



CALLI LAW, LLC
One Flagler Building, Suite 1100
14 Northeast 1st Avenue
Miami, Florida 33132
T. 786.504.0911
F. 786.504.0912
www.calli-law.com

PETITION FOR RETURN OF PROPERTY

Re: *In re Search Warrant dated November 5, 2021*, 21 Misc. 813 (AT)
In re Search Warrant dated November 3, 2021, 21 Misc. 819 (AT)
In re Search Warrant dated November 3, 2021, 21 Misc. 825 (AT)

Related to: 20 Mag. 12614
20 Mag. 12623
21 Mag. 548
21 Mag. 992
21 Mag. 2537
21 Mag. 2711
21 Mag. 3884

TABLE OF CONTENTS

	Page
INTRODUCTION	1
I. FACTUAL BACKGROUND.....	3
A. Project Veritas’ Lawful Receipt of the Abandoned Ashley Biden Diary	3
B. The U.S. Attorney’s Office/Federal Bureau of Investigation Inquiry and Seizures	7
1. The PV Warrants.....	7
2. Protocol to Protect Privileged Materials Seized from Project Veritas.....	10
3. The Microsoft Warrants.....	12
II. SUMMARY OF ARGUMENT	14
III. LEGAL STANDARDS	14
IV. ARGUMENT	16
A. The Use of Search Warrants to Seize Work Product and Documentary Materials Belonging to Project Veritas and Its Journalists Violated the Privacy Protection Act	16
B. The Use of Search Warrants to Seize Work Product and Documentary Materials Belonging to Project Veritas and Its Journalists Violated the First Amendment.....	20
C. The Use of Search Warrants to Seize Work Product and Documentary Materials Belonging to Project Veritas and Its Journalists Violated the Reporter’s Privilege.	25
D. The Government Violated the Fourth Amendment in Applying for and Executing the Search Warrants for Project Veritas’ Newsgathering Materials.	29
1. The Warrants Were Not Supported by Probable Cause.....	29
2. The Warrants Were Rendered Unreasonable by the Government’s Failure to Disclose Material Information to the Magistrate Judges.....	31
3. The Warrants Were a Disproportionate Response to the Gravity of the Alleged Offense Under Investigation.....	35
4. The Warrants Allowed Prohibited General Searches	35
5. The Investigative Team Violated Procedures Established by the Magistrate Judge to Protect Privileged	40

TABLE OF CONTENTS
(continued)

	Page
6. The Government Compounded Its Fourth Amendment Violations by Sealing the Microsoft Warrants.....	41
E. The Court Must Conduct an Inquiry into the Information Submitted to, and Withheld From, the Magistrate Judges Who Issued the Warrants and Orders.	43
CONCLUSION.....	46

INTRODUCTION

The government opposes Project Veritas’ journalism. Predicating its investigation of Project Veritas and its journalists on the alleged “theft” of an abandoned diary belonging to Ashley Biden, then-presidential candidate Joe Biden’s 40-year-old daughter, the government has launched an attack on the free press. The Department of Justice (“DOJ”) and Federal Bureau of Investigation (“FBI”) invaded the homes of Project Veritas journalists using search warrants to investigate what would be (had it actually occurred) a low-level theft under Florida law by Project Veritas’ sources. But the government is using these Mafia-busting tactics to investigate what is, under the Supreme Court precedent applicable to newsgathering, a non-crime.

The sources who lawfully provided the abandoned diary to Project Veritas always represented that it was found abandoned in a house that Ashley Biden occupied temporarily. The First Amendment protects journalists who receive materials from sources even *if* those materials were stolen. Under the guise of investigating this non-crime, the government violated federal law in an unprecedented use of search warrants to seize newsgathering work product, other documentary materials, and extensive personal data from journalists James O’Keefe, Spencer Meads and Eric Cochran (“the PV Warrants”). This is no mere technicality—of the forty-seven electronic devices seized in pre-dawn raids on the homes of Project Veritas journalists, only six have been found to contain data responsive to the PV Warrants, and that data represents a fraction of the other privileged and personal information stored in those devices.

Project Veritas recently discovered another element of the government’s attack on the free press—for more than a year before prosecutors procured the PV Warrants, the government was secretly surveilling Project Veritas. Starting just a few weeks after being contacted by Ashley Biden’s attorney in the fall of 2020, prosecutors in the U.S. Attorney’s Office for the Southern District of New York procured a series of six secret orders and warrants to seize from Microsoft

any and all email communications sent or received by eight Project Veritas journalists, including founder James O’Keefe (collectively “the Microsoft Warrants”). The government also used these warrants to seize “contacts” and “address book” information that Microsoft stores for these journalists, including confidential source and donor information.¹

While the Microsoft Warrants covered various time periods, the government seized emails of some journalists going back to January 1, 2020—*eight months before* sources offered Project Veritas the abandoned diary. Using boilerplate applications and rote recitals, the prosecutors convinced various Magistrate Judges to seal the Microsoft Warrants for more than a year. It was only when Microsoft insisted that these matters be unsealed—after the FBI executed and publicized the PV Warrants—that the prosecutors had no alternative but to acquiesce in unsealing. The Microsoft Warrants were unsealed on March 10, 2021. We now know that the government seized nearly **two hundred thousand** Project Veritas emails and numerous other files.

This all-out assault on a news media organization should alarm all who believe in the First Amendment and the value of a free press. Project Veritas received the abandoned diary and other belongings lawfully, and its newsgathering work—the diary contained information that, if true, would be newsworthy and of public concern by any reasonable measure given that the subject of that information was then campaigning for the country’s highest office—was legitimate, ethical, and careful. Most fundamentally, this newsgathering is protected by the First Amendment as interpreted by *Bartnicki v. Vopper*, 532 U.S. 514 (2001). At this juncture, the Rules of Criminal Procedure empower the Court to protect the First Amendment and curb the government’s abuses.

Accordingly, Project Veritas and the aggrieved journalists move pursuant to Fed. R. Crim. P. 41(g) for the return of their property. Having unlawfully seized newsgathering material from

¹ Unlike legacy corporate media, Project Veritas engages in journalism pursuant to a non-profit model.

James O’Keefe, Project Veritas, and two former Project Veritas journalists, the government must return all electronic devices seized during the searches of the journalists’ homes. The government must also return and destroy its copies of all data it obtained both from those devices and from Microsoft. Four independently sufficient grounds support this relief:

- (1) the seizures violated the express provisions of the Privacy Protection Act (“PPA”);
- (2) the seizures violated the First Amendment;
- (3) the seizures violated the common law Reporter’s Privilege; and
- (4) the seizures violated the Fourth Amendment’s prohibition against unreasonable searches and seizures

I. FACTUAL BACKGROUND

The following facts are derived from materials in the government’s possession, including materials covertly seized from Microsoft, seized from the sources who lawfully provided the diary and personal effects to Project Veritas (before the government procured the PV Warrants), and claims made by Ashley Biden, her associates, and her attorney. The foregoing is summarized below. If the government does contest any of these facts, Project Veritas and its journalists request the opportunity to produce evidence *in camera* to prevent further intrusion upon the privileges that protect their newsgathering work.

A. Project Veritas’ Lawful Receipt of the Abandoned Ashley Biden Diary

Project Veritas “is a national media organization dedicated to ‘undercover investigative journalism.’” *Project Veritas Action Fund v. Rollins*, 982 F.3d 813, 817 (1st Cir. 2020). James O’Keefe is the journalist who founded Project Veritas and serves as its President. In 2020, Spencer Meads and Eric Cochran worked for Project Veritas as investigative journalists.

In early September 2020, confidential sources contacted Project Veritas to report that they had found a diary authored by Ashley Biden, the daughter of then-presidential candidate Joe Biden.

According to these sources, Biden left the diary and other belongings behind when she moved out of a house in Delray Beach Florida that one of the sources subsequently occupied. The sources described, and then sent images of, disturbing information about the author's father that would shock any parent and most voters. The sources reported that they found additional belongings with the diary—including mail, photographs, and other property naming Ashley Biden—that would enable Project Veritas to confirm that she was its author. The sources offered to bring the diary and belongings to Project Veritas in New York. Approximately a week after the initial contact, two of the sources traveled to New York and gave the diary and other Ashley Biden belongings to Project Veritas. Later in September, the sources gave additional Ashley Biden belongings to a Project Veritas journalist in Florida.

Over the course of the next month, Project Veritas journalists worked to authenticate the diary and its contents. Project Veritas engaged a handwriting expert who expressed the opinion that the diary was authored by the same person who signed "Ashley Biden," or otherwise wrote on, other documents provided by the sources. The Project Veritas journalists began producing a video news story regarding Ashley Biden's allegations about her father.

Project Veritas undercover journalists attempted to contact Ashley Biden by reaching out to her known acquaintances. In early October 2020, one of those acquaintances called a Project Veritas undercover journalist and conferenced into the call a person identifying herself as Ashley Biden. Biden responded that the belongings were hers and asked that they be delivered to a friend who lived in Delray Beach.

A few days later a high-level official of the Biden presidential campaign called the journalist and left a voicemail message. The official, who identified himself by name but not his position with the campaign, expressly stated that he was calling about a diary.

Project Veritas viewed these statements by Ashley Biden and the Joe Biden campaign official, in combination with the above-mentioned expert handwriting opinion and other corroborating information, as confirmation that the diary provided by the confidential sources was, in fact, authored by Ashley Biden. The Project Veritas journalists worked to finalize the video news story about the diary, but also continued to analyze the contents of the diary.

On or about October 12, Mr. O’Keefe decided against publishing the news story. In an email to staff, Mr. O’Keefe explained that while he was confident the diary was authentic, Project Veritas had been unable to corroborate its allegations regarding Joe Biden’s conduct towards his daughter when she was a child. *See* (Docket No. 38) at 13.

Subsequent events, however, caused Project Veritas to turn back to the potential news story. On October 14, 2020, the news website Revolver ran a detailed story on Hunter Biden’s laptop and materials contained therein, including information that echoed certain allegations made in Ashley Biden’s diary. *See Revolver Exclusive: Inside Source Alleges Underage Photos Found On Hunter’s Laptop Were of a Member of The Biden Family*, Revolver (Oct. 14, 2020) available at <https://www.revolver.news/2020/10/hunter-laptop-rudy-giuliani-underage-biden-family-member/>. Given these developments and the interest in the diary expressed by the Biden campaign, Project Veritas decided to contact campaign officials directly and ask to interview Joe Biden about allegations in the diary.

Project Veritas made this request in a letter authored by its in-house counsel and delivered to the Biden campaign on October 16, 2020. The campaign did not respond, but Project Veritas was soon contacted by a lawyer representing Ashley Biden. Project Veritas offered to return the property to Biden if she agreed to view it personally and confirm her ownership; Biden’s lawyer

refused to confirm ownership of the abandoned items and vowed to send the matter to the United States Attorney's Office for the Southern District of New York.

While Project Veritas was corresponding with Ashley Biden's lawyer, it continued its investigation to corroborate the content of the diary. Later in October, Project Veritas learned that another news organization had received a copy of what was described as Ashley Biden's diary and that other news organization was concerned its version was not authentic. Mr. O'Keefe concluded that this new information injected uncertainty into the assessment of the diary's content, and he informed his staff (for a second time) that Project Veritas would not publish its news story about the diary.

Shortly after Project Veritas' decision not to publish, a news blog named National File—which is not affiliated with Project Veritas—began publishing excerpts from the diary. *See Patrick Howley, EXCLUSIVE SOURCE: Biden Daughter's Diary Details 'Not Appropriate' Showers with Joe as Child, National File* (Oct. 24, 2020) available at <https://nationalfile.com/exclusive-source-biden-daughters-diary-details-not-appropriate-showers-with-joe-as-child/>.

National File published the full diary on October 26, 2020 and it remains on the internet to this day. *See FULL RELEASE: Ashley Biden Diary Reveals Child Sex Trauma, Drug Abuse, Resentment for Joe – Whistleblower, NATIONAL FILE* (Oct. 26, 2020) available at <https://nationalfile.com/full-release-ashley-biden-diary-reveals-child-sex-trauma-drug-abuse-resentment-for-joe-whistleblower/>. National File attributed its source for the diary as a leak from a whistleblower at another media organization that chose not to publish the diary or report its contents. Project Veritas has no affiliation or other connection with National File and any leak of its unpublished news story, if that occurred, was not caused or authorized by Project Veritas.

In early November 2020, Project Veritas arranged for the delivery of the diary and other abandoned belongings to the Delray Beach, FL police department.

B. The U.S. Attorney's Office/Federal Bureau of Investigation Inquiry and Seizures

1. The PV Warrants

Nearly a year after Project Veritas decided not to publish its news story and delivered the diary and belongings to local law enforcement, Project Veritas learned that the FBI had confronted two of its confidential sources for the news story. In late October 2021, the FBI seized electronic devices from these sources and attempted to interview them. Within a week, undersigned counsel delivered correspondence to the U.S. Attorney's Office documenting his efforts to communicate with the responsible prosecutors and offering to provide information on behalf of Project Veritas. *See* October 27, 2021 Letter from Paul Calli, Esq. to the USAO (Exhibit A). On November 1, 2021, Mr. Calli verbally conveyed detailed information to the prosecutors describing the circumstances of Project Veritas' lawful receipt of the Ashley Biden diary, making clear that Project Veritas was not involved in any theft of property and that all of Project Veritas's information on how the confidential sources found the property came from the sources themselves.

The proffer provided by counsel for Project Veritas would have caused any reasonable prosecutor to reciprocate by pursuing "negotiations with the affected member of the news media," as required by DOJ Regulations, to obtain from Project Veritas additional information about its acquisition of the diary. *See* 28 C.F.R § 50.10(a)(3). At the very least, any reasonable prosecutor would have paused pending plans to seize information from Project Veritas and/or its journalists while the government reviewed the contents of the electronic devices acquired from the confidential sources. But here, the prosecutors did neither.

On November 3, 2021, the prosecutors from the Southern District of New York, accompanied by local FBI agents, submitted applications to Magistrate Judge Cave for warrants to seize electronic devices from former Project Veritas journalists Spencer Meads and Eric Cochran.² The warrants were issued and included an admonishment to the executing agents to “collect evidence in a manner reasonably designed to protect any attorney-client *or other applicable privilege*.” See Warrants (Exhibit B and C, respectively) at 5 and 4. The Magistrate Judge further directed the agents “[w]hen appropriate . . . [to] use a designated ‘filter team,’ separate and apart from the investigative team, in order to address potential privileges.” *Id.*

The warrants were executed at the residence of Mr. Cochran and Mr. Meads, respectively, in the early morning hours of November 4, 2021. Both were initially handcuffed by the agents who spent several hours photographing and searching the premises. The FBI seized twenty-eight (28) devices from Cochran. See December 17, 2021 Letter from AUSA Sobelman to Special Master Barbara Jones (Exhibit D) at 2-3. In addition, the agents took at least sixteen photographs of the contents of one of Mr. Cochran’s devices (a mobile telephone) and made three recordings of audio files on that device, before the security settings caused the device to lock. *Id.* at 2 n.2.³ The government knew that the images and recordings were created when Mr. Cochran was working as a Project Veritas journalist. Notwithstanding Magistrate Cave’s directives that “[r]eview of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client *or other applicable privilege* (to the extent not waived)” and “[w]hen appropriate, the procedures shall

² By this time, Acting U.S. Attorney Audrey Strauss, whose office had obtained the covert Microsoft Warrants, had departed. The Office was led by the then-recently appointed United States Attorney, Damion Williams.

³ The FBI agents likely took many more photographs, and possibly other recordings, but we know about only 16 of them that the Special Master deemed responsive.

include use of a designated ‘filter team,’ separate and apart from the investigative team, in order to address potential *privileges*,” (Exhibit B) at 5, these photographs and recordings were immediately available to the investigative team. The investigative team continued to view them until counsel for Mr. Cochran moved for the appointment of a Special Master on November 12. (Exhibit D) at 2 n.2.

