Natanson's ability to receive tips about new topics that would have otherwise arisen in the days to come. Natanson Decl. ¶ 45.

These limitations have also hurt The Post, which relies on Natanson's vast and unique sourcing to generate and support news coverage across the newsroom. In the past year alone, Natanson authored or co-authored roughly 200 articles across more than twenty news desks, Natanson Decl. ¶ 7, an exceptionally high number. This prolific output is heavily dependent upon her deep source relationships, which have been at the very least significantly impaired, if not ended, by the government raid.

Natanson's confidential sources chose to "communicate via secure messaging services such as Signal because they fear retribution from the government due to their disclosures" and were therefore willing to disclose information based on an expectation of confidentiality. Natanson Decl. ¶¶ 39, 46. The longer The Post and Natanson's devices remain accessible to the government, "the greater the likelihood that [her] sources will be reluctant to speak with [her] in the future." Natanson Decl. ¶ 46. In other words, if the government remains free to rummage through the seized data, the government will effectively burn 1,100 of The Post's sources and censor their untold stories. This is on top of the inevitable deterring effect that future sources may feel about communicating with Natanson or, potentially, other Washington Post reporters, if it appears to the public that the government can simply confiscate reporters' devices at will.

The seizure accordingly imposed a "prior restraint" on "the publication of [Natanson's and The Post's journalism] or on [their] communication of ideas." *Zurcher*, 436 U.S. at 567; *Neb. Press Ass'n*, 427 U.S. at 559.

Because the seizure was a prior restraint, it was unconstitutional unless the government can overcome the "heavy presumption against its constitutional validity." *Neb. Press Ass'n*, 427 U.S. at 558 (citation omitted); *N.Y. Times*, 403 U.S. at 714 (per curiam) (citation omitted). In other words, the seizure was unlawful unless the government can show the restrained material would have "inevitably, directly, and immediately" caused immense harm to the country. *N.Y. Times*, 403 U.S. at 726-27 (Brennan, J., concurring); *see Neb. Press Ass'n*, 427 U.S. at 562 (court must assess the "gravity of the 'evil'" (quoting *United States v. Dennis*, 183 F.2d 201, 212 (2d Cir. 1950) (Hand, J.), *aff'd*, 341 U.S. 494 (1951)). In addition, the restraint must be narrowly tailored to address that concern. *In re Murphy-Brown, LLC*, 907 F.3d 788, 799 (4th Cir. 2018); *Neb. Press Ass'n*, 427 U.S. at 563 (court must assess whether "other measures would not suffice"); *see also Zurcher*, 436 U.S. at 564 ("Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'" (quoting *Stanford*, 379 U.S. at 485)).

The government cannot meet this burden. Even if it could somehow demonstrate some compelling risk of harm absent seizure, it could not show that the prior restraint was narrowly tailored. In particular, the government could have sought responsive records via less invasive legal process, such as a subpoena. Indeed, it served a grand jury subpoena on The Post the same day as the raid. While a search is "an immediate and substantial invasion of privacy," a subpoena is less invasive because it "commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands." *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000).[6] At bottom, it was plainly not a narrowly tailored effort

[6] Law enforcement has successfully relied on subpoenas to obtain evidence that it claimed it needed from journalists in criminal proceedings. *See generally, e.g.*, *United States v. Treacy*, 603 F. Supp. 2d 670 (S.D.N.Y. 2009); *In re Grand Jury Subpoenas*, 438 F. Supp. 2d 1111 (N.D. Cal.

for the government to seize a journalist's body of newsgathering materials, including confidential records for more than 1,100 sources, when it could have simply subpoenaed the records associated with the one individual at issue.

Because the search and seizure was an unconstitutional prior restraint, all the materials should be returned.

II. At the Very Least, Materials Beyond the Scope of the Warrant Should Be Returned and the Court Should Oversee the Return Process.

The government has no "*legitimate interest*[]" in preventing the return of the non-responsive seized materials to The Post and Natanson. *Rayburn*, 497 F.3d at 663 (citation omitted). Its only arguably legitimate interests are in retaining and using the narrow set of materials, if any, that are responsive to the warrant. Prompt return of the non-responsive materials is especially important and reasonable here given the nature of the non-responsive materials and the context of this seizure. As the Supreme Court has acknowledged, what is "reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." *Zurcher*, 436 U.S. at 564 (quoting *Roaden v. Kentucky*, 413 U.S. 496, 501 (1973)). Here, we are talking about the return of materials protected by the First Amendment that have nothing to do with the government's investigation and are beyond the scope of the government's warrant, including newsgathering materials, draft stories, communications with editors and other journalists about draft stories, and materials relating to confidential sources. Also included in the non-responsive materials are communications protected by attorney-client privilege.

2006); *In re Special Counsel Investigation*, 338 F. Supp. 2d 16 (D.D.C. 2004); *In re Multi-Jurisdictional Grand Jury*, 64 Va. Cir. 423 (Va. Cir. Ct. 2004); *United States v. Jennings*, 1999 WL 438984 (N.D. Ill. June 21, 1999).

A. The Government Seized an Enormous Volume of Data Beyond the Scope of the Warrant.

Seizures of computers and other electronic storage devices to be later searched for responsive materials present unique constitutional concerns because, by definition, such seizures are overinclusive—sweeping in electronic data that the government has no probable cause to collect because it is stored with other data the government may have probable cause to collect. Allowing the government to rummage through the intermingled data without limitation "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam), *overruled on other grounds by Hamer v. Neighborhood Hous. Servs. of Chi.*, 583 U.S. 17 (2017).

To safeguard against this risk, and to ensure the government retains the materials in which it has a legitimate interest, courts require the government to implement reasonable procedures when it seizes electronic evidence. *See id.* at 1177 (applying procedural safeguards from *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), to electronic searches). And when the government follows the seize-everything-sort-it-out-later approach as it did here, "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.*; *see also Tamura*, 694 F.2d at 595 ("[T]he wholesale *seizure* for later detailed examination of records not described in a warrant . . . has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'" (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980))).

The government seized a massive volume of data it had no probable cause to collect in the first instance. Ordering return of the beyond-the-scope data is not only reasonable, but necessary,

and it would not impair the government's legitimate interests. Withholding that data from The Post and Natanson would be entirely unreasonable.

B. The Seized Data Is Protected by the First Amendment.

The request for the government to return the beyond-the-scope data is all the more reasonable because the government's seizure of this data has constitutional implications beyond those presented by the "reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence." *Riley v. California*, 573 U.S. 373, 403 (2014). Even if the government could somehow overcome the First Amendment as to any extremely limited responsive data, if any, the beyond-the-scope data is indisputably protected by First Amendment, reporter's privilege, and statutory protections.

1. Continued withholding of the non-responsive data is an unconstitutional prior restraint.

As set forth in Section I, *supra*, depriving The Post and Natanson of access to her essential reporting tools is an unconstitutional prior restraint. Even if the government could make an argument as to why it should not return the limited materials, if any, that are responsive to the warrant ("records received from or relating to Aurelio Luis Perez-Lugones"), it has no legitimate interest in withholding materials that are beyond the scope of the warrant. Continued withholding of this vast trove of information is unreasonable.

2. The seized data is protected by a First Amendment privilege.

Return of the beyond-the-scope data also would be reasonable and consistent with the government's legitimate interests because this information is *unrelated* to the government's criminal investigation and, therefore, is protected from disclosure by the First Amendment.