The FBI seized seventeen (17) devices from Mr. Meads. *Id.* at 3-4. The agents even seized a laptop belonging to one of Mr. Meads’ roommates. *Id.*

The following day, November 5, one or more of the local prosecutors, accompanied by local FBI agents, again applied to Magistrate Judge Cave for a warrant, this time to seize electronic devices from Project Veritas’ founder and President James O’Keefe. It is not known what information the agents acquired (or remained in deliberate ignorance of) when executing the warrants for Mr. Meads and Mr. Cochran the preceding day that could justify the issuance of a warrant for the property of a third Project Veritas journalist.⁴ The warrant for Mr. O’Keefe’s home was issued by Magistrate Judge Cave and she included the same admonishments and directive that appeared in the Meads and Cochran warrants regarding procedures to protect privileges. (Exhibit E) at 4.

The FBI executed the warrant at Mr. O’Keefe’s home in the early morning hours of November 6. Mr. O’Keefe was handcuffed and required to stand in the public hallway of the apartment building dressed in his underwear. The FBI seized two cell phones from Mr. O’Keefe’s apartment. *See* (Exhibit D) at 1. In addition, the agents took at least fifteen photographs of the contents of one of the devices (a mobile telephone) before the security settings caused the device

⁴ Significantly, *no* evidence of any wrongdoing by Project Veritas has been found in the images, recordings and other items photographed or extracted by the FBI from the 45 devices seized from Mr. Meads and Mr. Cochran.

to lock. *Id.* at 1 n.1. Knowing that the contents of the device were created by Mr. O’Keefe in his capacity as the senior Project Veritas journalist, and notwithstanding Magistrate Cave’s directives that that “[r]eview of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client *or other applicable privilege* (to the extent not waived)” and “[w]hen appropriate, the procedures shall include use of a designated ‘filter team,’ separate and apart from the investigative team, in order to address potential *privileges*,” (Exhibit E) at 4, these photographs were immediately available to the investigative team. The investigative team continued to view them until counsel for Mr. O’Keefe moved for the appointment of a Special Master on November 10. (Exhibit D) at 1 n.1.

2. *Protocol to Protect Privileged Materials Seized from Project Veritas*

Upon application of Project Veritas and its journalists, and over the objection of the government, this Court issued an order appointing the Honorable Barbara Jones as Special Master in this matter to (1) review the contents of the devices seized from the Project Veritas journalists to determine what material is responsive to the warrants; (2) provide any such responsive material to the DOJ filter team; and (3) rule on objections the Project Veritas journalists raise in regard to the DOJ filter team’s proposed release of materials to the investigative team. *See* December 8, 2021 Order (Docket No. 12).

The FBI Computer Analysis Response Team (CART) analyzed the electronic devices seized from the Project Veritas journalists by the investigative team. The most recent report on the CART unit’s work organized those devices into three categories. *First*, the CART decided that 15 of the devices contained data within the temporal limits of the PV Warrants (August 1, 2020 – execution date) and submitted that data to the Special Master. *See* February 6, 2022 Letter

from AUSA Sobelman to Special Master Barbara Jones (Exhibit F). *Second*, the CART determined that 15 of the seized devices contained *no* data within the temporal limits of the PV Warrants. *Id.* *Third*, 17 of the seized devices are non-functional or otherwise cannot be accessed. *Id.*

The Special Master reviewed the data submitted by the CART unit and determined that another 10 devices seized by the FBI contained “no responsive materials.” *See* March 7, 2022 Special Master Report (Docket No. 61) at 1-2. The Special Master located material that she found to be responsive to the PV Warrants on *only* 6 of the devices seized by the FBI, specifically one-hundred fifty-five photographs/images, recordings, and other items. *Id.* at 2. Those items were contained on devices belonging to Mr. O’Keefe (15), Mr. Meads (66) and Mr. Cochran (74).

Pursuant to the protocol established by the Court, the Special Master delivered the items she determined to be responsive to the DOJ filter team, including journalists’ notes; photographs of information received from confidential sources; text messages and recorded calls from persons with information; records of journalists’ newsgathering activities; and journalists’ editorial communications regarding whether the Biden diary story should be published. Remarkably, the DOJ filter team contends that *none* of these items are deserving of protection under the First Amendment or the Reporter’s Privilege. Project Veritas, Mr. O’Keefe, Mr. Meads and Mr. Cochran have submitted to the Special Master objections to the DOJ filter team’s determinations, demonstrating these items comprise work product and other documentary material created in the course of newsgathering and are protected from disclosure by the First Amendment and/or the Reporter’s Privilege. The aggrieved journalists have also demonstrated that several items deemed

responsive to the PV Warrants by the Special Master, in fact, are not responsive. The Special Master has taken these objections under advisement.⁵

3. *The Microsoft Warrants*

On March 11, 2022, Project Veritas was notified by its electronic communications service provider, Microsoft, that for over a year the government has been secretly seizing and reviewing Project Veritas email and other enterprise information. Microsoft was finally able to notify Project Veritas of this surveillance because, as explained below, its attorneys resisted the government's renewal of non-disclosure orders and notified the prosecutors that Microsoft intended to institute litigation seeking leave to disclose these matters.

Undersigned counsel has now received copies of the following orders and warrants by which the government secretly seized voluminous Project Veritas data:

- 20 Mag. 12614: Served November 24, 2020, this subpoena seeks subscriber information for the account [Human Resource Manager at] projectveritas.com, without time limitation. The accompanying secrecy order prohibited Microsoft from disclosing the existence of the subpoena for one year; the order was extended 180 days. (Signed by Magistrate Judge Wang)
- 20 Mag. 12623: Served November 24, 2020, this order issued under 18 U.S.C. § 2703(d) requires Microsoft to produce information associated with the same account, again without time limitation. The order included a one-year secrecy provision that was later extended an additional year. (Signed by Magistrate Judge Gorenstein)
- 21 Mag. 548: Served January 15, 2021, this search warrant demanded email content and other information associated with the same account specified in 20 Mag. 12614 and 20 Mag. 12623 (but with the domain name misspelled as “[Human Resources manager at] projectvertias.com”), [Eric Cochran at] projectveritas.com, and [Spencer Meads at] projectveritas.com, for the period January 1, 2020 to present. The warrant contained a one-year secrecy provision, later extended an additional year. (Magistrate Judge signature somewhat indistinct but appears to be Magistrate Judge Wang)

⁵ Notably, the Special Master has not completed her review of the data extracted from the mobile device seized from Mr. O’Keefe. Nevertheless, the investigative team urged the Special Master to “pause” her review of Mr. O’Keefe’s device while she considers the objections submitted by Project Veritas and its journalists.

- 21 Mag. 992: Served January 26, 2021, this search warrant demanded email content and other information associated with [Additional Investigative Journalist at] projectveritas.com, for the period January 1, 2020 to present. It contained a one-year secrecy provision, later extended an additional year. (Signed by Magistrate Judge Freeman)
- 21 Mag. 2537: Served March 5, 2021, this search warrant demanded email content and other information associated with [Three Additional Investigative Journalists] for the period September 1 – December 1, 2020. It contained a one-year secrecy provision. (Signed by Magistrate Judge Lehrburger)
- 21 Mag. 2711: Served March 10, 2021, this order, issued under 18 U.S.C. § 2703(d), required Microsoft to produce information associated with [An Additional Investigative Journalist at] projectveritas.com, for the period September 1 – December 1, 2020. It included a one-year secrecy provision. (Signed by Magistrate Judge Moses)
- 21 Mag. 3884: Served April 9, 2021, this search warrant demanded email content and other information associated with [James O’Keefe at] projectveritas.com, for the period September 1 – December 1, 2020. It contained a one-year secrecy provision. (Signed by Magistrate Judge Aaron)

Significantly, these search warrants required the production of *any and all* emails, including content, within the prescribed time periods. As noted above, we have recently learned from Microsoft that the government seized nearly *two hundred thousand* Project Veritas emails and numerous other files. The warrants also required disclosure of all address and contact information.⁶

At the time Microsoft was served with the January 2022 extensions of the non-disclosure order, its attorneys had become aware of the execution of the PV Warrants and this Court’s December 8, 2021 Order appointing Special Master Jones to protect “any First Amendment concerns, journalistic privileges, and attorney-client privileges.” (Docket No. 48) at 4. The government’s actions to continue sealing the Microsoft Warrants raised significant concerns, however, given that the data seized from Microsoft very well could include documents protected

⁶ At the time the prosecutors obtained these warrants, the U.S. Attorney’s Office was led by Acting U.S. Attorney Audrey Strauss.

by those same privileges. Stated another way, at the very time that this Court has put in place a procedure to prevent disclosure of privileged material to the government investigative team, it appeared that the investigative team *already possessed* privileged materials and may not have informed this Court of that when opposing the appointment of a special master.

Microsoft, through its attorneys, advised that it would move to vacate the extensions of the non-disclosure orders and notify the Court of its concerns. The government relented and moved to lift any pending non-disclosure orders for the Microsoft Warrant, which motion was granted March 10, 2022. *See* 22 Mag. 2364 (Magistrate Judge Netburn).

Project Veritas has moved to compel the government to provide further information about its secret seizures of Project Veritas materials from providers, including Microsoft. (Docket No. 64). The full extent of the government's invasion of the newsgathering activities of Project Veritas journalists remains unknown.

II. SUMMARY OF ARGUMENT

The seizure of newsgathering materials from Project Veritas and its journalists was unlawful, and those materials must be returned pursuant to Fed. R. Crim. P. 41(g) for four, independently sufficient reasons: (1) the seizures violated the express provisions of the Privacy Protection Act; (2) the seizures violated the First Amendment; (3) the seizures violated the common law Reporter's Privilege; and (4) the seizures violated the Fourth Amendment.

III. LEGAL STANDARDS

Federal Rule of Criminal Procedure 41(g) provides that "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return...in the district where the property was seized." Upon the filing of a Rule 41(g) motion "[t]he court must receive evidence on any factual issue necessary to decide the motion."

Id. “[W]here no criminal proceedings against the movant are pending or have transpired, a motion for the return of property is treated as [a] civil equitable proceeding.” *Mora v. United States*, 955 F.2d 156, 158 (2d Cir. 1992). “Equitable considerations might justify an order requiring the government to return or destroy all copies of records that it has seized.” Fed. R. Crim. P. 41 (advisory committee notes (1989 amendments)).

The Privacy Protection Act, 42 U.S.C. § 2000aa *et seq.* (“the PPA”) makes it unlawful, notwithstanding any other law, for a government employee “in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product [or other documentary] materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.” 42 U.S.C. § 2000aa.a. The only exception to this prohibition is where there is “probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate [but not where] the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein.” *Id.* at § 2000aa.a.1.

The DOJ itself has construed this “suspect” exception to the PPA to be applicable only where “the member of the news media is a subject or target of a criminal investigation for conduct *not* based on, or within the scope of, newsgathering activities.” § 50.10(d)(4) (emphasis added).

The First Amendment forbids government action that “abridge[es] the freedom of speech, or of the press; or the right of the people peaceably to assemble.” U.S. Const. amend. I.

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV.

IV. ARGUMENT

A. The Use of Search Warrants to Seize Work Product and Documentary Materials Belonging to Project Veritas and Its Journalists Violated the Privacy Protection Act

Project Veritas, Mr. O’Keefe, Mr. Meads and Mr. Cochran are all protected by the PPA inasmuch as the singular purpose of Project Veritas’ business is to “disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.” 42 U.S.C. § 2000aa.a. The materials seized from Mr. O’Keefe, Mr. Meads and Mr. Cochran comprise work product materials and/or documentary materials protected by the PPA. And there can be no legitimate dispute that these materials were created or acquired in the course of newsgathering activities.

In opposing the appointment of a special master, the government relegated to a footnote its conclusory assertion that it is relying on the “suspect” exception to the PPA to justify the seizures. Gov’t Opp. to Appointment of Special Master (Docket No. 29) at 14 n.10. In the government’s view, this exception is triggered because

There is probable cause to believe that Project Veritas, O’Keefe, Cochran, and Meads were **actively involved** in the unlawful conduct under investigation – the interstate transportation of stolen property, as well as the theft of certain of the property itself.

Id. at 7 (emphasis added). The government has never suggested in any of its various pleadings opposing the appointment of a Special Master and other relief sought by Project Veritas that any of its journalists actually **stole** the Biden diary or other belongings initially received from confidential sources. Any such suggestion would be frivolous: the sources offered these items to Project Veritas and delivered the property to New York. Instead, the government’s coy description of its supposed probable cause, and the secondary theories of liability cited in the warrants, suggest

that the government’s investigation theory was (or, at least, is now) that after receiving the Biden diary and other belongings from the sources Project Veritas requested and obtained additional Biden property.⁷ Such a “solicitation,” in the view of the prosecutors, is a crime.

But there is no “active involvement” exception to the PPA, and the government cited no decision applying such a theory to uphold seizures from a member of the news media. The “suspect” exception is triggered only where there is probable cause to believe that a journalist is *actually committing* (or has committed) a criminal offense. *See* 42 U.S.C. § 2000aa.a.1. What is more, the PPA expressly excludes from this exception a journalist’s “receipt, possession, communication, or withholding of [stolen] materials or the information.” *Id.* Therefore, in the absence of probable cause to believe that a Project Veritas journalist committed a breaking and entering to steal the Biden diary—and the government has not claimed (nor could it) that it has any evidence of such conduct—there is no basis in the text of the PPA for issuance of the PV Warrants. Put differently, there is no accurate and complete set of facts the government could have provided to the Magistrate Judge that would make the seizures lawful under the PPA.

Congress directed the DOJ to promulgate regulations to provide for the protection of privacy interests, including the First Amendment principles underlying the PPA, when prosecutors seek to obtain documentary materials in criminal investigations. *See* 42 U.S.C. § 2000aa-11. Those regulations governing DOJ use of subpoenas and search warrants to obtain documents and other information from members of the news media are codified at 28 C.F.R. § 50.10 (“the DOJ Regulations”). The government has previously assured the Court that when obtaining the PV

⁷ See PV Warrants (Exhibits B, C, and E) citing § 371 (conspiracy to possess and transport stolen goods); § 2 (aiding and abetting); § 3 (accessory after the fact); and § 4 (misprision of felony). The PV Warrants also cite § 2314 (interstate transportation of stolen property) and § 2315 (possession of stolen property), but as explained below those offenses are so plainly foreclosed by the PPA and *Bartnicki* that citation to them raises serious questions about the government’s motives.

Warrants its prosecutors “complied with all applicable regulations and policies regarding potential members of the news media in the course of this investigation, including with respect to the search warrants at issue.” Gov’t Opp. to Appointment of Special Master (Docket No. 29) at 2 n.2. This assurance, however, was untrue. As explained below, the DOJ regulations *prohibit* reliance on the PPA suspect exception to seize newsgathering materials.

Importantly, the DOJ regulations recognize that even *subpoenas* to obtain information from members of the news media are “extraordinary measures, not standard investigatory practices.” 28 C.F.R § 50.10(a)(3). As such, subpoenas may be used only with

authorization by the Attorney General, or by another senior official . . . when the information sought is essential to a successful investigation, prosecution, or litigation; after all reasonable alternative attempts have been made to obtain the information from alternative sources; and after negotiations with the affected member of the news media.

Id. These requirements for pursuit of alternative sources of information and negotiations with the affected media member, however, are relaxed where the Attorney General determines that the “suspect” exception to the PPA is applicable. *See* § 50.10(c)(4)(i). In that circumstance the Attorney General could approve issuance of a subpoena to a member of the news media even where the “investigation relat[es] to an offense committed in the course of, or arising out of, newsgathering activities.” *Id.*⁸

⁸ Just a few months before the agents/prosecutors applied for the PV Warrants, the Attorney General announced that the DOJ “will no longer use compulsory legal process for the purpose of obtaining information from or records of members of the news media acting within the scope of newsgathering activities.” *See* July 19, 2021 Attorney General Memorandum, *avail. at* <https://www.justice.gov/ag/page/file/1413001/download> at 1. This new policy was prompted by a recognition that DOJ’s internal procedural protections heretofore may have insufficiently weighed “the important national interest in protecting journalists from compelled disclosure of information revealing their sources, sources they need to apprise the American people of the workings of their government.” *Id.*

The DOJ Regulations, however, establish markedly more stringent limitations on the use of *search warrants* to seize information from a member of the news media. The Attorney General or his designee is authorized to approve application for a news media search warrant pursuant to the “suspect exception” of the PPA only “when the member of the news media is a subject or target of a criminal investigation for conduct *not* based on, or within the scope of, newsgathering activities.” § 50.10(d)(4) (emphasis added). Therefore, this DOJ regulation *prohibits* the use of warrants to seize newsgathering materials, and neither the Attorney General nor his designee could have approved the applications for the PV Warrants.⁹

In cases where prosecutors have broken DOJ’s own rules, the government is quick to argue that a DOJ regulation “does not create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States.” *See, e.g.*, Gov’t Opp. to Appointment of Special Master (Docket No. 29) at 2 n.1. But these regulations were enacted at the direction of Congress to ensure that its prohibition on the use of search warrants to seize newsgathering materials was understood and respected by prosecutors. The DOJ’s own interpretation of the PPA “suspect” exception—that it is available as a basis for using search warrants only to obtain *non-*newsgathering information—would certainly have informed the Magistrate Judge’s decision whether or not to issue the PV Warrants. Likewise, § 50.10(d)(4) should lead this Court to construe the PPA “suspect” exception no more expansively than the DOJ does and to conclude that the PV Warrants were unlawful.

⁹ It would seem implausible that the Attorney General or any other official at “Main Justice,” being fully apprised of the circumstances nevertheless approved the search warrant applications in disregard of the PPA, the DOJ regulations, and the Attorney General’s recent pronouncement severely limiting the use of search warrant permitted under the regulations. In the highly unlikely event that this occurred, however, this occurrence would have been material to the Magistrate Judge’s assessment of probable cause inasmuch as it would have revealed a political motive to use the warrants to punish newsgathering perceived as unfavorable to the President and his family.

B. The Use of Search Warrants to Seize Work Product and Documentary Materials Belonging to Project Veritas and Its Journalists Violated the First Amendment.

The Microsoft Warrants enabled the government to rummage through the Project Veritas virtual newsroom, at the government's leisure, for more than a year and continuing to the present time. *See, e.g.,* Mel Bunce et al., “*Our Newsroom in the Cloud: Slack, Virtual Newsrooms, and Journalistic Practice*,” 20 *News Media & Soc’y* 3381 (Dec. 31, 2017), available at <https://bit.ly/34lHrhV>. Through this secret and persistent surveillance, the government seized the identities of confidential sources, documents and information received from those sources, story leads and outlines, draft and final news videos, donor information, and much more. These seizures were not limited to sensitive information pertaining to the Biden diary news story; the government seized “all” such data for an entire year stored in the email accounts of certain Project Veritas journalists. These covert seizures were in blatant violation of the First Amendment. Likewise, the seizures from journalists’ homes enabled by the PV Warrants were, by design, conducted under the glare of the public spotlight, but were no less in disregard of First Amendment rights.

Bartnicki v. Vopper, 532 U.S. 514 (2001) forecloses the theory apparently underpinning the government’s investigation of Project Veritas—that its journalists encouraged sources to obtain and provide property that the government contends was “stolen.” In *Bartnicki*, the Court held that the government may not constitutionally punish a journalist’s receipt of information from a source who obtained it unlawfully where the recipient’s purpose is to disseminate that information to the public. The plaintiff in *Bartnicki* invoked Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which prescribes criminal penalties and civil damages for the intentional disclosure of the contents of an electronic communication when the defendant “know[s] or ha[s] reason to know that the information was obtained” through an illegal interception. 18 U. S. C. § 2511(1)(c). Vopper, a radio commentator, played on his public affairs talk show a recording of a surreptitiously

intercepted cell phone conversation to which Bartnicki was a party. *Bartnicki*, 532 U.S. at 519. Bartnicki filed an action for damages against Vopper and other media representatives who published the recording, and the defendants raised various defenses including that disclosure was protected by the First Amendment. *Id.* at 520. The government intervened on appeal in support of the enforcement of the statute’s sanctions.

The ruling in *Bartnicki* is clear and controlling here. The Court held that a member of the media is not liable for receiving or publishing newsworthy information that was obtained unlawfully by a source. *Id.* at 533-34 (“[t]he enforcement of [a federal criminal statute] implicates the core purposes of the First Amendment it imposes sanctions on the publication of truthful information of public concern”). Remarkably, the prosecutors here applied for the PV Warrants on the basis of alleged offenses—conspiracy to possess stolen goods (§ 371), and possession of stolen goods (§ 2315)—that *Bartnicki* *expressly* held were not offenses. *See* (Exhibits B, C, and E) at 1.¹⁰ The government’s reliance on the federal statute prohibiting interstate transportation of stolen property (§ 2314) is likewise foreclosed by *Bartnicki*. The plaintiff there argued that the “delivery” of the unlawful recording was conduct that could be sanctioned without impinging upon protected speech, but the Court was unpersuaded:

It is true that the delivery of a tape recording might be regarded as conduct but given that the purpose of such a delivery is to provide the recipient with the text of recorded statements, it is like the delivery of a handbill or pamphlet, and as such, it is the kind of ‘speech’ that the First Amendment protects.

Bartnicki, 532 U.S. at 527.¹¹

¹⁰ This is another indication that these prosecutors did not obtain the approval of the Attorney General to seek the PV Warrants. We are confident that the Attorney General and his staff are familiar with *Bartnicki*.

¹¹ The Solicitor General supported these unsuccessful arguments, emphasizing the deterrent effect of the statute. *Id.* at 529-30 and n.13.

Bartnicki limits liability to circumstances where the journalist actually “participate[d] in the theft.” *Democratic Nat’l Committee v. Russian Fed’n*, 392 F. Supp. 3d 410, 434-36 (S.D.N.Y. 2019). For this reason, the government’s “active involvement” theory fares no better under First Amendment scrutiny than it does under the PPA statutory analysis. *See supra* at 16-17. That phrase appears nowhere in *Bartnicki*, and the government has not cited (nor have we located) a decision limiting its holding to deny First Amendment protection to a member of the news media on that ground. To the contrary, decisions of this Court and others have construed *Bartnicki* to preclude nearly identical theories of liability regarding journalists who received stolen information. This Court in *Democratic Nat’l Committee* rejected the claim that Wikileaks and others who disseminated information hacked from DNC computers were liable under conspiracy, accessory-after-the-fact, or aiding and abetting theories for “soliciting” stolen information and “encouraging” the hacker to disseminate it. Judge Koeltl declined the plaintiffs’ invitation to infer a conspiracy from the fact that some defendants met with associates of the hacker, observing that it is a “common journalistic practice. . . to ‘meet[] with information thieves’ or ‘solicit[] stolen information.’” *Id.* at 435. And Judge Koeltl interpreted *Bartnicki*’s threshold for liability—whether a party played a part in an illegal interception—to mean actually “participate in the theft.” *Id.*; *see also id.* at 436 (defendants “could have published the documents themselves without liability because they did not participate in the theft and the documents are of public concern”). Judge Koeltl adopted the First Circuit’s analysis of *Bartnicki* in *Jean v. Mass. State Police*, 492 F.3d 24 (1st Cir. 2007). Local police threatened to prosecute Jean, a political activist who maintained a website displaying information critical of law enforcement, for publishing an illegally recorded video of an arrest and search. *Id.* at 25-26. Jean sought an injunction citing her First Amendment rights. The district court entered an injunction, and on appeal the government argued

that *Bartnicki* was distinguishable on the ground that Jean “assisted, conspired, [] served as an accessory to”, “aid[ed] and abet[ed],” and was in “active collaboration” with the individual who made the illegal recording. *Id.* at 31, 33. The First Circuit rejected the government’s efforts to distinguish *Bartnicki*, reasoning that “the fact that [the defendant in *Bartnicki*] received the tape ‘passively’ and Jean received the tape ‘actively’ is a distinction without a difference.” *Id.* at 32.

This Court need not look far to determine how equitable considerations relevant to deciding a Rule 41(g) motion should apply. There is a great body of First Amendment jurisprudence that regularly favors the issuance of equitable relief in favor of those who seek to exercise their rights to free speech and association. It is a matter of black letter law that the “loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.” *Elrod v. Burns*, 427 U.S. 347, 373 (1976). And the chilling effect on protected First Amendment activities constitutes irreparable injury and generally supports the issuance of injunctive relief. *Ostrokowski v. Local 1-2, Utility Workers of America, AFL-CIO*, 530 F. Supp. 208, 215 (S.D.N.Y. 1980) (citing *Chicago Area Military Project v. City of Chicago*, 508 F.2d 921, 926 (7th Cir. 1975)).

The mere threat of prosecution for speech that the government deems “objectionable” violates the First Amendment. *See, e.g., Bantam Books v. Sullivan*, 372 U.S. 58, 71-72 (1963). Relief is regularly afforded where one demonstrates “an objectively justified fear of real consequences” *before* they actually occur. *Initiative & Referendum Institute v. Walker*, 450 F.3d 1082, 1088 (10th Cir.2006) (internal quotations omitted). Here, the First Amendment injury has already occurred—the seizure of Project Veritas’s records because the government deems its newsgathering about the Biden family objectionable.

The First Amendment also protects the right to political privacy and association with like-minded supporters, sources and other journalists. Those rights been violated here by the compelled

disclosure of text messages among Project Veritas board members and advisors about whether or not to publish, discussions with other news organizations about stories, internal communications among Project Veritas journalists, photographs of source material, communications with external sources, and internal journalist drafts and notes.

The seizure of newsgathering materials and consequent threat to prosecute journalists is precisely the sort of punitive action that discourages the exercise of constitutionally protected rights. *Mills v. Alabama*, 384 U.S. 214, 218-19 (1966). Few journalists would risk investigating the most powerfully connected individuals in the United States government if their First Amendment freedoms could be brushed aside so easily. This chilling effect is compounded by the fact that the government's investigation here was triggered by, and is seeking to punish, the **content of speech**. There can be no serious dispute that the DOJ and FBI have brought their collective forces to bear upon Project Veritas and its journalists because of their newsgathering work about the Ashley Biden diary. The notion that there is a compelling federal law enforcement interest in **how** the diary was acquired and whether its acquisition violated Florida's petty theft statute is nonsense. It is the fact that Project Veritas acquired the diary and prepared to report about its contents to the potential detriment of then-candidate Joe Biden that has animated the interest of the government. Enforcement action motivated by a "disagreement with the message" violates the First Amendment. *Police Dep't of Chicago v. Mosle*, 408 U.S. 92, 95 (1972) ("But, above all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content"); *see also Doe v. Ashcroft*, 334 F. Supp. 2d 471, 507-08 (S.D.N.Y. 2004), *vacated on other grounds sub nom. Doe v. Gonzales*, 449 F.3d 415, 418 (2d Cir. 2006) (FBI national security letters restricting disclosure of law enforcement activity are content-based and subject to strict scrutiny).

In sum, the newsgathering materials seized from Project Veritas are unquestionably entitled to protection under the First Amendment. It is clear from *Bartnicki* and cases interpreting it that a journalist cannot be held liable for the receipt, transportation, or possession of stolen property, or even for “actively” encouraging a thief. It follows that the government procured the Microsoft Warrants and the PV Warrants on the basis of applications presenting probable cause to believe that a *non-crime* had occurred. The consequent seizures, therefore, were unlawful, and all of the devices and information extracted from them must be returned to Project Veritas and its journalists.

C. The Use of Search Warrants to Seize Work Product and Documentary Materials Belonging to Project Veritas and Its Journalists Violated the Reporter’s Privilege.

That the PPA and First Amendment protect newsgathering information from government seizure is not the end of the story. In the years after *Branzburg v. Hayes*, 408 U.S. 665 (1972) declined to reach the question of whether a qualified common law privilege also protects newsgathering, at least ten Circuit Courts of Appeal have answered that question in the affirmative. *See* Introduction to the Reporter’s Privilege Compendium, *available at* <https://www.rcfp.org/introduction-to-the-reporters-privilege-compendium> (last updated Nov. 5, 2021) (gathering cases). Many of these decisions rely on Federal Rule of Evidence 501, which authorizes federal courts to develop privileges “in the light of reason and experience.” *Id.*; *see also* *Trammel v. United States*, 445 U.S. 40, 47 (1980) (“[Rule 501] acknowledges the authority of the federal courts to continue the evolutionary development of testimonial privileges.”).

In this Circuit, “the reporter’s qualified privilege extends to both civil and criminal cases.” *United States v. Burke*, 700 F.2d 70, 77 (2d Cir. 1983). *Burke* recognized that:

What is required is a case-by-case evaluation and balancing of the legitimate competing interests of the newsman’s claim to First Amendment protection from

forced disclosure of his confidential sources, as against the defendant's claim to a fair trial which is guaranteed by the Sixth Amendment.

Id. There is no principled reason for a different test when it is the government seeking to force disclosure of the newsman's materials. Indeed, Sixth Amendment fair trial rights are fundamental. *See, e.g., Barber v. Page*, 390 U.S. 719, 721 (1968) (noting "essential and fundamental requirement for [a] fair trial which is this country's constitutional goal"). There is no comparable constitutional guarantee for the government's right to seize or otherwise gather evidence independent of a grand jury investigation.¹²

"[T]o protect the important interests of reporters and the public in preserving the confidentiality of journalists' sources, disclosure may be ordered only upon a clear and specific showing that the information is: highly material and relevant, necessary or critical to the maintenance of the claim, and not obtainable from other available sources." *Burke*, 700 F.2d at 76-77. The government **could not** have satisfied that standard in the applications for the Microsoft Warrants or the PV Warrants. First, as the Court can see from *in camera* examination of the photographs, images, and recordings seized by the FBI, these materials show only that Project Veritas gathered information to prepare a news story about the Biden diary. None of the materials from the seized items designated as relevant by the Special Master indicate that Project Veritas journalists participated in its theft. The seized items, therefore, could not be considered "highly material [or] critical to the maintenance of the claim" by any reasonable measure. *Burke*, 700 F.2d at 77.

Second, the government could not have presented truthful and complete information to the Magistrate Judges sufficient to show that the information was not obtainable from other available

¹² As explained below, the U.S. Attorney's Office and FBI procured the Microsoft Warrants and PV Warrants independent of any grand jury investigation.

sources. As explained above, at the time the government applied for the PV Warrants, it had already seized a computer and mobile telephone from the confidential sources who, after acquiring the Biden diary, lawfully offered it to Project Veritas. *See supra* at 7. On information and belief, the government did not reveal to the Magistrate Judge that the information sought via the PV Warrants was available from these alternative sources.

In his concurring opinion in *In Re Grand Jury, Judith Miller*, 438 F.3d. 1141, 1178 (D.C. Cir. 2006), Judge Tatel chronicled the development of the Reporter's Privilege and described the essence of the requisite balancing test in a simple question: does "the public interest in punishing the wrongdoers...outweigh[] any burden on newsgathering?" That balancing weighs overwhelmingly in favor of Project Veritas and its journalists. The public's interest in punishing an alleged theft of personal belongings (primarily papers) left behind in a residence, and in which the owner thereafter demonstrated no interest, is minimal. Indeed, Biden never filed a burglary or theft report with the local police. As far as we are aware, the interest taken in this matter by the U.S. Attorney's Office and the FBI arose only after Project Veritas' request to the Biden Campaign for comment on the diary led Ashley Biden's lawyer to solicit the assistance of the prosecutors. *See supra* at 6. That is a partisan political interest, not a compelling law enforcement need.