The Fourth Circuit "recognizes a qualified 'journalist's privilege,'" also known as a reporter's privilege, "that protects the media" from compelled disclosure of confidential sources

and unpublished newsgathering materials. *Horne v. WTVR, LLC*, 893 F.3d 201, 212-13 (4th Cir. 2018). Such compelled disclosure "restrain[s]" the "free flow of newsworthy information" and "hamper[s]" the "public's understanding of important issues and events . . . in ways inconsistent with a healthy republic." *Ashcraft v. Conoco, Inc.*, 218 F.3d 282, 287 (4th Cir. 2000). Courts in this Circuit have repeatedly applied the reporter's privilege to prevent disclosure of the kinds of records at issue here. *See, e.g.*, *Horne*, 893 F.3d at 212-13 (identity of confidential source); *Ashcraft*, 218 F.3d at 287-88 (confidential sources); *Church of Scientology Int'l v. Daniels*, 992 F.2d 1329, 1335 (4th Cir. 1993) (editors' notes, tapes, and draft articles); *Chestnut v. Kincaid*, 2022 WL 350117, at *1, 3-4 (D. Md. Feb. 4, 2022) ("audio or video recordings of statements provided or interviews conducted" for an article).[7]

Although the reporter's privilege is not absolute, the government has no plausible argument here that "society's need for the confidential information" contained on Natanson's devices—outside what is responsive to the warrant—"outweighs the intrusion on the reporter's First Amendment interests." *Ashcraft*, 218 F.3d at 287 (citing *Branzburg v. Hayes*, 408 U.S. 665, 690 (1972) (discussing privilege in criminal context)). In assessing whether the privilege is overcome, the Fourth Circuit considers "(1) whether the information is relevant, (2) whether the information can be obtained by alternative means, and (3) whether there is a compelling interest in the information." *Id.* Any attempt to defeat the reporter's privilege would be stalled at the first prong. The government executed a search warrant seeking "records received from or relating to Aurelio Luis Perez-Lugones." Latcovich Decl., Ex. A (Search and Seizure Warrant). But the non-

[7] The Post's and Natanson's sources and unpublished information are protected not only by the Fourth Circuit's reporter's privilege, but also by qualified common law protections and overlapping state shield laws, such as Washington D.C.'s shield law, which offers absolute protection to confidential sources, as well as qualified protection to unpublished newsgathering material. D.C. Code § 16-4701 *et seq.*

responsive data contained on Natanson's devices, including information about her 1,100 sources, conversations with sources, notes, recordings, draft articles, and similar materials have nothing to do with that criminal investigation and are categorically *irrelevant*. So too are the materials related to her *colleagues'* sources. Natanson Decl. ¶ 8.

That the government seized these materials as part of a criminal investigation does not erase Natanson's privilege to protect confidential sources *unrelated* to its criminal investigation. Although the Fourth Circuit has held that "reporters have no privilege different from that of any other citizen not to testify about knowledge *relevant* to a criminal prosecution," *United States v. Sterling*, 724 F.3d 482, 497 (4th Cir. 2013) (citation omitted and emphasis added), that does not mean the government can use criminal process to trample a journalist's privilege over material that is *irrelevant* to the prosecution. The Fourth Circuit has cautioned that journalists cannot be compelled to "give information bearing only a remote and tenuous relationship to the subject of the investigation," or information that "implicates confidential source relationships without a legitimate need." *Id.* (quoting *Branzburg*, 408 U.S. at 709-10 (Powell, J., concurring)). That is precisely what the government has taken here with its sweeping seizure of privileged, beyond-the-scope data. And the Fourth Circuit has further warned that the privilege will protect against efforts to "to disrupt a reporter's relationship with his news sources," *id.* at 494 (quoting *Branzburg*, 408 U.S. at 707-08 (Powell, J., concurring)), which must prevent the government from threatening to burn 1,200 confidential government sources because it has a criminal case against one individual. *See supra*.[8]

[8] The Post and Natanson preserve for later proceedings, including possible appellate proceedings, that the privilege should apply in federal criminal cases. *See, e.g.*, *United States v. Capers*, 708 F.3d 1286, 1303 (11th Cir. 2013) (information may only be compelled if highly relevant, necessary to the proper presentation of the case, and unavailable from other sources).

3. The non-responsive data is protected by the Privacy Protection Act.

Returning the non-responsive data is also reasonable because much of it is protected by the Privacy Protection Act (or PPA), which makes it "unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials." 42 U.S.C. § 2000aa(a). "Work product materials" are materials intended for publication that contain the author's "mental impressions, conclusions, opinions, or theories." *See* 42 U.S.C. § 2000aa-7(b).

The PPA exempts searches and seizures of work product related to alleged crimes committed under the Espionage Act, *see* 42 U.S.C. § 2000aa(1). The only data that even arguably could fall into that category would be any work product relating to Perez-Lugones. The seized work product that is outside the scope of the warrant remains protected. The Sixth Circuit flagged the risks relating to the search of intermingled information that includes both PPA-protected and non-PPA protected material. *Guest v. Leis*, 255 F.3d 325, 341-42 (6th Cir. 2001). In that case, the court did "not find liability under the PPA for seizure of the PPA-protected materials," but emphasized "that *police may not then search the PPA-protected materials that were seized incidentally to the criminal evidence*." *Id.* at 342 (emphasis added). Critical to the court's finding of no PPA liability was the fact that *no* protected materials had been searched when the claim was filed. *See id.* Here, the government has no legitimate interest in refusing to return the PPA-protected materials.

C. The Data Beyond the Scope of the Warrant Includes Items Protected by the Attorney-Client Privilege.

Return of the beyond-the-scope data also would be reasonable and consistent with the government's legitimate interests because it includes privileged attorney-client communications, as well as privileged communications between Natanson and her physician. *See* Natanson Decl.

¶¶ 25, 34; Latcovich Decl. ¶¶ 9, 12-14. "[T]he attorney-client privilege is 'the oldest of the privileges for confidential communications known to the common law.'" *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 172-73 (4th Cir. 2019) (quoting *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981)). The government has no legitimate interest in rummaging through The Post's or Natanson's privileged information and has no legitimate interest in preventing its return to them. *See, e.g.*, *id.* at 183 (enjoining post-seizure review protocol that authorized government review of potentially privileged materials because "[f]ederal agents and prosecutors rummaging through law firm materials that are protected by the attorney-client privilege and the work-product doctrine is at odds with the appearance of justice").

D. The Data Sought by the Warrant Is Being Preserved.

The government has seized the data already. It has represented that it is in the process of preserving the seized data. Its legitimate interest in preserving potential evidence, therefore, will be satisfied. *See United States v. Carey*, 172 F.3d 1268, 1275-76 (10th Cir. 1999) ("Because in Mr. Carey's case, officers had removed the computers from his control, there was no exigent circumstance or practical reason to permit officers to rummage through all of the stored data regardless of its relevance or its relation to the information specified in the warrant." (citation omitted)).

E. Continuing Judicial Oversight Will Protect the Government's Access to Data Within the Scope of the Warrant and Use of That Data in Other Proceedings.

Rule 41(g) expressly provides that if a court grants a motion for return of property, it "may impose reasonable conditions to protect access to the property and its use in later proceedings." Fed. R. Crim. P. 41(g). The government will no doubt assert that it has an interest in retaining possession of the materials within the scope of the warrant for use in other proceedings. Continuing judicial oversight of the return process is a reasonable condition that would vindicate

the government's claimed interest in retaining and using data within the scope of the warrant and protect The Post and Natanson's interests as well. Indeed, Rule 41(g) "contemplates judicial action that will respect both possessory and law enforcement interests." Fed. R. Crim. P. 41(g) advisory committee's note to 1989 amendment. Several leading cases have required judicial oversight, particularly where, as here, the seized documents include documents protected by the Constitution or the attorney-client privilege.

In the context of a warrant authorizing the search of a student news organization, for example, the Supreme Court acknowledged that "[t]he hazards of such warrants can be avoided by a neutral magistrate carrying out his responsibilities under the Fourth Amendment, for he has ample tools at his disposal to confine warrants to search within reasonable limits." *Zurcher*, 436 U.S. at 567; *see also, e.g.*, *In re Search Warrant Dated November 5, 2021*, 2023 WL 8868371, at *1 (S.D.N.Y. Dec. 21, 2023) (appointing special master to review seized materials potentially protected by First Amendment and attorney-client privilege and to issue report and recommendation to district court regarding disclosure of responsive, non-privileged documents to government investigators).