The import of the matters under investigation here cannot be seriously compared to investigations of the leak of a covert CIA agent's identity, *see In re Grand Jury, Judith Miller*, 438 F.3d. at 1173; the leak of government plans to seize assets of terrorist organizations, *see New York Times Co. v. Gonzales*, 459 F.3d 160, 163 (2d Cir. 2006); or even to the unlawful use and sale of drugs. *See Branzburg v. Hayes*, 408 U.S. 665 (1972).

On the other side of the scale lies the First Amendment's express protection for "freedom . . . of the press" which forecloses any debate about that institution's "important role in the

discussion of public affairs.” *Mills v. Alabama*, 384 U.S. 214, 218-19 (1966). “Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs.” *Brown v. Hartlage*, 456 U.S. 45, 52 (1982). The press, “which includes not only newspapers, books, and magazines, but also humble leaflets and circulars...play[s] an important role in the discussion of public affairs.” *Mills*, 384 U.S. at 219. “Suppression of the right of the press to praise or criticize governmental agents and to clamor and contend for or against change...muzzles one of the very agencies the Framers of our Constitution thoughtfully and deliberately selected to improve our society and keep it free.” *Id.*

The DOJ itself has recognized that these critical free press interests outweigh the government’s investigative needs even for the most serious of crimes, and even where only non-content information is being sought by investigators. In the only instance that we are aware of where the DOJ obtained § 2703(d) orders to compel a service provider to produce non-content email information for journalists, the DOJ: (1) authorized the service provider (Google) to provide pre-disclosure notice to the news organization (The New York Times), allowing for a judicial challenge to the orders; and (2) ultimately withdrew the orders even though the offense under investigation was the leak of classified information. M. Schmidt and A. Goldman, *Project Veritas Says Justice Dept. Secretly Seized Its Emails*, N.Y. TIMES (March 22, 2022), available at <https://www.nytimes.com/2022/03/22/us/politics/project-veritas-emails.html>. This transparent and measured approach in an investigation involving the reporting of leaked classified information, is strikingly different than the clandestine and wide-ranging campaign by the prosecutors here to pursue journalists who received an allegedly stolen personal diary but never published it.

The DOJ Regulations establish federal policy, reinforcing the legislative mandate of the PPA, to protect “news media from forms of compulsory process, whether civil or criminal, which might impair the news gathering function.” 28 C.F.R. § 50.10. As noted, that policy prohibits the very action taken by the prosecutors and agents here—the use of warrants to seize newsgathering materials from a member of the media. In these circumstances, the balancing of interests required by the Reporter’s Privilege tilts entirely in favor of Project Veritas and its journalists.

D. The Government Violated the Fourth Amendment in Applying for and Executing the Search Warrants for Project Veritas’ Newsgathering Materials.

For the reasons identified above, neither the Microsoft Warrants nor the PV Warrants were supported by probable cause. The warrants also were rendered unreasonable when the prosecutors withheld material information from the magistrate judges who issued these warrants, including that the warrants were prohibited by the DOJ’s own regulations. The searches were also unreasonable because the warrants were a disproportionate response to the gravity of the offense under investigation. And the execution of the Microsoft Warrants and the PV Warrants also violated the Fourth Amendment in numerous respects.

1. The Warrants Were Not Supported by Probable Cause

When government officials apply for a search warrant they are required to “provide the magistrate with a substantial basis for determining the existence of probable cause. *Illinois v. Gates*, 462 U.S. 213, 239 (1983). Here, as explained above, the prosecutors and agents are investigating a non-crime based on complaints received from Ashley Biden’s lawyer and, quite possibly, the Joe Biden campaign. Simply put, it is not a crime for a journalist to receive, possess, transport, or solicit property stolen by another party. *See supra* at 20-25. The government’s crutch—that Project Veritas was “actively involved” in obtaining the Ashley Biden diary and

belongings—is a thin reed that collapses under the weight of authority from this and other courts. *Id.*

From the very beginning the prosecutors knew (or certainly should have known) that there was no crime committed by Project Veritas. The complaint lodged by Ashley Biden’s lawyer with then Acting U.S. Attorney Audrey Strauss in or about early November 2020 in no way provided “specific and articulable facts” showing reasonable grounds to believe that Project Veritas had committed a criminal offense, let alone facts amounting to probable cause. The Project Veritas correspondence with Biden’s attorney, which presumably she supplied to the prosecutors, indicated that Project Veritas had acquired the Biden diary and property lawfully. Likewise, Biden and her associates almost certainly recorded the telephone conversations they had with the undercover Project Veritas journalist. The prosecutors listening to those recordings would have learned significant facts casting doubt on the proposition that the Biden diary was stolen, including that Biden was uncertain where and when she had lost track of her diary and that she did not then claim it had been stolen.

It is doubtful that, prior to submitting their first application for a § 2703(d) order just weeks after being contacted by Ashley Biden’s lawyer, the prosecutors and agents spoke to any witness (other than Biden) who had direct contact with, or observed the actions of, the Project Veritas journalists. As mentioned above, the FBI did not contact the Project Veritas confidential sources until late October 2021, nearly a year after the government procured the first § 2703(d) order on November 24, 2020. That initial § 2703(d) application could only have been based on speculation and generalities. And to the extent that the four applications for Microsoft Warrants submitted in January-April 2021 were based on data and emails derived from earlier orders/warrants, the applications were inaccurate or misleading. As noted above, the electronic communications that

the government has seized, either directly from the Project Veritas journalists or the confidential sources, consistently evidence that the sources already had possession of Biden’s diary and other property *before* contacting Project Veritas.

2. *The Warrants Were Rendered Unreasonable by the Government’s Failure to Disclose Material Information to the Magistrate Judges*

A magistrate judge can perform a proper assessment of probable cause only if “the applicant agency fully and accurately provides information in its possession that is material to whether probable cause exists [and] the government [has] a heightened duty of candor . . . in *ex parte* proceedings.” *In re Accuracy Concerns Regarding FBI Matters Submitted to FISC*, 411 F.Supp.3d 333, 335-36 (U.S. Foreign Intel. Surveillance Ct., Dec. 17, 2019) (internal quotations omitted). “[O]mitting . . . highly relevant information [about a search of electronic data] is inconsistent with the government’s duty of candor in presenting a warrant application. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.” *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring). The affiant may not “selectively include[] information bolstering probable cause, while omitting information that d[oes] not.” *United States v. Perkins*, 850 F.3d 1109, 1117 (9th Cir. 2017).

The applications for the Microsoft Warrants and the PV Warrants were deficient in (at least) the following respects. *First*, and most fundamentally, there is substantial reason to believe that the prosecutors misled the Magistrate Judges by claiming that Project Veritas was not a news organization entitled to the protections of the PPA and First Amendment. After all, the government unsuccessfully made those very same arguments to this Court. *See* (Docket No. 29) at 9-10.

Second, the government was not candid with the Magistrate Judges regarding the prohibitions of the PPA. To be sure, courts are “presumed to know the law and apply it in making their decisions.” *Walden v. Arizona*, 497 U.S. 639, 653 (1990). But the fact that the Magistrate Judges may have been generally familiar with the PPA did not relieve the government of its duty to be candid in describing the conduct of Project Veritas journalists. For example, had the government revealed that Project Veritas acquired the Biden diary and belongings in the course of newsgathering, the Magistrate Judges would have realized that the PPA precluded the seizures.

Conversely, if the warrant application stated that Project Veritas and its journalists were “actively involved” in the theft of the Biden diary or other property—just as the government has represented to this Court, *see* (Docket No. 29) at 7—such a conclusory and misleading characterization would have infected the probable cause determination. As explained above, there is no “active involvement” exception to the PPA, and any statement to the contrary would have misled the Magistrate Judges. Had the Magistrate Judges been accurately and fully informed, they would have realized that the PPA and First Amendment made unlawful the issuance of the warrants in the circumstances.

Third, the agents and prosecutors likely misrepresented to the Magistrate Judges that they had obtained the necessary approvals under the DOJ Regulations and/or failed to advise them that these regulations *expressly prohibited* the use of search warrants based on newsgathering conduct. As explained above, the government cannot excuse omissions of this kind by invoking the disclaimer that DOJ regulations grant no rights to the public. “Where the rights of individuals are affected, it is incumbent upon agencies to follow their own procedures. This is so even where the internal procedures are possibly more rigorous than otherwise would be required.” *Morton v. Ruiz*, 415 U.S. 199, 235 (1974). The notion that DOJ can enact regulations to extoll its virtue, but that

prosecutors are then free to ignore those regulations without consequence, is especially offensive in the context of a probable cause determination where those prosecutors must be candid with the court.

The importance courts attach to these DOJ Regulations in determining whether to approve warrants is illustrated by the November 9, 2021 Order issued by Chief Judge Howell of the District Court for the District of Columbia.¹³ This Order circulated to district and magistrate judges the Attorney General's July 19, 2021 Memorandum announcing that, with very narrow exceptions, applications for search warrants (and other compulsory process) to obtain information from members of the news media were *prohibited*. The Order also directed that "any government application for a warrant...seeking information from or records of an individual or entity who is, or who purports to be, a member of the news media...shall include a statement confirming that...the submitting attorney is familiar with...the applicable requirements set forth in [DOJ Regulations], the Justice Manual, and the July 19, 2021 DOJ Memorandum." Implicit in a prosecutor's representation of familiarity with a regulation is that she has complied with it.

Surely the Magistrate Judges here, when presented with the applications for the Microsoft Warrants and PV Warrants, would have expected no less than the disclosures required by this Order. It stands to reason that they would have wanted to know that the applicants *had not* obtained the requisite approval of the Attorney General or his designee to apply for the PV Warrants because DOJ policy precluded it.

Fourth, having seized electronic devices from Project Veritas confidential sources prior to applying for the PV Warrants, the government knowingly withheld from the Magistrate Judge, or was reckless in failing to disclose to her, the material contents of those devices, including:

¹³ Available at <https://www.dcd.uscourts.gov/sites/dcd/files/Revised%20Executive%20Order%202021-67.pdf>

1. communications showing that the sources who offered the Biden diary and belongings to Project Veritas in September 2020 possessed that property before approaching Project Veritas;
2. communications showing that the sources provided these materials to Project Veritas, and its journalists did not remove the items from any residence or other location; and
3. a Contributor Agreement between Project Veritas and the sources, negotiated by legal counsel, which confirmed: (a) the representations of the sources that they had obtained the Biden diary and other belongings lawfully; and (b) Project Veritas acquired these items from the sources in the course, and for the purpose, of newsgathering.

Had the government disclosed this information to Magistrate Judge Cave, she would have been able to determine that there was no basis for believing that Project Veritas or its journalists participated in the alleged theft of Biden's property, much less grounds rising to the level of probable cause. Stated another way, the Magistrate Judge would have realized that the agents and prosecutors were investigating Project Veritas and its journalists for a *non-crime*.

Fifth, on information and belief the government did not inform the Magistrate Judge when applying for the PV Warrants that, less than a week before, counsel for Project Veritas delivered a letter to the prosecutors advising that counsel was authorized to provide information voluntarily regarding the subject of the investigation and, alternatively, to accept any subpoena for Project Veritas records. *See* (Exhibit A). If Magistrate Judge Cave were familiar with the PPA, almost certainly she would have considered this offer of cooperation by Project Veritas to be material to her determination that the proposed seizures were consistent with the statute as well as the implementing DOJ regulations. *See* 42 U.S.C. § 2000aa-11a.2 (directing that DOJ impose “requirement that the least intrusive method or means of obtaining such materials be used”); 28 C.F.R § 50.10(a)(3) (requiring “all reasonable alternative attempts [to] have been made to obtain the information from alternative sources; and after negotiations with the affected member of the news media have been pursued”).

Each of these misrepresentations or omissions constitutes an independently sufficient ground for finding that the government failed to “provide the magistrate with a substantial basis for determining the existence of probable cause.” *Gates*, 462 U.S. at 239. Not only was there no probable cause for the Microsoft Warrants and PV Warrants, but also the conduct of the government, especially when viewed in its totality, interfered with the Magistrate Judges’ performance of their duties.

3. *The Warrants Were a Disproportionate Response to the Gravity of the Alleged Offense Under Investigation*

The Fourth Amendment establishes a requirement that “all searches and seizures must be reasonable.” *Kentucky v. King*, 563 U.S. 452, 459 (2011). Reasonableness has many dimensions, and one is “proportionality between the gravity of the offense and the intrusiveness of the search.” *United States v. Lyles*, 910 F.3d 787, 795–96 (4th Cir. 2018). That was absent here. Even accepting, *arguendo*, the government’s characterization of the conduct under investigation, the alleged non-violent theft of personal papers is a relatively minor offense. *Cf. Welsh v. Wisconsin*, 466 U.S. 740, 750 (1984) (the “underlying offense . . . [was] relatively minor”). But in fact, as explained above, the prosecutors are investigating Project Veritas and its journalists for what is, under, *Bartnicki*, a non-crime. By no reasonable measure can the wholesale seizure of newsgathering materials, attorney-client privileged communications, and irrelevant personal information be considered a proportional response to an alleged low-grade larceny, much less to a non-crime.

4. *The Warrants Allowed Prohibited General Searches*

“The chief evil that prompted the framing and adoption of the Fourth Amendment was the indiscriminate searches and seizures conducted by the British under the authority of general warrants.” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (internal quotations omitted).

This practice is foreclosed by the requirement that an affidavit supporting a search warrant indicate “that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). There must “be a nexus . . . between the item to be seized and criminal behavior.” *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967); accord *United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (requiring that affidavits must set forth “sufficient facts demonstrating why the police officer expects to find evidence in the [place to be searched] rather than in some other place”) (citation omitted).

The Microsoft Warrants are textbook examples of prohibited general warrants. The first such warrant dated January 14, 2021 (21 Mag. 548) demanded production of, *inter alia*, “all [email] content and other information within the Provider’s possession, custody, or control associated with the accounts [of 3 Project Veritas journalists]” reaching back to **January 1, 2020**. *See* (Document No. 64-1) at p. 12 of .pdf. Of course, there could be no probable cause to believe Project Veritas committed a crime associated with the Biden diary in the **eight months** before its journalists acquired that diary in September 2020. Nor could there be probable cause to believe that **each and every** email sent or received during a one-year period “contain[s] evidence, fruits, and instrumentalities of crime.” *Id.* at p. 10 of .pdf. These general warrants enabled the government to obtain, and later peruse at their leisure, communications that the Project Veritas journalists had with confidential sources, other journalists, legal counsel, family members, and friends.¹⁴

¹⁴ The government has recently claimed that it “employed” a filter team to review the Project Veritas data seized from Microsoft. *See* (Docket No. 68) at 1. But the government declines to say whether this team “filtered” for both attorney-client and journalistic privileges. *Id.* There is substantial cause to believe that no review was conducted to filter newsgathering materials: (1) the prosecutors are of the view that Project Veritas is not engaged in journalism; and (2) the U.S. Attorney’s Office Filter Team does not appear to have a First Amendment element in its filter mechanism. *See* (Docket No. 69) at 2.

The stunning reach of the Microsoft Warrants is not limited to the email content. The warrants also commanded the production of “[a]ll address book, contact list, or similar information associated with the Subject Accounts.” *See e.g. id., passim*. Thus, for each of the eight Project Veritas journalists named in the Microsoft Warrants the government obtained the names and contact information for every source, donor, or other confidential associate. And, although the time period for compelled production of O’Keefe’s email content was limited to a four-month period, the directive to produce his contact and address information was not. *See id.* at p. 32 of .pdf. This breach of confidentiality is especially harmful to Project Veritas as its investigative journalism relies heavily on whistleblowers, including those within the federal government.

The PV Warrants also ran afoul of the prohibition against general warrants in authorizing the agents to seize “any and all cellphones, tablets, computers, and electronic storage media” from Meads and Cochran, *see* (Exhibits B and C), and “any and all cellphones” from Mr. O’Keefe.” *See* (Exhibit E). This “any and all” language gave the FBI agents license to seize data regardless of the temporal limitation expressed elsewhere in the warrants. *See* (Exhibits B, C and E) at 3 (August 1, 2020 – Present). As explained above, the FBI CART unit subsequently determined that nearly one-third of the forty-seven devices seized by the agents contained no information within the prescribed time period, and the Special Master found that an additional ten devices seized by the FBI contained no responsive data. *See supra* at 10-11.

The government has admitted the FBI has the technical capability to determine, without viewing the contents of a device, when it was last accessed and thereby to rule out that the device contains information within the warrant period. *See* (Exhibit D) at 5. The FBI agents executing the PV Warrants almost certainly were accompanied by a member of the CART unit who could have used this technology on site instead of seizing all devices. *Cf. United States v. Comprehensive*

Drug Testing, Inc., 621 F.3d 1162, 1171 (9th Cir. 2010) (“it was wholly unnecessary for the case agent to view any data for which the government did not already have probable cause because there was an agent at the scene who was specially trained in computer forensics”).

The FBI agents conducting the search also could have employed on-site less intrusive techniques—for example, attempting to power up each device—to determine whether a device was even readable. Of the 47 devices seized by the FBI, 10 were non-functional or otherwise not readable. *See* (Exhibit F) at 2-4. Moreover, “advancements in technology enable the Government to create a mirror image of an individual’s hard drive, which can be searched as if it were the actual hard drive but without interfering with the individual's use of his home, computer, or files.” *United States v. Gains*, 755 F.3d 125, 135 (2d Cir. 2014); *vacated on other grounds*, 824 F.3d 199 (2016). There is no discernable reason why the FBI could not have made images of the computers, laptops, and storage devices that it seized and left the hardware in the possession of its owners.

The FBI’s seizure of electronic devices from Mr. Meads and Mr. Cochran was particularly indiscriminate, executed without any apparent effort to determine whether the devices were used when the journalists worked for Project Veritas, or even that the devices were operable. In particular, of the 17 devices seized from Mr. Meads, only 2 were determined by the FBI and Special Master to contain information responsive to the PV Warrants. *See* Special Master Report at 2 (Item Nos. 1B57, 1B58). Of the 28 devices seized from Cochran, only 3 were determined by the FBI and Special Master to contain information responsive to the PV Warrants. *See* Special Master Report (Document No. 61) at 1-2 (Item Nos. 1B42, 1B41, 1B40). This indiscriminate seizure of every electronic device in the premises, when only ten percent of the devices contained responsive data, is precisely the kind of general search that the Fourth Amendment forbids.

If there could have been any reasonable dispute that the FBI conducted prohibited general searches in executing the PV Warrants, any doubt has been eliminated by the government's conduct after the FBI CART unit processed the seized devices. As detailed above, the FBI is holding at least 41 devices seized from Mr. O'Keefe, Mr. Meads and Mr. Cochran that either indisputably contain no information responsive to the PV Warrants, cannot be accessed by the CART unit, or have been determined to be inoperable. And yet the government has taken no action to return these devices to the Project Veritas journalists.

When the government discovers that it has seized information outside the scope of a search warrant, the non-responsive information must be returned. *See, e.g., Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976) (“to the extent such papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily and the trial judge was correct in suppressing others”); *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) (“when items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items. . .”). The retention of seized documents for which the government has not established probable cause converts the seizure into an unlawful general warrant. *See CDT*, 621 F.3d at 1176 (noting “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant”). In all events, Project Veritas and its journalists should not have to remain deprived indefinitely by the unlawful search and seizure of their privileged work product, other documentary materials, and personal information that both the FBI CART unit, and the Special Master have determined fall outside the scope of the PV Warrants. This Petition demands the return of those devices and all data extracted or copied therefrom. *See United States v. Ganius*, 824 F.3d 199, 219 (2d Cir. 2016) (“Rule 41(g) permits a defendant or any ‘person aggrieved’ by

either an unlawful or lawful deprivation of property . . . to move for its return”) (internal quotations and citations omitted).

“The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981). “Opposition to such searches was in fact one of the driving forces behind the Revolution itself.” *Riley v. California*, 573 U.S. 373, 403 (2014). That the federal government would continue to use such writs nearly two hundred fifty years later is alarming; that the writs were being used by the government to punish a news organization for gathering unfavorable information about the President is intolerable.

5. *The Investigative Team Violated Procedures Established by the Magistrate Judge to Protect Privileged*

The investigative team knowingly disregarded the Magistrate Judge’s directives regarding the protection of privileged information. Each of the PV Warrants contains the instruction that the collection of evidence be performed “in a manner reasonably designed to protect any attorney-client or other applicable privilege [including] the use of a designated ‘filter team’ separate and apart from the investigative team.” *See* (Exhibits B, C, and E) at 5. And yet, it appears that no filter agents were employed on-site to execute the PV Warrants even though the investigation team knew that (1) Mr. O’Keefe, Mr. Meads and Mr. Cochran were journalists; (2) electronic devices seized from the Project Veritas sources two weeks earlier contained evidence that these journalists were engaged in newsgathering when receiving and investigating the information provided by the sources; and (3) the proffer received by the prosecutors from Project Veritas’s counsel just three days before the PV Warrants were executed provided unmistakable notice that Project Veritas and its journalists were asserting First Amendment and other journalistic privileges.

What is more, the members of the investigative team executing the PV Warrants took photographs of, or otherwise copied, images, recordings and videos stored in mobile devices seized from Mr. O’Keefe (15) and Mr. Cochran (19) “prior to th[e] device locking pursuant to [their] security settings.” *See* (Exhibit D) at 1-22 & nn.1-2. The agents then circulated those materials to other agents and prosecutors on the investigative team. The government has acknowledged that the investigative team viewed this material until Project Veritas and its journalists filed their respective motions for appointment of a Special Master. *See* (Exhibit D) at 1-2 & nn. 2-3. The prosecutors continued to view this evidence even after receipt of a written demand from counsel for Project Veritas that the government cease extraction of the data. *See* (Exhibit D) and (Exhibit G).

It is readily apparent that the investigative team reserved to itself decision-making authority on First Amendment and other privilege questions. They ignored the filter team and other protective procedures established by the Magistrate Judge (and required by the DOJ regulations). Not only has the investigative team been tainted by this exposure to privileged materials, but also their deliberate disregard of warrant requirements and DOJ rules cast further doubt on the reliability of their representations to the Magistrate Judge and this Court.

6. *The Government Compounded Its Fourth Amendment Violations by Sealing the Microsoft Warrants*

The government compounded its Fourth Amendment violations by causing the Microsoft Warrants to be sealed, thus preventing Project Veritas from challenging the grounds for, and scope of, these seizures. The government procured these sealing orders through mere recitals of the text of 18 U.S.C. § 2705(b), which allows for non-disclosure orders when there is “reason to believe that notification of the existence of the [warrant] will result in...destruction of or tampering with evidence...or otherwise seriously jeopardizing an investigation.” Section 2705(b), however,

establishes a *will*, not a may, threshold for non-disclosure orders. *Id.* Project Veritas certainly wanted to protect its confidential sources from harassment (both official and political). But nothing in its communications with Biden’s lawyer or the Joe Biden campaign could have justified a representation to a magistrate judge of reason to believe Project Veritas journalists “will” interfere with the investigation if notified of its existence.

The prosecutors’ recitals of “jeopardy” were no more credible when made in the first § 2705(b) application filed in November 2020, than when repeated verbatim fourteen months later in the government’s application for renewal of non-disclosure orders. *See* 21 Mag. 992 (January 13, 2022). By January 2022 the FBI had very publicly executed and publicized the PV warrants, and the Court had appointed a Special Master to protect the privileged materials seized during those searches. And yet the prosecutors were still representing to magistrate judges that disclosing the seizure of Project Veritas records would jeopardize the investigation. *Id.*

* * *

In sum, in procuring and executing the PV Warrants, the investigative team: violated the PPA; rights guaranteed to Project Veritas and its journalists by the First Amendment, common law Reporter’s Privilege, and the Fourth Amendment; the applicable DOJ Regulations; and the requirements established by the Magistrate Judge. As a result, Project Veritas and its journalists are aggrieved by the unlawful search and seizure of privileged work product and other documentary materials, as well as by the deprivation of that property. Accordingly, all of the seized devices must be returned to Mr. O’Keefe, Mr. Meads and Mr. Cochran, respectively. Fed. R. Crim. P. 41(g). Furthermore, all data extracted, downloaded, imaged, or otherwise copied from those devices by the FBI must be returned or destroyed. *Id.* advisory committee notes (1989 amendments).

E. The Court Must Conduct an Inquiry into the Information Submitted to, and Withheld From, the Magistrate Judges Who Issued the Warrants and Orders.

Rule 41(g) requires that the Court “receive evidence on any factual issue necessary to decide the motion.” The Court must therefore conduct an inquiry that requires the government to come forward with the information that it submitted to the Magistrate Judges, and to answer whether it withheld the material information identified above.

Project Veritas previously requested that the PV Warrant applications be unsealed (Docket No. 33), and the Court denied the request on the ground that disclosure was not necessary for Project Veritas and its journalists to respond to the government’s arguments opposing the appointment of a Special Master. (Docket No. 42). These applications now *are* “necessary to decide th[is] motion,” Fed. R. Crim. P. 41(g), and should be made available to counsel.

The government cannot properly withhold the applications by invoking Fed. R. Crim. P. 6(e) because this investigation has been conducted by the FBI and U.S. Attorney’s Office *independent of* any grand jury inquiry. Indeed, as explained below, it is doubtful that any grand jury has actually been convened to investigate Project Veritas and its journalists. The Microsoft Warrants were obtained promptly after Ashley Biden’s attorney enlisted the aid of the U.S. Attorney’s Office in November 2020. The PV Warrants were obtained for Mr. Meads’ and Mr. Cochran’s homes were obtained almost exactly a year later. But absent a showing that the facts in the warrant applications were gathered through the grand jury process, the contents are not “matter(s) occurring before the grand jury.” Fed. R. Crim. P. 6(e)(2)(B).

There is cause to believe that there has never been an actual grand jury investigation of Project Veritas. On November 4, the day the PV Warrants were executed at Mr. Meads’ and Mr. Cochran’s homes, the prosecutors emailed to counsel for Project Veritas a document purporting to

be a grand jury subpoena (Exhibit H). The document, which appears to be an electronically generated form, does not refer to any particular grand jury then-empaneled by the Chief Judge of this Court. Rather, the document purports to command attendance before “the GRAND JURY” at 40 Foley Square, Room 220, on November 24, 2021. But when a representative of Project Veritas appeared with counsel at that location, on the designated date and time, to lodge Project Veritas’ objections to the compelled production of privileged materials, *there was no grand jury sitting*. See November 26, 2021 Paul Calli, Esq. Letter to AUSA Mitzi Steiner (Exhibit I).

The grand jury may not be used as “a pawn in a technical game,” and the Constitution and federal law tolerate no such result. See *U.S. Dist. Ct. for S. Dist. Of W. Virginia*, 238 F.2d 713, 722 (4th Cir. 1957) (quoting *United States v. Johnson*, 319 U.S. 503, 512 (1943) (Frankfurter, J.)). The government argues when it is convenient for it to do so that the execution of search warrants by the FBI are “independent of” proceedings before the grand jury,” see, e.g., *United States v. Eastern Air Lines, Inc.*, 923 F.2d 241 (2d Cir. 1991), but then solemnly intones the words “grand jury” to shroud in secrecy actions undertaken by the prosecutors and FBI agents for their own purposes. In *Eastern Air*, the government represented to the court, in support of the position that a search warrant affidavit should be unsealed, that its contents were “based on the government’s investigations independent of the investigations by the grand jury and that the affidavit did not reflect matters that had occurred before the grand jury.” *Id.* at 244. The Second Circuit reasoned that “this finding is supported by the government’s representation that the 13 confidential informants cited in the affidavit made their statements to the investigators voluntarily, have not testified before the grand jury, and have not received grand jury subpoenas.” *Id.*

There is reason to believe that is exactly the circumstance here—the prosecutors and FBI agents who applied for the Microsoft orders and warrants merely conveyed to the magistrate judges

information obtained from “informants,” such as Ashley Biden’s lawyer, and that information had not been, and never was, submitted to a grand jury. Absent a showing to the Court that the information in the warrant applications, and the Project Veritas materials seized as a result, were matters occurring before the grand jury, the prosecutors may not shroud its investigation in secrecy by invoking the need to protect “the proper functioning of our grand jury system.” (Docket No. 65) at 3.

In one of its recent filings, the government attempted to add support to these insinuations by reciting that “[s]ince the inception of *the Government’s investigation*, it has been assigned to a duly empaneled grand jury sitting in the Southern District of New York. Gov’t Sur-Reply (Docket No. 68) at 2 (emphasis added). This is a telling admission that all along this has been, and is, an investigation by the U.S. Attorney’s Office and the FBI. That there may have been a record entry made somewhere “assigning” the investigation being conducted by prosecutors and agents to a grand jury, again, begs the actual question. A grand jury did not seize, or cause the seizure, of Project Veritas emails from Microsoft—the prosecutors and agents did. A grand jury did not seize, or cause the seizure, of privileged and personal property from the Project Veritas journalists—the prosecutors and agents did. There was an “assigned” grand jury for the government investigation at issue in *Eastern Air Lines* that actually returned charges, but that assignment did not render the search warrant executed in that investigation by the FBI a “matter occurring before the grand jury.” 923 F.2d at 244 (“the government’s investigations [was] independent of the investigations by the grand jury”).

The occasional use by the government of forms like the one sent to counsel for Project Veritas to compel the production of documents does not alter the fact that nothing is actually “occurring before the grand jury.” Fed. R. Crim P. 6(e)(2)(B). It would elevate form over

substance to allow the government to shroud their work in secrecy by solemnly intoning the words “grand jury.” Nor should the government be allowed to attempt to justify its conduct through *ex parte* submissions. See, e.g., *Abourezk v. Reagan*, 785 F.2d 1043, 1061 (D.C. Cir. 1986), *aff’d*, 484 U.S. 1 (1987) (“[i]t is . . . the firmly held main rule that a court may not dispose of the merits of a case on the basis of *ex parte*, in camera submissions”).

There is nothing secret about the government’s diary investigation. Numerous news articles have been published recounting the work of the investigators, including articles that appeared nearly contemporaneously with the FBI execution of the PV Warrants. See e.g., Josh Gerstein, *FBI Raid on Project Veritas Founder’s Home Speaks Questions About Press Freedom*, POLITICO (Nov, 13, 2021) available at <https://www.politico.com/news/2021/11/13/raid-veritas-okeefe-biden-press-521307>. The privacy interests of Project Veritas, its journalists and sources have already been compromised by these very public government seizure tactics. It would be a cynical ploy for the government to cite privacy as a ground for denying Project Veritas access to the facts underlying these seizures as is necessary for resolution of this Petition.

CONCLUSION

Media Company Project Veritas was approached by sources who lawfully provided Ashley Biden’s diary and personal effects, representing that this property had been abandoned. Project Veritas investigated a news story about the diary, and what Ashley Biden alleged about her father, who was campaigning to be the President of the United States. Project Veritas conducted its investigative reporting with diligence, integrity, and within the bounds of the law.

In sharp contrast, the government has unlawfully seized voluminous newsgathering information protected by the First Amendment and Reporter’s Privilege. But the government has produced nothing, nor can it, to support its specious claim that Project Veritas and its journalists

participated in the theft of property or otherwise committed a crime. The government knows the truth: Project Veritas engaged in journalism protected by the First Amendment. But it is a form of journalism of which the government disapproves, especially where the subject of the newsgathering is the President. But disapproval of Project Veritas' reporting is no justification for secret email surveillance of newsgathering communications, or pre-dawn raids of journalists' homes. These actions are expressly prohibited by the PPA (as well as the DOJ regulations and policy implementing it), the First Amendment, and common law Reporter's Privilege.

Whether these prosecutors have operated without appropriate supervision, or the highest levels of the Biden administration's DOJ are complicit in this investigation into Ashley Biden's abandoned diary, it is time for the Court to curb the government's lawless behavior. The Court should grant this Motion and require the government to immediately return all seized materials to the aggrieved journalists.