The Fourth Circuit has required judicial oversight of the review and return process when potentially privileged or constitutionally protected materials are at issue. *See In re Search Warrant Issued June 13, 2019*, 942 F.3d 159 (4th Cir. 2019). In that case, the government raided a law firm and seized documents protected by the attorney-client privilege and the work product doctrine, including privileged materials relating to indicted clients. The law firm sought "return of the seized property, pursuant to Rule 41(g)." *Id.* at 168. The district court approved a procedure that allowed a government filter team to review potentially privileged documents prior to return to the law firm. *Id*. at 166, 169. The Fourth Circuit rejected this procedure, which "authorized government agents

and prosecutors to rummage through" "client communications and lawyer discussions" in disregard of "the attorney-client privilege, the work-product doctrine, and the Sixth Amendment." *Id.* at 179. The Fourth Circuit held that either "the magistrate judge (or an appointed special master) — rather than the Filter Team — must perform the privilege review of the seized materials." *Id.* at 181.

Similarly, following the raid of a congressional office, a congressman moved for return of property pursuant to Rule 41(g), and the D.C. Circuit ordered return with judicial oversight of the return process to protect the constitutional interests at stake. *See United States v. Rayburn House Off. Bldg.*, 497 F.3d 654 (D.C. Cir. 2007). First, the district court was required to provide "copies of all the seized documents to the Congressman." *Id.* at 658. Thereafter, the district court, "using the copies of computer files[,]" was to "search for the terms listed in the warrant, and provide a list of responsive records to [the] Congressman"; the Congressman then had "an opportunity to review the records and, within two days, to submit, *ex parte*, any claims that specific documents are legislative in nature"; and, finally, the district court was to "review *in camera* any specific documents or records identified as legislative and make findings regarding whether the specific documents or records are legislative in nature." *Id.* As to responsive materials covered by the Speech or Debate Clause, "the Congressman [wa]s entitled, as the district court may in the first instance determine pursuant to the Remand Order, to the return of all materials (including copies)." *Id.* at 665. As to responsive materials not covered by the Speech or Debate Clause, the government was permitted to retain them "absent any claim of disruption of the congressional office by reason of lack of original versions." *Id.*

These cases and the circumstances of this seizure dictate that judicial oversight is not only reasonable, it is necessary. The supervising judicial officer can implement the details of the return process with input from the parties.

CONCLUSION

For the reasons set forth above, to remedy the unconstitutional prior restraint, The Post and Natanson respectfully request return of all seized materials and an order instructing the government to maintain, but not review, the preservation copies under seal until this matter is resolved. The Post and Natanson have an undeniable interest in, and need for, the seized data. Withholding this data would harm them irreparably, violate their constitutional rights, and constitute an unlawful prior restraint. Return is the only adequate remedy. At the very least, The Post and Natanson request return of the materials that are not responsive to the warrant, with judicial oversight of the return process. Given the important interests at stake, judicial oversight of the return process is necessary as the Fourth Circuit has recognized in analogous circumstances.

Dated: January 21, 2026

Respectfully submitted,

/s/ Simon Latcovich
Simon A. Latcovich (VSB No. 73127)
Sean M. Douglass (VSB No. 83835)
Thomas G. Hentoff (*pro hac vice* forthcoming)
Tobin J. Romero (*pro hac vice* forthcoming)
Nicholas G. Gamse (*pro hac vice* forthcoming)
WILLIAMS & CONNOLLY LLP
680 Maine Avenue SW
Washington, DC 20024
Telephone: (202) 434-5000
Facsimile: (202) 480-8371
slatcovich@wc.com
sdouglass@wc.com
thentoff@wc.com
tromero@wc.com
ngamse@wc.com

Counsel for Movant The Washington Post

/s/ Amy Jeffress
Amy Jeffress (VSB No. 36060)
Trisha Anderson (*pro hac vice* forthcoming)
HECKER FINK LLP
1050 K Street NW, Suite 1040
Washington, DC 20001
Telephone: (212) 763-0883
ajeffress@heckerfink.com
tanderson@heckerfink.com

Counsel for Movant Hannah Natanson

CERTIFICATE OF SERVICE

I hereby certify that on January 21, 2026, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Eastern District of Virginia, using the electronic case filing system of the court.

/s/ Simon Latcovich
Simon A. Latcovich (VSB No. 73127)

Counsel for the Washington Post

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

United States of America

v.

[redacted]

Case No. 1:26-sw-54

DECLARATION OF HANNAH NATANSON

I, Hannah Natanson, hereby declare as follows:

1. I am over 18 years of age, of sound mind, and otherwise competent to make this Declaration.

2. I am currently a reporter at The Washington Post ("The Post"), where I cover President Trump's reshaping of the federal government and its effects. Before that, I covered education for four years.

3. I won a George Foster Peabody Award in 2024 for a podcast series on school gun violence. I was also part of a team of Post journalists awarded the 2022 Pulitzer Prize for Public Service for coverage of the January 6, 2021 insurrection at the U.S. Capitol.

4. My additional honors include being a 2020 Finalist for the Pulitzer Prize for Breaking News Reporting (part of a team); a 2020 National First-Place Award for News Reporting from the Education Writers Association, as well as a four-time finalist for various other national awards from the Education Writers Association between 2020 and 2024; a 2024 finalist for the Poynter Journalism Prizes First Amendment Award; a 2023 Society of Professional Journalists Dateline Award for Investigative Journalism; and a 2024 Eli M. Oboler Memorial Award from the American Library Association.

5. On December 24, 2025, The Post published a story about my own reporting over the past year. That story noted that my efforts to show how President Trump has transformed government had brought me 1,169 new sources.

6. These sources included federal employees from more than 120 government agencies or subagencies. This included multiple sources from every Cabinet-level agency.

7. During the past year, relying heavily on these sources, I authored or co-authored more than 200 articles across roughly twenty news desks. That is an unusually high publication volume and variety, which speaks to the breadth of the sources I worked with and covered.

8. The materials seized from me also include information about my colleagues' sources. I shared a byline with approximately 130 reporters during the past year alone.

9. Most of these sources ultimately communicated with me through Signal, a messaging app that I could access either on my phone or computer.

10. I took steps to protect the identity of those sources.

11. On Wednesday, January 14, 2026, at approximately 6:00 AM, FBI agents showed up at my house to execute a search warrant.

12. The agents provided me a copy of the search warrant and forbade me from moving freely throughout my residence.

13. I understood from my interactions with the FBI agents that the relevant investigation was of Aurelio Luis Perez-Lugones.

14. FBI agents ultimately seized the following materials:

a. A MacBook Pro that is owned by The Post and that I used for work;

b. A second silver MacBook Pro that I personally own but also previously used for work;

c. An iPhone that The Post owns that I used for work;

d. A 1 TB portable hard drive;

e. A Garmin running watch that I personally own; and

f. A voice recorder that is owned by The Post that I used for work.

15. I used my Post computer for work. In particular, I sent and received emails and documents using Microsoft Outlook, Slack, and Signal and also communicated through text messages and phone calls.

16. I have reviewed a Post IT Department report that shows I sent and received more than 30,000 emails over the last year alone. My Post computer kept local copies of emails in Outlook.

17. When my Post computer was seized, I believe that I was logged into Proton Drive, which is a cloud-based service that I used to save sensitive information in an encrypted form, including confidential information derived from sources and notes on story concepts and ideas.

18. When my Post computer was seized, I believe that I was also logged into Google Drive. That is another cloud-based service that I used to save information, including confidential information derived from sources and notes on story concepts and ideas. In addition, my colleagues use this platform to share information for reporting with me.