Respectfully submitted,

CALLI LAW, LLC

/s/

By: _____

Paul A. Calli

Charles P. Short

14 NE 1st Avenue

Suite 1100

Miami, FL 33132

T. 786-504-0911

F. 786-504-0912

pcalli@calli-law.com

cshort@calli-law.com

Admitted Pro Hac Vice

Harlan Protass

PROTASS LAW PLLC

260 Madison Avenue

22nd Floor

New York, NY 10016
T. 212-455-0335
F. 646-607-0760
hprotass@protasslaw.com

*Counsel for James O'Keefe,
Project Veritas and Project
Veritas Action Fund*

Benjamin Bar
BARR & KLEIN PLLC
444 N. Michigan Avenue
Suite 1200
Chicago, IL 60611
T. 202-595-4671
ben@barrklein.com

Admitted Pro Hac Vice

Adam Hoffinger
GREENBERG TRAURIG LLP
2101 L Street N.W., Suite 1000
Washington, DC 20037
T. 202-331-3173
hoffingera@gtlaw.com

Counsel for Eric Cochran

Stephen R. Klein
BARR & KLEIN PLLC
1629 K Street, NW
Suite 300
Washington, DC 20006
T. 202-804-6676
steve@barrklein.com

Admitted Pro Hac Vice

Brian E. Dickerson
THE DICKERSON LAW GROUP, P.A.
6846 Trail Boulevard
Naples, FL 34108
T. 202-570-0248
bdickerson@dickerson-law.com

Pro hac vice admission pending

Eric Franz
THE LAW OFFICES OF ERIC FRANZ, PLLC
220 Old Country Road
Mineola, NY 11501
T. 212-355-2200
eric@efranzlaw.com

Counsel for Spencer Meads

cc: All Counsel of Record (via ECF)

EXHIBIT A



CALLI LAW, LLC
One Flagler Building, Suite 1100
14 Northeast 1st Avenue
Miami, Florida 33132
T. 786.504.6911
F. 786.504.0912
www.calli-law.com

October 27, 2021

Via Federal Express

Daniel Gitner
Criminal Division Chief
United States Attorney's Office
Southern District of New York
One St. Andrews Plaza
New York, NY 10007

Re: James O'Keefe and Project Veritas

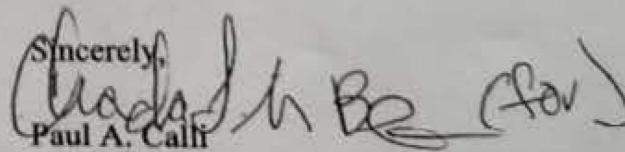
Dear Mr. Gitner:

This Firm represents James O'Keefe and Project Veritas. Mr. O'Keefe is a journalist and Project Veritas is a non-profit media and journalism organization.

I believe that your office is conducting an investigation regarding a matter about which Project Veritas has material and helpful information. I believe the Assistant United States Attorney handling the investigation is Mitzi Steiner. Yesterday my call to your office was put through to Ms. Steiner's office at my request, and Ms. Steiner answered. I identified myself, my clients, and requested an opportunity to speak regarding the investigation. Ms. Steiner asked me how I obtained her name, whether I obtained any other information, stated that she could not speak with me and thanked me for my call before hanging up.

Based on the foregoing I hope that your office has not formed misapprehensions about my clients.

My clients have authorized me to provide an attorney proffer. When or if your office is interested in communicating regarding the investigation, please contact me. In the interim, I am authorized to accept any letter or subpoena from the Department of Justice by email, on behalf of my clients. Reference is hereby made, however, to 28 C.F.R § 50.10 and Justice Manual 9-13.400.

Sincerely,

Paul A. Calli
Chas Short

CC: Mitzi Steiner, Assistant United States Attorney, Via Federal Express
Laura Grossfield Birger, Criminal Division Chief, Via Federal Express

EXHIBIT B

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means

Original

Duplicate Original

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
the Premises Known and Described as [REDACTED]

21 MAG 10547

Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

the Premises Known and Described as [REDACTED], as described in Attachment A-1

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

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):

See Attachment A-1

YOU ARE COMMANDED to execute this warrant on or before November 17, 2021 (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 _____
(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: 11/3/2021 3:49pm

Sarah L. Cave
Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	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(s) 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: _____

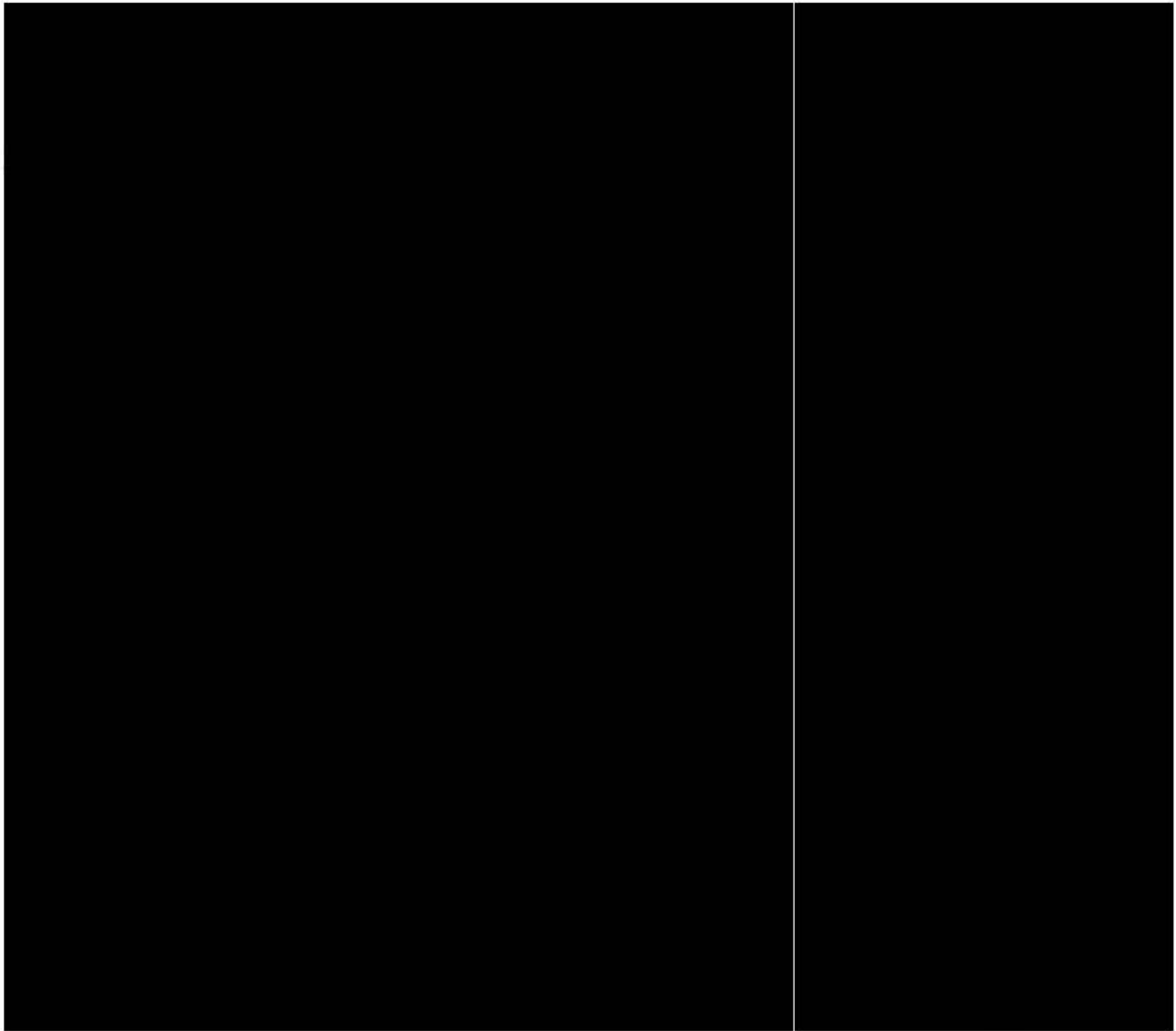
Executing officer's signature

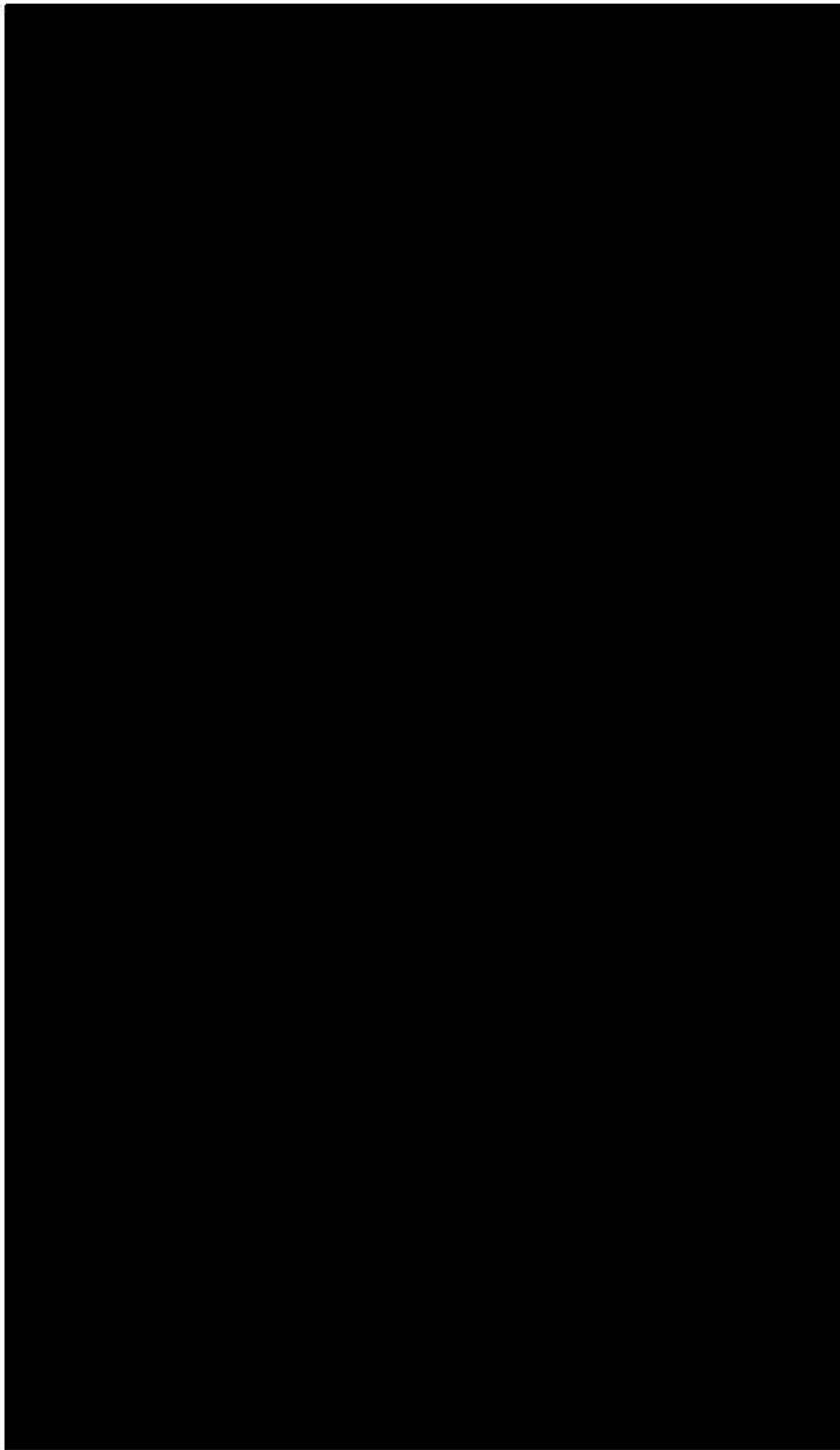
Printed name and title

ATTACHMENT A-1

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:





II. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones, tablets, computers, and electronic storage media within the Subject Premises, including, but not limited to, the cellphones that are or were assigned to the call numbers [REDACTED] or [REDACTED] (collectively, the "Subject Devices").

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the "Subject Offenses") for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to Ashley Biden (and representatives thereof) and/or Ashley Biden's family, friends, or associates with respect to her stolen property.

c. Evidence of the location of Ashley Biden's property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of Ashley Biden's stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from Ashley Biden had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of Ashley Biden's stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of Ashley Biden or property associated with her, and drafts of communications to Ashley Biden, President Biden, and Ashley Biden's associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from Spencer Meads the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of Meads to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Meads to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Meads to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

.

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

Any Electronic Devices in the Possession, Custody, or Control of Spencer Meads, as described in Attachment A-2

)
)
)
)
)
)
)

21 MAG 10547

Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

Any Electronic Devices in the Possession, Custody, or Control of Spencer Meads, as described in Attachment A-2

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

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):

See Attachment A-2

YOU ARE COMMANDED to execute this warrant on or before November 17, 2021 (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 (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: 11/3/2021 3:49pm

Sarah L. Cave
Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	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(s) 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

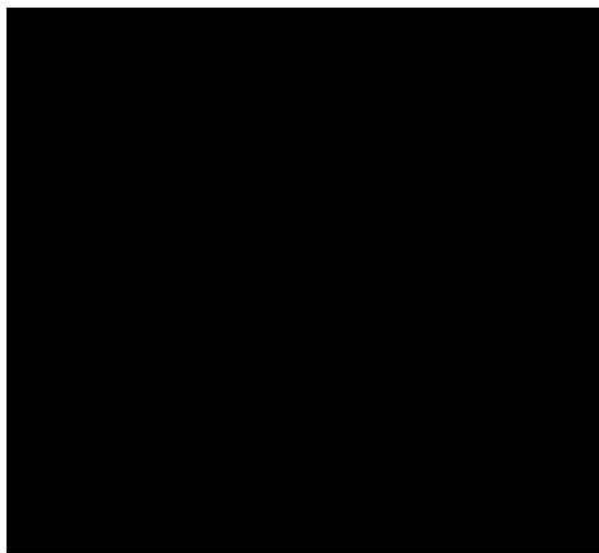
Printed name and title

ATTACHMENT A-2

I. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones, tablets, computers, and electronic storage media within the possession, custody, or control of Spencer Meads, including, but not limited to, the cellphones that are or were assigned to the call numbers [REDACTED] or [REDACTED] (collectively, the "Subject Devices"). The search of Meads shall include any and all clothing and personal belongings, backpacks, briefcases, purses, and bags that are within Meads's immediate vicinity and control at the location where the search warrant is executed. Meads was born on [REDACTED], and is depicted in the following photograph:



B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the "Subject Offenses") for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to Ashley Biden (and representatives thereof) and/or Ashley Biden's family, friends, or associates with respect to her stolen property.

c. Evidence of the location of Ashley Biden's property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of Ashley Biden's stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from Ashley Biden had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of Ashley Biden's stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of Ashley Biden or property associated with her, and drafts of communications to Ashley Biden, President Biden, and Ashley Biden's associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from Spencer Meads the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of Meads to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Meads to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Meads to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in

this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

Case ID: _____

On (date) 11/4/2021

item (s) listed below were:

- Collected/Seized
- Received From
- Returned To
- Released To

(Name) _____

(Street Address) _____

(City) _____

Description of Item (s): ten phones; one smartphone,
one blackberry; one flip phone; one Asus laptop
one Lenovo Laptop, one fob with micro SD,
one macbook; one sandisk

[A large diagonal line is drawn across the remaining lines of the form. Handwritten text along the line includes 'APR 11/4/2021' and '11/4/2021'. There are also some scribbles and initials.]