19. I also used my computer to draft and edit potential stories.

20. I also used Slack on my computer. Slack is a messaging system that permits users to create various "channels," which are text conversations between different groups of users. Post reporters and editors use these channels (in addition to direct messages) to communicate about sources and stories. For example, I am a participant in numerous specific Slack channels and direct message communications regarding:

a. Reporters sharing confidential information about sources and stories;

b. Editors sharing confidential information about sources and stories;

c. Ongoing lines of coverage;

d. Special story channels; and

e. Conferring about edits on stories, including prepublication review and legal advice, with my editors.

21. Slack is how the Post newsroom often shares information from sources, originates and debates story ideas, and discusses edits to draft stories. Thus, having access to Slack is like having access to the Post newsroom.

22. I also used Ellipsis on my computer. Ellipsis is The Post's content management system. It provides an enormous window into The Post's journalism, with all stories in progress. Thus, having access to Ellipsis is like having access to the Post newsroom.

23. I similarly used my iPhone for work. My iPhone included Signal, Slack, and email apps in addition to text messages and phone calls that I used to communicate.

24. My iPhone included the Outlook app, which stored emails from my Post email account, my personal Gmail account, and a Gmail account that I use for news alerts.

25. My personal Gmail account contains personal information, including medical information, financial information, and even information about my wedding planning.

26. My phone also contains text messages, including some text messages with confidential sources.

27. My phone also contains voice recordings with confidential sources.

28. I use my other Gmail account in part to create news alerts to track potential story ideas.

29. In the last year, I communicated with sources primarily using Signal, although I also communicated with some sources via email, text, phone, and other channels.

30. I previously used my personal computer for work. I had not used that computer for work for approximately nine months, but that computer also contained Outlook, which included locally stored emails from my Post account and two Gmail accounts. I also used Slack on that computer. The messages stored locally on that computer likely date back further than those on my Post computer.

31. I regularly communicated with other reporters and editors about sources and other material and information I gathered as part of the newsgathering process. These communications would occur via email, Slack, Signal, text messages, or phone calls.

32. These communications would include information gathered from confidential sources, including sources that were not my own (i.e., my colleagues' sources), and including information that was never published.

33. These communications regarding sources and other material I gathered as part of the newsgathering process would be on my computers and phone.

34. Moreover, I would sometimes communicate with Post lawyers when I needed legal advice about sourcing or a story. That said, it was more common for my editors to consult legal counsel and receive advice in connection with my reporting, which would then be reflected in communications from the editor to me. This advice could be conveyed through all channels of communication with my editors, including but not limited to email, Signal, Slack, and text messages.

35. The voice recorder seized by the government houses recordings of interviews going back years. Many of these recorded conversations include information provided confidentially by sources.

36. The government has not returned any of the seized property.

37. The search warrant at issue references Aurelio Luis Perez-Lugones. I never communicated with him via any platform other than Signal or phone. I never used any other platform discussed above to communicate with him (e.g., email or my voice recorder).

38. Given the huge volume of materials the government seized, any government review of the materials will necessarily expose information relating to confidential sources, unpublished newsgathering, and other journalistic work product that has nothing whatsoever to do with Perez-Lugones.

39. In my experience, sources strongly prefer to communicate via secure messaging services such as Signal because they fear retribution from the government due to their disclosures. For example, I have communicated with more than 1,200 confidential sources via Signal during the first year of the Trump administration alone. Every day, on average, I would receive somewhere between dozens and over 100 tips from these sources. Since the seizure, that number has fallen to zero.

40. I need my devices back to do my job.

41. I also need my devices back to help my colleagues do their jobs. An enormous part of my role in the newsroom was to develop tips for news stories that I would then pass off to colleagues or use to partner with them on future reporting.

42. The government's seizure of all of my devices has eliminated my ability to collect information and publish news stories.

43. For example, I no longer have access to my more than 1,200 Signal contacts or communications with any of my sources. I literally cannot contact them without access to my devices. Nor can I review my past messages with them on Signal.

44. The government's seizure of my devices has restrained my ability to publish stories that I was actively working on at the time of the seizure. As a journalist, I am constantly working on dozens of potential leads and articles at any one time. At the time of the seizure, I was in particular working on three short-form stories which I expected to publish soon, along with four medium-term stories, four long-term, sensitive stories, one audio project, and two narrative/investigative story series intended to span 2026. But I have been unable to work on or publish any of those articles since the seizure.

45. In addition, the government's seizure of my devices has also further limited my ability to engage in newsgathering with future stories for publication that were not even in development at the time of the raid. I have stopped receiving tips through my Signal, which was a primary source for story ideas for myself and for the Post newsroom.

46. Without access to my devices, I cannot contact my sources. Even if I am ultimately able to reconnect with my sources, there is a substantial likelihood that they will be deterred by the government's seizure of my devices from communicating with me in the future. The longer my devices remain in possession of the government and I am not able to contact my sources, the greater the likelihood that my sources will be reluctant to speak with me in the future. If my sources become aware that the government has access to, or is reviewing, my source information, the harm to my newsgathering efforts will be even greater.

I declare under penalty of perjury that the foregoing is true and correct according to the best of my knowledge, information, and belief.

Executed this 20 day of January, 2026.

Hannah Natanson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In the Matter of the Search of the Real Property and Premises, Alexandria, VA	Case No. 1:26-sw-54

DECLARATION OF BRETT A. ROBERSON

I, Brett A. Roberson, hereby declare as follows:

1. I am over 18 years of age, of sound mind, and otherwise competent to make this Declaration.

2. I am a Director at AlixPartners, LLP, a global business consulting firm, where I have been a senior member of the digital forensics investigation team since 2007. AlixPartners has been engaged by Williams & Connolly to provide digital forensic services in conjunction with this matter.

3. I am familiar with the facts in this declaration, from either personal knowledge or from documents that have been provided to me. Insofar as they are within my own knowledge, the facts and matters in this declaration are true to the best of my own knowledge and belief and, if called upon to testify, I would testify competently thereto.

4. I began my digital forensics career in 2005 with Deloitte's computer forensic investigations practice group, and since that time have been providing federal, state, local, and tribal courts and governments, along with companies around the world, with digital forensics and

related investigative services. I earned a Bachelor's degree in Business Administration and International Studies from Abilene Christian University, in Abilene, Texas. I hold and have held several digital forensic and technology certifications including the Certified Information Systems Security Professional (CISSP) and OpenText's EnCase® Certified Examiner (EnCE), for which I am currently in process of recertifying.

5. A copy of my curriculum vitae is provided at the end of this declaration as Attachment 01.

Slack Description

6. Slack is a widely used workplace communication platform and service that offers access via desktop applications, web browsers, and mobile devices. The desktop application is available for the Windows, macOS, and Linux operating systems.

7. In the normal course of operation, the Slack desktop application stores user data locally on the device where it is installed. Based on my professional experience and through forensic analyses of Slack installations, the desktop application typically stores data in predictable, discoverable locations on the local file system and contains:

a. SQLite databases containing message history, channel information, and user data;

b. Cache files containing downloaded files, images, and other attachments;

c. Log files recording application activity and user actions;

d. And IndexedDB and Local Storage data containing application state and user preferences.

8. The data stored by the Slack desktop application is not encrypted at rest by default on the local file system. It is stored in standard database formats (primarily SQLite) and file system structures that are readily accessible using standard forensic tools and techniques.

9. In my professional opinion, this data storage behavior occurs automatically in the normal course of the application's operation, without any special configuration or user action required. Users do not need to take affirmative steps to cause this data to be stored locally; it is the default behavior of the application.

10. Standard digital forensic methodologies can be applied to extract, preserve, and analyze this locally stored data in a forensically sound manner, maintaining chain of custody and data integrity.

11. The locally stored data may include messages, files, and other communications that were transmitted through the Slack platform during the period the application was in use on the subject device.

12. I declare under penalty of perjury that the foregoing is true and correct according to the best of my knowledge, information, and belief.

Executed this 20th day of January 2026.

Brett A. Roberson

ATTACHMENT 1

AlixPartners

CURRICULUM VITAE
OF
Brett A. Roberson

POSITION	Director, AlixPartners, LLP, Dallas, Texas
EDUCATION	B.A. in Business Administration and International Studies, Abilene Christian University
PROFESSIONAL HISTORY	Mr. Roberson has more than 25 years of experience in information technology and as a forensic investigator and manager. Beginning in 2005, he has continuously provided computer forensic consulting and electronic discovery services for many matters. Mr. Roberson has a wide range of experience with information technology infrastructure and security, forensic acquisition and forensic analysis, including computer tampering, contractual disputes, employment matters, network intrusions, intellectual property theft, and fraud.
PROFESSIONAL EXPERIENCE	Mr. Roberson has extensive experience providing design and installation of information technology infrastructures and network security administration. He has provided technical expertise in criminal and civil investigations. As a Director for a global consulting firm, Mr. Roberson has also been tasked with development of policies and procedures, case management, quality control workflows and resource allocation.
RANGE OF EXPERIENCE	Mr. Roberson has performed a variety of services related to computer forensics and investigations. A sample of these includes: • Computer forensics investigations • Detection of intellectual property theft • Analysis of a computer/cloud user's actions over specific time periods • Recovery of deleted files • Forensic analysis of electronic document authenticity and metadata • Defensible forensic collection of ESI • Filtering and searching for responsive documents and the de-duplication of mass ESI • Client site assessment of ESI, assistance with identification of

items potentially responsive to eDiscovery obligations
- Remote forensic imaging and analysis

ACCREDITATIONS AND LICENSES	EnCase® Certified Examiner (EnCE), Guidance Software – Recertification in Process CCE Certification in Process GIAC GCFR Certification in Process
ADDITIONAL TRAINING AND EDUCATION	SANS FOR509 – Enterprise Cloud Forensics and Incident Response – IN PROGRESS Magnet Axiom Investigations Apple iOS Mobile Forensics, Blackbag Technologies Intermediate Apple OSX Hardware and Software Forensics – Blackbag Technologies EnCase NTFS, Guidance Software CISSP Training and Certification (Does Not Possess Cert Post-Expiry) EnCase Advanced Internet & Email Examinations, Guidance Software EnCase Internet & Email Examinations, Guidance Software EnCase Intermediate Computer Forensics, Guidance Software EnCase Level 1 Computer Forensics, Guidance Software Interrogation and Elicitation Techniques, BIA Private Investigations Skip Tracing, Surveillance and Interrogation and Elicitation Techniques, PIEducation Intermediate Microsoft SQL Training - LearningTree
Testimony	January 2021: Provided deposition testimony related to iOS backup data recovery in Securities and Exchange Commission v Eric Pulier. In the United States District Court; Central District of California. Case No. 17-CV-07124-PSG (RAOx).
Other Relevant	Managed and conducted forensic analyses focusing on document and

Experience

email forgery allegations on a high-profile cryptocurrency dispute. Prepared for Federal court testimony as expert witness for defense counsel.

Performed a deep dive analysis of PDF documents in which a vendor representative altered invoices to a client to inflate the receivables by over USD $300,000.

Managed and conducted investigation of financial services firm employee allegedly performing identity theft and wire fraud that led to separation of the employee and court ordered remuneration. Additional examination for company around obligations to inform client and public re: potential data breach. Analysis yielded significant attempts at obfuscation of web browser history and stolen login information.

Conducted high profile forensic imaging and analysis of over 400 laptops, desktops and mobile devices involved in mobile device hacking incident by a global media conglomerate.

Provided numerous sworn affidavits and declarations regarding the validity and admissibility of various forensic artifacts, computing and mobile devices, and cloud data sources.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

United States of America

v. [redacted]

Case No. 1:26-sw-54

DECLARATION OF SIMON A. LATCOVICH

I, Simon A. Latcovich, hereby declare as follows:

1. I am over 18 years of age, of sound mind, and otherwise competent to make this Declaration.

2. I am a partner at the law firm Williams & Connolly LLP. I am licensed to practice law in the District of Columbia, Maryland, and Virginia, and I am in good standing with the bars of these jurisdictions. I was first admitted to the bar over 19 years ago.

3. Williams & Connolly LLP represents The Washington Post ("The Post") in this matter.

4. The evidence set out in this Declaration is based on my personal knowledge.

5. On January 14, 2025, at approximately 6:00 AM, the government executed a search warrant at the residence of Hannah Natanson, a reporter for The Post. A true and correct copy of that Search and Seizure Warrant is attached as Exhibit A.

6. The government seized numerous electronic devices, including a MacBook computer with 512GB of memory, an iPhone, and a voice recorder that are owned by The Post. The government also seized a MacBook computer owned by Ms. Natanson. Ms. Natanson was

authorized to and in fact did work for The Post on all of these devices. A true and correct copy of the Receipt for Property is attached as Exhibit B.

7. A true and correct copy of the Aurelio Luis Perez-Lugones Complaint and Affidavit in support is attached as Exhibit C.

8. A true and correct copy of the grand jury subpoena served on The Post on January 14, 2026, is attached as Exhibit D.

9. On January 14, 2026, the same day the FBI raided Ms. Natanson's residence, I reached out to the government to advise that the seized items contain materials protected by the First Amendment and the attorney-client privileges. A true and correct copy of my email correspondence is attached as Exhibit E. I asked the government to refrain from reviewing the documents pending a discussion. *See id.*

10. On January 15, 2026, the parties conferred regarding the seized documents. No agreements regarding the handling of the data were reached because government counsel asserted that all issues had to be vetted with more senior government officials. The government also represented that it was in the process of extracting data from the devices and preserving data, and that it was not reviewing content, but would begin to do so soon.

11. On January 16, 2026, the parties conferred twice regarding the seized data. I proposed a process that would involve the government's preservation of the seized data, returning the seized property, and reviewing only the identified responsive material, if any, identified by counsel for The Post and Natanson.

12. After conferring with the unnamed, more senior officials, the government called back that same day and rejected this proposal, but agreed that it would not begin a substantive review of the seized data pending further discussion on Tuesday, January 20, 2026. The

government asked us to provide a list of attorney names on January 20 to assist in a privilege review. I explained that a list of attorney names would be an inadequate basis to screen privileged information because editors at The Post, as opposed to reporters, generally request and receive legal advice from attorneys and then disseminate that advice to reporters.

13. I also explained that a list of attorney names would not address the significant First Amendment privilege issues and asked for further time to discuss these complex issues before the government commenced its review. The government expressed doubt that the unnamed, senior officials would agree to a proposal designed to protect the significant First Amendment interests at stake.

14. On January 20, 2026, I explained that we were still concerned about the First Amendment and attorney-client privilege issues and proposed that the government return the seized property and that we would treat the devices as covered by the grand jury subpoena served on The Post.

15. The government rejected this proposal.

16. I then informed the government that we intended to seek judicial relief and would file a motion within twenty-four hours. I noted that Judge Rushing on the Fourth Circuit had previously written in a similar Rule 41(g) matter that, "In other cases, the government has voluntarily delayed review for a brief time until the court could schedule a hearing on the target's motion for a restraining order or injunction. That sensible procedure preserves the status quo until a court can rule." *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 184 (2019) (citation omitted).

17. The government stated that it would not refrain from conducting a substantive review of the seized material pending judicial resolution of this dispute. Instead, the government

was continuing to process documents and would review them as soon as that process was done. The government would not agree to inform us even when it began a substantive review.

18. Moreover, the government refused to take a position one way or the other on any protocol to protect either attorney-client privilege or First Amendment privileges.

19. To be clear, the government would not represent that it intended to undertake any process to protect First Amendment privileges.

I declare under penalty of perjury that the foregoing is true and correct according to the best of my knowledge, information, and belief.

Executed this 20th day of January 2026.