Received By: [Signature]
(Signature)

Printed Name/Title: TO SIGN
[Signature] ADDA

Received From: [Signature]
(Signature)

Printed Name/Title: John Vourdens, SA

EXHIBIT C

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

the Premises Known and Described as [REDACTED]
[REDACTED]
described in Attachment A-3

21 MAG 10547

Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

the Premises Known and Described as [REDACTED], as described in Attachment A-3

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

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):

See Attachment A-3

YOU ARE COMMANDED to execute this warrant on or before November 17, 2021 (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 (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: 11/3/2021 3:49pm


Judge's signature

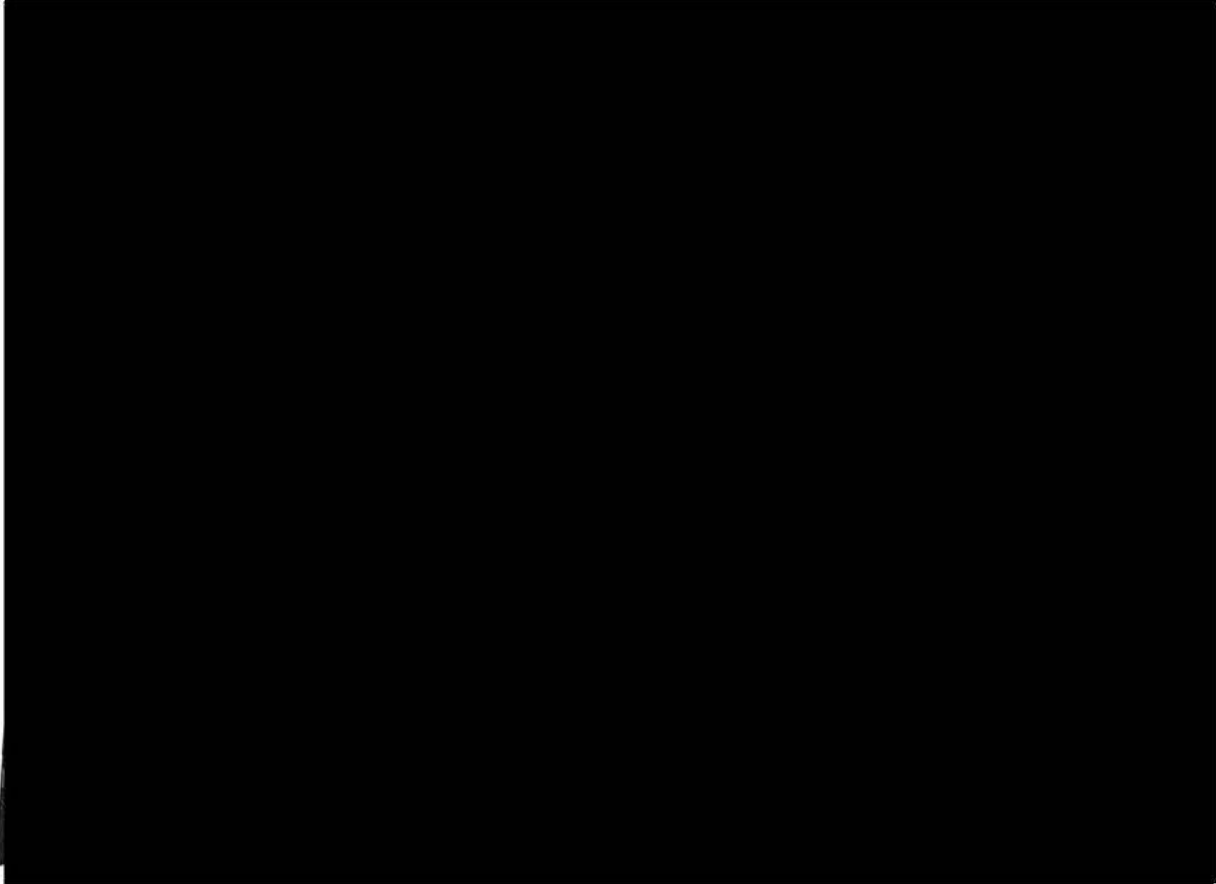
City and state: New York, New York

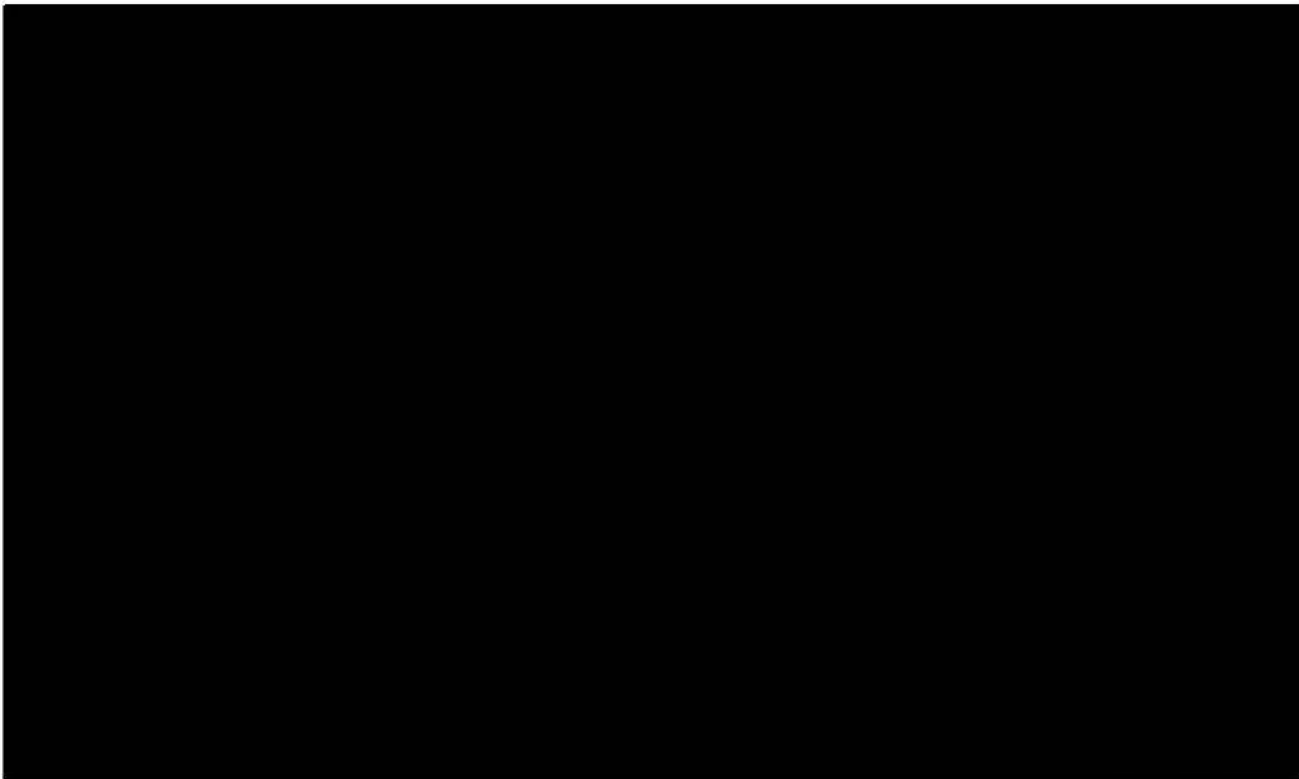
Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-3

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:





II. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones, tablets, computers, and electronic storage media within the Subject Premises, including, but not limited to, the cellphones that are or were assigned to the call numbers [REDACTED] or [REDACTED] (collectively, the "Subject Devices").

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the "Subject Offenses") for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to Ashley Biden (and representatives thereof) and/or Ashley Biden's family, friends, or associates with respect to her stolen property.

c. Evidence of the location of Ashley Biden's property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of Ashley Biden's stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from Ashley Biden had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of Ashley Biden's stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of Ashley Biden or property associated with her, and drafts of communications to Ashley Biden, President Biden, and Ashley Biden's associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from Eric Cochran the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of Cochran to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Cochran to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Cochran to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in

this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

Case ID: NY - 3339758

On (date) 4-NOV-2021

item (s) listed below were:

- Collected/Seized
- Received From
- Returned To
- Released To

(Name) Eric Cochran

(Street Address) [REDACTED]

(City) [REDACTED]

Description of Item (s):

- ~~7 THUMB DRIVES~~
- ~~1 CELL PHONE~~
- 1 COMPUTER PIECE WITH MICRO SD CARD
- 7 MICRO SD CARDS, 3 ADAPTORS
- 2 HARD DRIVES
- ~~1 HARD DRIVE~~
- 1 TOSHIBA HARD DRIVE WITH CORD SIN: [REDACTED]
- 1 NEXUS TABLET SIN: [REDACTED]
- 2 SD STORAGE CARDS, 1 USB
- 1 SEAGATE HARD DRIVE
- 1 LAPTOP WITH CHARGER
- 1 CELL PHONE
- 1 GAMING TABLET WITH POWER CORD

MCP

Received By: [Signature]
(Signature)

Printed Name/Title: M. Perclass / SA

Received From: Eric Cochran
(Signature)

Printed Name/Title: Eric Cochran

Mitzi Steiner Assistant to US Attorneys
212-637-2284

EXHIBIT D



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

December 17, 2021

BY EMAIL

The Honorable Barbara S. Jones
Bracewell LLP
1251 Avenue of the Americas, 49th Floor
New York, New York 10020
barbara.jones@bracewell.com

Re: *In re Search Warrant dated November 5, 2021, 21 Misc. 813 (AT)*
In re Search Warrant dated November 3, 2021, 21 Misc. 819 (AT)
In re Search Warrant dated November 3, 2021, 21 Misc. 825 (AT)

Dear Judge Jones:

The Government respectfully submits this letter to provide an update concerning the status of the electronic devices that are the subject of the Special Master's review.

Devices Seized from James E. O'Keefe, III

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B62	Silver iPhone A1921 Model, IMEI: [REDACTED]		Attempts to access ongoing		
1B61	White iPhone 12 Pro Max, IMEI: [REDACTED] ¹	Yes	Attempts to access ongoing		

¹ Prior to this device locking pursuant to its security settings (and before Mr. O'Keefe filed a motion for the appointment of a special master), law enforcement agents took photographs of a limited set of the device's contents as displayed on its screen. The Government will provide those photographs, which the Government has not reviewed since the filing of Mr. O'Keefe's motion, for inclusion in the Special Master's review.

As reflected above, law enforcement's attempts to access these devices are ongoing. The Government invites Mr. O'Keefe to provide the passwords for these devices in the event he wishes to expedite the extraction process.

Devices Seized from Eric Cochran

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B42	Key Fob SD Card		In queue to be processed		
1B41	Gaming Tower and Power Cord		In queue to be processed		
1B40	Google Pixel 5 ²	Yes	In queue to be processed		
1B39	Seagate Hard Drive		In queue to be processed		
1B38.1	SD Storage Card		In queue to be processed		
1B38.2	SD Storage Card		In queue to be processed		
1B38.3	USB		In queue to be processed		
1B37	Nexus Tablet		In queue to be processed		
1B36	Toshiba Hard Drive		In process		
1B35	Microsoft laptop		In queue to be processed		
1B34	Seagate Hard Drive		In process		
1B33	Seagate Hard Drive		In queue to be processed		
1B32.1	Micro SD card		In process		
1B32.2	Micro SD card		In queue to be processed		
1B32.3	Micro SD card		In queue to be processed		
1B32.4	Micro SD card		In queue to be processed		

² Prior to this device locking pursuant to its security settings (and before Mr. Cochran filed a motion for the appointment of a special master), law enforcement agents took photographs and video recordings of a limited set of the device's contents as displayed on its screen. The Government will provide those photographs and video recordings, which the Government has not reviewed since the filing of Mr. Cochran's motion, for inclusion in the Special Master's review.

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B32.5	Micro SD card		In queue to be processed		
1B32.6	Micro SD card		In queue to be processed		
1B32.7	Micro SD card		In queue to be processed		
1B31	Raspberry PI with Micro SD Card		In queue to be processed		
1B30	Cellphone		In queue to be processed		
1B29.1	Thumbdrive		In queue to be processed		
1B29.2	Thumbdrive		In queue to be processed		
1B29.3	Thumbdrive		In queue to be processed		
1B29.4	Thumbdrive		In queue to be processed		
1B29.5	Thumbdrive		In queue to be processed		
1B29.6	Thumbdrive		In queue to be processed		
1B29.7	Thumbdrive		In queue to be processed		

Devices Seized from Spencer Meads

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B60	Sandisk Extreme Plus		In process		
1B58	One Apple iPhone IMEI: [REDACTED]	Yes	Complete	Pending	To Be Provided Week of 12/20/21
1B57	FOB with Micro SD, FCC: [REDACTED]	Yes	Complete	Pending	To Be Provided Week of 12/20/21
1B56	Lenovo laptop with charger, serial: [REDACTED]		In process		

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B55	ASUS laptop ID: [REDACTED]		In process		
1B54	Flip phone MEDI: [REDACTED], Serial: [REDACTED]	No	Complete	N/A	N/A
1B53	Blackberry MEDI Hex: [REDACTED]	No	Complete	N/A	N/A
1B52	Rose Gold iPhone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B51	Rose Gold iPhone IMEI: [REDACTED]		In queue to be processed		
1B50	Silver iPhone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B49	Black smartphone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B48	Silver and White iPhone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B47	Silver iPhone IMEI: [REDACTED]		Non-functional; attempts to repair ongoing		
1B46	Silver iPhone IMEI: [REDACTED]		Non-functional; attempts to repair ongoing		
1B45	Black iPhone IMEI: [REDACTED]		In queue to be processed		
1B44	White iPhone IMEI: [REDACTED]	Yes	Complete	Pending	To Be Provided Week of 12/20/21
1B43	Black iPhone IMEI: [REDACTED]		Non-functional; attempts to repair ongoing		

In addition, an Apple laptop was recovered from Meads's residence that was subsequently determined to belong to one of Meads's roommates. That device has been returned to that individual.


* * *

Based on information provided by the Federal Bureau of Investigation (“FBI”), the FBI is able to obtain information about whether there is data in a particular timeframe present on a computer or electronic storage media (such as a hard drive) without first extracting the entire device, but it is not able to do so for cellphones or tablets. Accordingly, for the computers and electronic storage media for which the extraction process has not yet commenced, the FBI will first ascertain the timeframe of data present on the device and then proceed to extract data from the device only if that date is August 1, 2020 or later; for the computers and electronic storage media for which the extraction process is underway or has been completed, the Government will provide to the Special Master the contents of those devices only if the date of the most recent data present on the device is from August 1, 2020 or later. Similarly, for cellphones and tablets, the FBI will extract the contents of each device and then the Government will only provide to the Special Master the contents of those devices for which the date of the most recent data present on the device is from August 1, 2020 or later.

The Government is available to provide any additional information that would be of assistance to the Special Master.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: 

Jacqueline Kelly
Robert B. Sobelman
Mitzi Steiner
Assistant United States Attorneys
(212) 637-2456/2616/2284

Cc: Daniel S. Connolly, Esq.
David A. Shargel, Esq.
Paul A. Calli, Esq.
Charles P. Short, Esq.
Harlan Protass, Esq.
Benjamin Barr, Esq.
Stephen Klein, Esq.
Adam S. Hoffinger, Esq.
Steven E. Harrison, Esq.
Brian Dickerson, Esq.
Eric Franz, Esq.