Simon A. Latcovich

EXHIBIT A

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

Type text here

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The Real Property and Premises at [redacted]

Case No. 1:26sw 54

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

The real property and premises at [redacted] described on Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime further described in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before January 27, 2026 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to William B. Porter.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: January 13, 2026, at 9:45 p.m

Judge's signature

City and state: Alexandria, VA

William B. Porter, United States Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 1:26sw 54	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

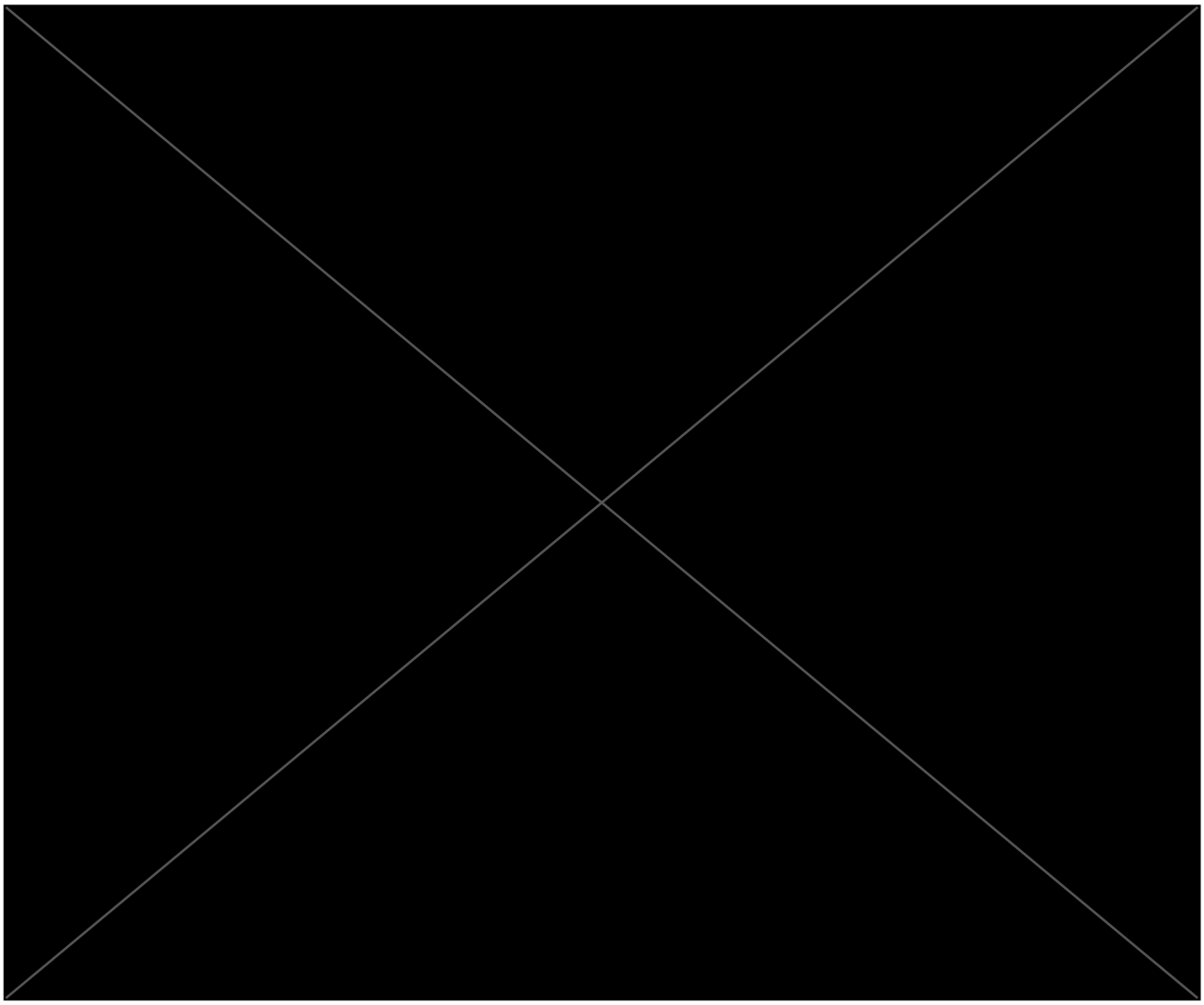
Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-1 (Real Property)

Residence to Be Searched



ATTACHMENT B

Items to be Seized

All digital devices,[1] other electronic storage media,[2] or components of either identified during the searches that are reasonably believed to be used by Natanson (collectively, the "NATANSON ELECTRONICS"), including a mobile phone associated with the number 202.580.5477, the search of which must be limited to all records and information, including classified and/or national defense information, from the time period October 1, 2025, to the present, which constitute records received from or relating to Aurelio Luis Perez-Lugones, as evidence of violations of 18 U.S.C. § 793. Additionally, as necessary to effectuate the search and seizure of the foregoing, this warrant also authorizes the seizure of the following for the same period of October 1, 2025, to the present:

a. Notations of any password that may control access to a computer operating system or individual computer files;

b. Evidence of the attachment to the NATANSON ELECTRONICS of other storage devices or similar containers for electronic evidence;

c. Evidence of counter forensic programs (and associated data) that are designed to eliminate data from the NATANSON ELECTRONICS;

d. Evidence of the times the NATANSON ELECTRONICS was used;

e. Passwords, encryption keys, and other access devices that may be necessary to access the NATANSON ELECTRONICS;

f. Documentation and manuals that may be necessary to access the NATANSON ELECTRONICS or to conduct a forensic examination of the NATANSON ELECTRONICS; and,

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), Pods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include thumb/flash drives, SD cards, hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. Surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. Performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the Target Offense that are the matter of the investigation.

If after performing these procedures, the directories, files, or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file, or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated, absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

Biometric Unlock

During the execution of the search of HANNAH NATANSON as described in Attachment A-3, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of HANNAH NATANSON to the fingerprint scanner of the device; (2) hold a device found during the search in front of the face of HANNAH NATANSON and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that an occupant state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel an occupant to state or otherwise provide that information. However, the voluntary disclosure of such information by an occupant is permitted. To avoid confusion on that point, if agents in executing the warrant ask an occupant for the password to any device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

EXHIBIT B

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # WF-415979S

On (date) JANUARY 14, 2026

item(s) listed below were:
- [x] Received From
- [ ] Returned To
- [ ] Released To
- [ ] Seized

(Name)

(Street Address) [redacted]

(City)

Description of Item(s):

(1) HS HANDY RECORDER S/N 22313 in case
(1) SILVER MACBOOK PRO MODEL A2442 S/N FRW577Y6GN in case
(1) 1TB SEAGATE PORTABLE DRIVE MODEL SRDØØF S/N NA7Q49SF
(1) SILVER MACBOOK PRO MODEL A2442 S/N TFQC597H41 with charging cable
(1) PURPLE GARMIN FORERUNNER 165 S/N 8A2015865 with charging cable
(1) PINK iPHONE with black case and white charging cable + stand

Received By: (Signature)

Received From: (Signature)

EXHIBIT C

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America)
v.)
)
Aurelio Luis Perez-Lugones) Case No. 1:26-mj-00045-CJC
)
)
)
)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 8, 2026 in the county of Howard County in the _____ District of Maryland, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §793(e)	Unlawful retention of national defense information

This criminal complaint is based on these facts:

See affidavit.

☑ Continued on the attached sheet.

Complainant's signature

SA Keith Starr, FBI
Printed name and title

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: January 9, 2026

Judge's signature

City and state: Baltimore, Maryland

Chelsea J. Crawford, US Magistrate Judge
Printed name and title

PCM/TMS: USAO 2025R00683

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	
v.	*	**CASE NO.** 1:26-mj-00045-CJC
	*	
AURELIO LUIS PEREZ-LUGONES,	*	
	*	
Defendant	*	
	*	
	*******	

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Keith Starr, being duly sworn, declare and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since 2021. I am currently assigned to the FBI Washington Field Office. I have spent most of my time as an FBI Special Agent working national security investigations, including the mishandling of classified information. I am assigned to the Counterintelligence Division at the FBI's Washington Field Office. I investigate, among other things, offenses involving the unauthorized disclosure of classified information to those not entitled to receive the same, including members of the media. I use a variety of techniques to conduct these investigations, including writing and executing search warrants, interviewing witnesses, victims, and subjects, and conducting arrests. In my current position, I am responsible for conducting and assisting in investigations into the activities of individuals whose conduct may constitute a threat to national security and/or a violation of federal law. As a result of my training, education, and experience, I am familiar with the manner in which criminal activity is carried out, and the efforts of persons involved in such activity to avoid detection by law enforcement. As a Special Agent of the FBI, I am authorized to investigate violation of laws of the United States, and execute warrants issued under the authority of the United States.

2. I make this affidavit in support of a criminal complaint charging that, on or about January 8, 2026, in the District of Maryland and elsewhere, the Defendant, **AURELIO LUIS PEREZ-LUGONES** ("**PEREZ-LUGONES**"), committed the offense of unlawful retention of national defense information, in violation of 18 U.S.C. § 793(e).

3. Unless otherwise noted, the conclusions and beliefs expressed in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I have drawn from my training, experience, and knowledge of the investigation. The facts contained in this affidavit come from my review of the evidence, my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. Except as explicitly set forth below, I have not distinguished in this affidavit between facts of which I have personal knowledge and facts of which I have hearsay knowledge. This affidavit is intended only to demonstrate that probable cause exists in support of the requested criminal complaint, and does not include all information known to me or to other law enforcement officers regarding this investigation.

STATUTORY AUTHORITY AND DEFINITIONS

4. Under 18 U.S.C. § 793(e), "[w]hoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or

willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it [commits a federal offense.]"

5. Under Executive Order 13526, the unauthorized disclosure of material classified at the "TOP SECRET" level ("TS"), by definition, "reasonably could be expected to cause exceptionally grave damage to the national security" of the United States. Exec Order 13526 § 1.2(a)(1), 75 Fed Reg. 707, 707-08 (Jan. 5, 2010). The unauthorized disclosure of information classified at the "SECRET" level ("S"), by definition, "reasonably could be expected to cause serious damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(2). The unauthorized disclosure of information classified at the "CONFIDENTIAL" level ("C"), by definition, "reasonably could be expected to cause damage to the national security" of the United States. Exec. Order 13526 1.2(a)(3).

6. Sensitive Compartmented Information ("SCI") is classified information related to intelligence sources, methods, and analytical processes. SCI is to be processed, stored, used, or discussed in an accredited Secured Compartmented information Facility ("SCIF"), and only individuals with the appropriate security clearance and additional SCI permissions are authorized to access such classified national security information. For a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

7. Pursuant to Executive Order 13526, information classified at any level shall be lawfully accessed only by persons determined by an appropriate United States government official to be eligible for access to classified information, who has signed an approved non-disclosure agreement, who has received a security clearance, and who has a "need to know" the classified information. Classified information shall only be stored or discussed in an approved facility.

PROBABLE CAUSE

PEREZ-LUGONES' U.S. Government Employment and Access to Classified Information

8. **PEREZ-LUGONES** is a United States citizen born in Miami, Florida, and now lives in Laurel, Maryland. **PEREZ-LUGONES** was a member of the United States Navy from 1982 to 2002. From 1995 to 2002, as a member of the United States Navy, **PEREZ-LUGONES** held a Top Secret security clearance. **PEREZ-LUGONES** has been a Government contractor in various capacities since 2002.

9. Currently, **PEREZ-LUGONES** works as a systems engineer and information technology specialist for a Government contracting company whose primary customer is a Government agency. **PEREZ-LUGONES'** workplace is in Annapolis Junction, Maryland. **PEREZ-LUGONES'** workplace is owned and operated by another Government contracting company. **PEREZ-LUGONES'** role is administrative. **PEREZ-LUGONES** has access to classified systems so that he can maintain, support, and optimize various computer systems, networks, and software. **PEREZ-LUGONES** is a system administrator with heightened access to classified systems, networks, databases, and repositories as required for his job.

10. Due to his employment, **PEREZ-LUGONES** possesses a Top Secret security clearance with access to SCI.

11. **PEREZ-LUGONES** has had access to SCI since at least 2000. As a security clearance holder, **PEREZ-LUGONES** has received instruction on the proper handling of classified information, including the proper storage of classified information. As part of his employment, **PEREZ-LUGONES** was also required to take regular, annual training that included refresher training on the proper marking and handling of classified information.

12. In September 2025, **PEREZ-LUGONES** took and passed a web-based training on handling classified information and a web-based training on the unauthorized disclosure of classified information.

13. Because **PEREZ-LUGONES** held a security clearance in the United States Navy and as a Government contractor, the Government entrusted **PEREZ-LUGONES** with access to classified information and national defense information so long as he needed to know that information to perform his job.

14. Absent a work-related reason to access those systems, **PEREZ-LUGONES** is not authorized to access classified systems, networks, databases, or repositories, nor is he permitted to view or print the classified information from classified systems.

PEREZ-LUGONES' Printing of Classified Materials

15. On several occasions since at least October 2025, while having authorized access to classified systems, **PEREZ-LUGONES** navigated to and searched databases or repositories containing classified information without authorization. There, **PEREZ-LUGONES** accessed and viewed classified intelligence reports or summaries of classified intelligence reports. Those reports or report summaries were produced, created, or maintained by several Government agencies.

16. On October 28, 2025, **PEREZ-LUGONES** used databases or repositories to search for, access, and view a classified intelligence report related to a foreign country ("Country 1"). That report was classified Top Secret. **PEREZ-LUGONES** took a screenshot of the report and pasted that screenshot in a Microsoft Word document titled "Microsoft Word – Document1."

17. Notably, **PEREZ-LUGONES'** screenshot of the report rendered one of the four bullet points at the end of the report illegible due to how the screenshot was cropped.

18. **PEREZ-LUGONES** also opened an attachment to that report, took screenshots of the attachment, and pasted those screenshots into the same Microsoft Word document.

19. Afterward, **PEREZ-LUGONES** printed the Microsoft Word document hours before logging off the system for the day. The illegible bullet point referenced above is also illegible in the printed version of the Microsoft Word document.

20. **PEREZ-LUGONES** had no need to know and was not authorized to search for, access, view, screenshot, or print any of this information.

21. **PEREZ-LUGONES** should be aware, based on his training and experience as a security clearance holder, that he cannot remove classified information from a SCIF without authorization, proper packaging, and a government-issued courier card.

22. **PEREZ-LUGONES** did not have authority to remove any classified or sensitive information. **PEREZ-LUGONES** did not receive specific requests to search for, access, view, screenshot, or print the classified or sensitive reports referenced above, nor did he have a need to conduct those searches.

23. **PEREZ-LUGONES'** job duties do not include accessing, viewing, printing, or manipulating classified information or defense information of any kind related to Country 1. **PEREZ-LUGONES'** job duties are limited to administrative tasks, which were described above.

24. Government security clearance holders are aware, often through mandatory in-person or web-based training, that Government classified systems are or can be monitored by the sponsoring agency, which can include monitoring printing activity.

25. An individual may try to avoid creating an obvious record of printing activity (*e.g.*, avoid printing a document with classification markings in the file name, which would reflect that the document being printed is classified) by taking screenshots of classified information and printing those screenshots or pasting those screenshots in a text document. This type of activity

would obfuscate the title of the printed document, making it seemingly innocuous, but it would not necessarily obfuscate the content of the printed document.

26. **PEREZ-LUGONES'** employer can retrieve records of print activity on classified systems, including copies of printed documents.

27. **PEREZ-LUGONES** printed on classified systems during the times described above.

28. **PEREZ-LUGONES'** employer retrieved copies of the documents **PEREZ-LUGONES** printed on October 28, 2025.

29. As described above, a review of **PEREZ-LUGONES'** printing activity on that dates showed that he had printed innocuous sounding documents (i.e., Microsoft Word – Document 1) that really contained classified and sensitive reports.

NOTETAKING

30. On January 5, 2026, **PEREZ-LUGONES** accessed and viewed a classified intelligence report related to Government operational activity. The report was classified up to Secret, and was maintained on databases or repositories.

31. On January 6, 2025, **PEREZ-LUGONES** left his residence for his workplace in his vehicle at about 8:00 a.m. He arrived at and entered the workplace at around 8:15 a.m. Shortly thereafter, **PEREZ-LUGONES** logged onto the classified system.

32. At around 4:00 p.m., **PEREZ-LUGONES** left the SCIF and then returned to the SCIF a short time later. At around 4:10 p.m., **PEREZ-LUGONES** picked up a yellow notepad, examined and removed approximately three pages, folded those pages in half, and set those pages on his desk. **PEREZ-LUGONES** then gathered his things, picked up the pages he had removed from the notepad, and left his desk area with the pages in hand. **PEREZ-LUGONES** left the

workplace at around 4:25 p.m., with a black bag. **PEREZ-LUGONES** was observed looking around the workplace parking garage before entering his vehicle and driving to his residence.

33. After leaving the workplace on January 6, 2026, **PEREZ-LUGONES** arrived at his residence at around 4:41 p.m. **PEREZ-LUGONES** did not leave his residence the rest of the night.

34. The following day, January 7, 2026, **PEREZ-LUGONES** left his residence for the workplace in his vehicle at around 8:00 a.m., arriving at around 8:11 a.m. Shortly thereafter, **PEREZ-LUGONES** logged on to the classified system.

35. At around 9:00 a.m., **PEREZ-LUGONES** took notes on a yellow notepad. Throughout the morning, **PEREZ-LUGONES** looked back and forth between the screen corresponding the classified system and the notepad, all the while writing on the notepad.

36. At around 10:52 a.m., on January 7, 2026, **PEREZ-LUGONES** left his desk with a yellow notepad page, leaving the workplace, getting into his vehicle, and driving to his residence.

A Search of PEREZ-LUGONES' Car and Residence Revealed Documents Marked as Classified

37. On January 8, 2026, a federal court issued search warrants authorizing the search of **PEREZ-LUGONES**'s residence in Laurel, Maryland, as well as his vehicle, and other locations. The searches were conducted the same day.

38. While searching the authorized areas listed above, investigators located multiple documents that were marked as SECRET.

39. While searching **PEREZ-LUGONES**'s car, investigators located a lunch box in which a document was marked as SECRET. Prior video surveillance observed **PEREZ-LUGONES** at his cubicle in the SCIF at his workplace looking at this same document on January 8, 2026. Additional prior investigation of **PEREZ-LUGONES** in the SCIF at his workplace also identified him removing the classification header/footer markings from this document prior to leaving his workplace. The document identified in the lunch box by investigators during the authorized search of **PEREZ-LUGONES**'s car was the same classified document without the classification header/footer markings that **PEREZ-LUGONES** was seen handling in the SCIF at his workplace.

40. While searching **PEREZ-LUGONES**'s residence, investigators located a document in the basement of the residence marked as SECRET.

41. One or more of these documents are related to national defense.

CONCLUSION

42. I submit that this affidavit establishes probable cause in support of a criminal complaint charging **PEREZ-LUGONES** with the unlawful retention of national defense

information, in violation of 18 U.S.C. § 793(e), and thus respectfully request that the Court issue a complaint charging **PEREZ-LUGONES** with that offense.

Respectfully submitted,

Keith Starr
Special Agent
Federal Bureau of Investigation

Affidavit submitted by e-mail and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 9th day of January, 2026.

HONORABLE CHELSEA J. CRAWFORD
UNITED STATES MAGISTRATE JUDGE

EXHIBIT D

2025R00683 - 009

AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

UNITED STATES DISTRICT COURT

for the

District of Maryland

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To: The Washington Post
Attention: John B. Kennedy, General Counsel & Labor
1301 K Street NW
Washington, DC 20071

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place:	Date and Time:
United States District Court, Baltimore 101 W. Lombard Street, 8th floor Baltimore, MD 21201	Wednesday January 28, 2026 9:00 AM

YOU MUST also bring with you the following documents, electronically stored information, or objects (blank if not applicable):

See Attached.

In lieu of personal appearance, you may comply with this subpoena by submitting the requested information to the person named on the Attachment.

Date: January 14, 2026

Catherine M. Stavlas
Signature of Clerk or Deputy Clerk

The name, address, and telephone number of the United States Attorney, or Assistant United States Attorney, who requests this subpoena, are:

Kelly O. Hayes, United States Attorney/Michael Hanlon, Assistant United States Attorney
36 S. Charles Street, 4th Floor Baltimore, MD 21201
410-209-4800

USAO#2025R00683-009

ATTACHMENT

The Washington Post
1301 K Street NW
Washington, D.C. 20071
Attention: John B. Kennedy, General Counsel & Labor

Please provide the following records and information, for the time period October 1, 2025, to the present, regarding Aurelio Luis Perez-Lugones ("Perez-Lugones") in the custody and control of The Washington Post:

a. Records of communications between any Washington Post employee and Perez-Lugones, including but not limited to voice, electronic mail, voicemail, text message, and encrypted application communications, in whatever form; and

b. All records received by the Washington Post from Perez-Lugones, including but not limited to any documents marked classified, and any notes taken from documents marked classified.

Provide the responses and direct any questions to:

Special Agent Matthew Johnson
Federal Bureau of Investigation
601 4th Street NW, Washington D.C. 20535
Telephone: 202-278-2000

CERTIFICATION UNDER FEDERAL RULES OF EVIDENCE 803(6) AND 902(11)

I HEREBY CERTIFY that I, _____, am the Custodian of Records for _____ (NAME OF BUSINESS*)[1]. I further certify that:

1. The attached record, consisting of _____ pages, is a true and correct copy / original record of _____ (NAME OF BUSINESS), hereafter "the business", which is maintained by me or under my supervision;

2. It is the regular practice of the business to make and maintain such records;

3. The records were made at or near the time of the occurrence(s) reflected thereon;

4. The records were made by a person or persons with knowledge, or from information transmitted by a person with knowledge of the matters contained thereon.

5. I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____ Date

_____ Signature

_____ Name (Typed or Printed)

_____ Title

[1] The term "business" includes business, institution, association, profession, occupation and calling of every kind, whether or not conducted for profit.

EXHIBIT E

From: Latcovich, Simon
To: Michael.Hanlon@usdoj.gov
Cc: Romero, Tobin; Gamse, Nicholas
Subject: RE: Washington Post / Natanson
Date: Wednesday, January 14, 2026 6:56:09 PM

Michael,

Tried to reach today, but sorry we did not connect. We would like to discuss a review protocol for the documents seized today pursuant to a search warrant given that they contain materials protected by the attorney-client privilege and the First Amendment. Please don't begin a review process until we have had a chance to confer. We are happy to do so at your convenience.

Best regards,
Simon

Simon Latcovich
Williams & Connolly LLP
680 Maine Avenue SW, Washington, DC 20024
202-434-5967 | vcard | www.wc.com/slatcovich

From: Latcovich, Simon <SLatcovich@wc.com>
Sent: Wednesday, January 14, 2026 4:14 PM
To: Michael.Hanlon@usdoj.gov
Subject: Washington Post / Natanson

Michael,

Good afternoon. I just left you a voicemail. Could you please give me a call about the Washington Post matter? Thanks.

Best regards,
Simon

Simon Latcovich
Williams & Connolly LLP
680 Maine Avenue SW, Washington, DC 20024
202-434-5967 | vcard | www.wc.com/slatcovich