EXHIBIT E

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means

Original

Duplicate Original

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)
the Premises Known and Described as [REDACTED])
[REDACTED])
)

21 MAG 10685
Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

the Premises Known and Described as [REDACTED] as described in Attachment A-1

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

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):

See Attachment A-1

YOU ARE COMMANDED to execute this warrant on or before November 19, 2021 (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 (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: 11/5/2021 11:18am


Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	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(s) 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: _____

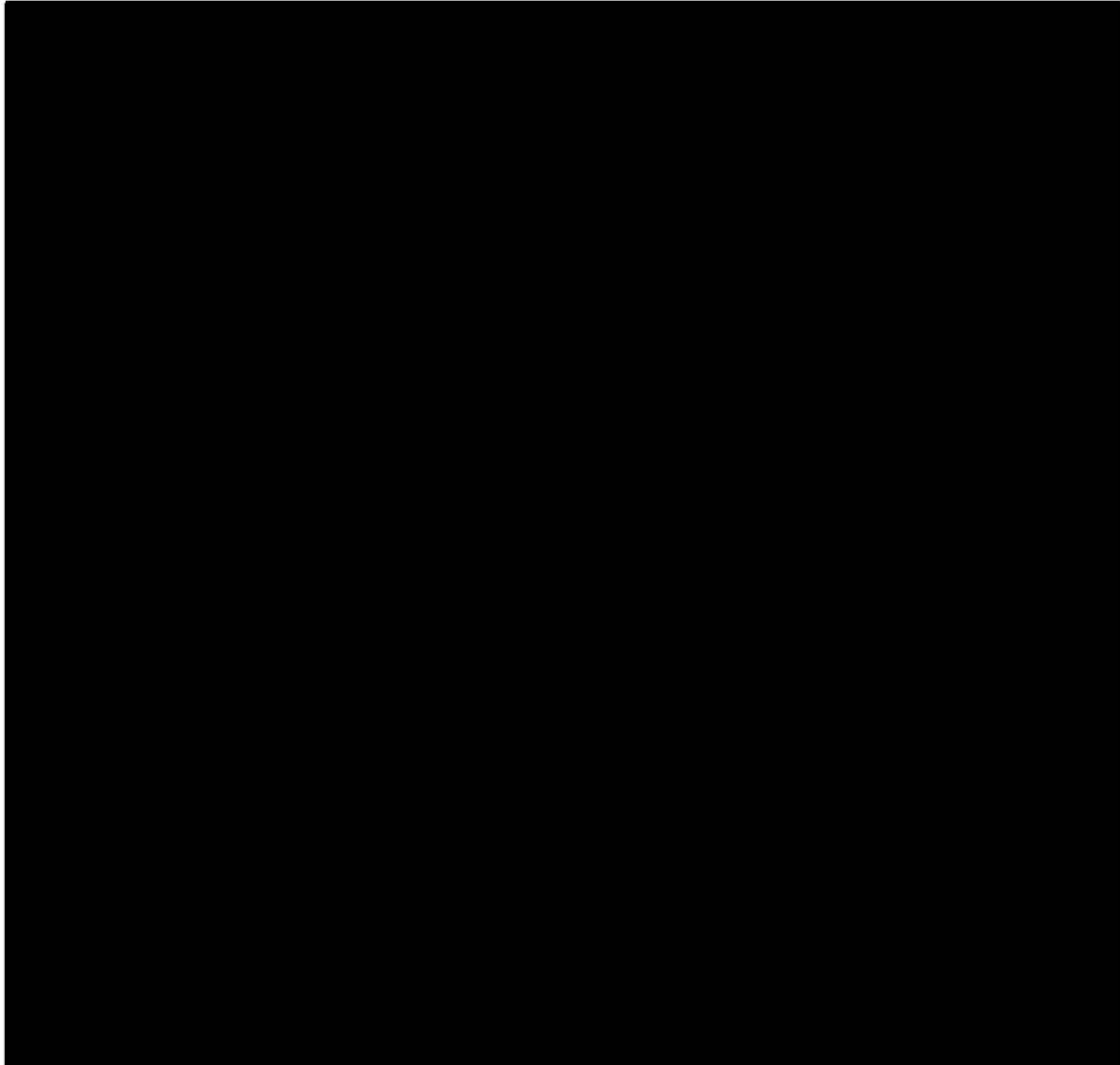
Executing officer's signature

Printed name and title

ATTACHMENT A-1

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:



II. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the Subject Premises, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the "Subject Devices").

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the "Subject Offenses") for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to Ashley Biden (and representatives thereof) and/or Ashley Biden's family, friends, or associates with respect to her stolen property.

c. Evidence of the location of Ashley Biden's property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED] about obtaining, transporting, transferring, disseminating, or otherwise disposing of Ashley Biden's stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from Ashley Biden had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of Ashley Biden's stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of Ashley Biden or property associated with her, and drafts of communications

to Ashley Biden, President Biden, and Ashley Biden's associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from James E. O'Keefe, III the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O'Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O'Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O'Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

Case ID: _____

On (date) 11/6/21 _____

item (s) listed below were:

- Collected/Seized
- Received From
- Returned To
- Released To

(Name) JAMES O'KEEFE

(Street Address) _____

(City) _____

Description of Item (s):

1 WHITE IPHONE [REDACTED] 12 PRO MAX
1 SILVER IPHONE [REDACTED]

JV 11/6/21

Received By: *[Signature]*
(Signature)

Printed Name/Title: James O'Keefe

Received From: *[Signature]*
(Signature)

Printed Name/Title: SA John Vourden's

EXHIBIT F



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

February 6, 2022

BY EMAIL

The Honorable Barbara S. Jones
Bracewell LLP
1251 Avenue of the Americas, 49th Floor
New York, New York 10020
barbara.jones@bracewell.com

Re: *In re Search Warrant dated November 5, 2021, 21 Misc. 813 (AT)*
In re Search Warrant dated November 3, 2021, 21 Misc. 819 (AT)
In re Search Warrant dated November 3, 2021, 21 Misc. 825 (AT)

Dear Judge Jones:

The Government respectfully submits this letter to provide an update concerning the status of the electronic devices that are the subject of the Special Master's review.

Devices Seized from James E. O'Keefe, III

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B62	Silver iPhone A1921 Model, IMEI: [REDACTED]		Attempts to access ongoing		
1B61	White iPhone 12 Pro Max, IMEI: [REDACTED]	Yes	Complete	512 GB	2/3/22

Devices Seized from Eric Cochran

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B42	Key Fob SD Card	Maybe	Complete	5.33 GB	1/14/22
1B41	Gaming Tower and Power Cord	Yes	Complete	369.6 GB	1/14/22

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B40	Google Pixel 5	Yes	In process		
1B39	Seagate Hard Drive	N/A	Damaged – unable to be processed	N/A	N/A
1B38.1	SD Storage Card	Yes	Complete	3.166 GB	1/14/22
1B38.2	SD Storage Card	Yes	Complete	11.4 GB	1/14/22
1B38.3	USB Drive	Yes	Complete	16.09 GB	1/14/22
1B37	Nexus Tablet	No	Complete	N/A	N/A
1B36	Toshiba Hard Drive	Yes	Complete	18.21 GB	1/14/22
1B35	Microsoft laptop		In process		
1B34	Seagate Hard Drive	Yes	Complete	21.06 GB	1/14/22
1B33	Seagate Hard Drive	N/A	Damaged – unable to be processed	N/A	N/A
1B32.1	Micro SD card	Yes	Complete	17.28 GB	1/21/22
1B32.2	Micro SD card	No	Complete	N/A	N/A
1B32.3	Micro SD card	Yes	Complete	6.63 MB	1/21/22
1B32.4	Micro SD card	No	Complete	N/A	N/A
1B32.5	Micro SD card	N/A	Not readable – unable to be processed	N/A	N/A
1B32.6	Micro SD card	No	Complete	N/A	N/A
1B32.7	Micro SD card	N/A	Not readable – unable to be processed	N/A	N/A
1B31	Raspberry Pi with Micro SD Card	No	Complete	N/A	N/A
1B30	Cellphone		Attempts to access ongoing		
1B29.1	Thumbdrive	N/A	Not readable – unable to be processed	N/A	N/A
1B29.2	Thumbdrive	N/A	Not readable – unable to be processed	N/A	N/A
1B29.3	Thumbdrive	No	Complete	N/A	N/A
1B29.4	Thumbdrive	Yes	Complete	138.8 KB	1/14/22
1B29.5	Thumbdrive	Yes	Complete	100.2 MB	1/14/22
1B29.6	Thumbdrive	No	Complete	N/A	N/A
1B29.7	Thumbdrive	No	Complete	N/A	N/A

Devices Seized from Spencer Meads

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B60	Sandisk Extreme Plus	N/A	Not readable – unable to be processed	N/A	N/A
1B58	One Apple iPhone IMEI: [REDACTED]	Yes	Complete	63.5 GB	12/22/21
1B57	FOB with Micro SD, FCC: [REDACTED]	Yes	Complete	10.3 MB	12/22/21
1B56	Lenovo laptop with charger, serial: [REDACTED]	N/A	Not readable – unable to be processed	N/A	N/A
1B55	ASUS laptop ID: [REDACTED]	No	Complete	N/A	N/A
1B54	Flip phone MEDI: [REDACTED], Serial: [REDACTED]	No	Complete	N/A	N/A
1B53	Blackberry MEDI Hex: [REDACTED]	No	Complete	N/A	N/A
1B52	Rose Gold iPhone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B51	Rose Gold iPhone IMEI: [REDACTED]		In process		
1B50	Silver iPhone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B49	Black smartphone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B48	Silver and White iPhone IMEI: [REDACTED]	No	Complete	N/A	N/A
1B47	Silver iPhone IMEI: [REDACTED]	N/A	Non-functional – unable to be processed	N/A	N/A
1B46	Silver iPhone IMEI: [REDACTED]		Attempts to access ongoing		

Item No.	Device	Data on or After 8/1/20	Status	Size	Date Provided to Special Master
1B45	Black iPhone IMEI: [REDACTED]		In process		
1B44	White iPhone IMEI: [REDACTED]	Yes	Complete	19.4 GB	12/22/21
1B43	Black iPhone IMEI: [REDACTED]	N/A	Non-functional – unable to be processed	N/A	N/A

The Government is available to provide any additional information that would be of assistance to the Special Master.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: Robert B. Sobelman
Jacqueline Kelly
Robert B. Sobelman
Mitzi Steiner
Assistant United States Attorneys
(212) 637-2456/2616/2284

Cc: Daniel S. Connolly, Esq.
David A. Shargel, Esq.
Paul A. Calli, Esq.
Charles P. Short, Esq.
Harlan Protass, Esq.
Benjamin Barr, Esq.
Stephen Klein, Esq.
Adam S. Hoffinger, Esq.
Steven E. Harrison, Esq.
Brian Dickerson, Esq.
Eric Franz, Esq.

EXHIBIT G



CALLI LAW, LLC
One Flagler Building, Suite 1100
14 Northeast 1st Avenue
Miami, Florida 33132
T. 786.504.0911
F. 786.504.0912
www.calli-law.com

November 6, 2021

Mitzi Steiner
Assistant United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Via PDF email: Mitzi.Steiner@usdoj.gov

Robert Sobelman
Assistant United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

**Via PDF email:
Robert.Sobelman@usdoj.gov**

Jacqueline Kelly
Assistant United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

**Via PDF email:
Jacqueline.Kelly@usdoj.gov**

Re: Seizure of James O'Keefe's Cell Phone

Dear Ms. Steiner, Mr. Sobelman and Ms. Kelly:

I am writing on behalf of Project Veritas, and James O'Keefe, both of whom I represent.

By this letter, I request that the government sequester and not access Mr. O'Keefe's cell phone, which it seized this morning. Mr. O'Keefe's cell phone contains attorney-client privileged communications and attorney work product related to this investigation. It also contains attorney-client privileged materials and attorney work product for numerous matters unrelated to the government's inquiry. For example, it contains privileged materials related to Project Veritas's defamation suit against the New York Times. The cell phone contains other materials that are protected by the attorney-client and work product privileges belonging or relating to Mr. O'Keefe individually, Project Veritas, and/or the Project Veritas Action Fund.

In addition to the above-described privileged materials, Mr. O'Keefe's cell phone contains other material protected by the First Amendment that the government must not access, including donor information for Project Veritas and Project Veritas Action Fund, information related to on-

going news investigations unrelated to the government's inquiry, and whistleblower information. The privileged and First Amendment information (hereinafter "Protected Information") may not lawfully be accessed by your office, the FBI, or any so-called "taint team" that the government has assembled, or may plan to assemble, for the purpose of reviewing the seized electronic devices.

The government's seizure of Mr. O'Keefe's cell phone violates The Privacy Protection Act ("PPA"), 42 U.S.C. 2000aa. The PPA generally prohibits the search and seizure of "work product materials" possessed by a person or entity in connection with "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. 2000aa(a). There is no exception applicable on the present facts.

Likewise, the PPA's prohibition on the search and seizure of non-work product materials is applicable. The general rule for non-work product materials under the PPA is that "documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in our affecting interstate commerce" are prohibited from search and seizure in connection with a criminal investigation. 42 U.S.C. 2000aa(b). There is no exception applicable on the present facts.

The seizure also violated 28 C.F.R. 50.10 and the Justice Manual's guidance on that regulation. 28 C.F.R. 50.10 states that the government's use of subpoenas and search warrants "to seek information from, or records of, non-consenting members of the news media [are] extraordinary measures, not standard investigative practices." 28 C.F.R. 50.10(a)(3). The government must obtain high level approvals before seeking a search warrant on a member of the news media like Mr. O'Keefe, and the member of the news media should be given "reasonable and timely notice" of the high level determination. 28 C.F.R. 50.10(e)(2)(i). The exceptions are not applicable. Moreover, you are aware I was willing to accept service of a grand jury subpoena on behalf of Mr. O'Keefe (as I did for Project Veritas) and rather than pursue less First Amendment intrusive means, the government chose to execute a search warrant. This contravenes the policy preferences articulated in both 28 C.F.R. 50.10(a)(3) and the corresponding guidance in Justice Manual 9-13.400.

I also request that the government sequester and not access devices seized from Spencer Meade and Eric Cochran earlier this week. Both individuals are former employees of Project Veritas, and the devices seized from them may contain some of the same attorney-client, work product and First Amendment information described above that is the protected property of Project Veritas.

So that we may take appropriate action, please provide forthwith:

1. A copy of the warrants by which electronic devices were seized from Mr. O'Keefe, Mr. Meade and Mr. Cochran;
2. A copy of the search warrant affidavits for the foregoing; and
3. A description of the government's efforts to comply with the requirement of 28 CFR 50.10 and J.M. 9-13.400, including but not limited to:

- a. Whether the government obtained approval from senior DOJ officials prior to applying for the search warrants,
- b. If not, why it did not,
- c. Whether this matter was submitted to DOJ's News Media Review Committee,
- d. And if not, why not.

It is imperative that you acknowledge this request immediately and provide written assurances that the government will sequester and not access the seized electronic devices. Should you decline this request, or fail to respond within twenty-four (24) hours, we will seek immediate judicial intervention.

Sincerely,

A handwritten signature in blue ink that reads "Paul A. Calli". The signature is written in a cursive, flowing style.

Paul A. Calli

Chas Short

EXHIBIT H



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

November 4, 2021

Project Veritas
c/o Paul A. Calli, Esq.
Calli Law, LLC
One Flagler Building, Suite 1100
14 Northeast 1st Avenue
Miami, Florida 33132
pcalli@calli-law.com

Re: Grand Jury Subpoena


Dear Mr. Calli,

Please be advised that the accompanying grand jury subpoena has been issued in connection with an official criminal investigation of a suspected felony being conducted by a federal grand jury. The Government hereby requests that you voluntarily refrain from disclosing the existence of the subpoena to any third party. While you are under no obligation to comply with our request, we are requesting you not to make any disclosure in order to preserve the confidentiality of the investigation and because disclosure of the existence of this investigation might interfere with and impede the investigation.

Thank you for your cooperation in this matter.

Very truly yours,

DAMIAN WILLIAMS
United States Attorney

By: 
Mitzi Steiner
Assistant United States Attorney
(212) 637-2284

Grand Jury Subpoena

United States District Court
SOUTHERN DISTRICT OF NEW YORK

TO: Project Veritas
c/o Paul A. Calli, Esq.

GREETINGS:

WE COMMAND YOU that all and singular business and excuses being laid aside, you appear and attend before the GRAND JURY of the people of the United States for the Southern District of New York, at the United States Courthouse, 40 Foley Square, Room 220, in the Borough of Manhattan, City of New York, New York, in the Southern District of New York, at the following date, time and place:

Appearance Date: November 24, 2021 Appearance Time: 10:00 a.m.

to testify and give evidence in regard to alleged violations of:

18 U.S.C. §§ 2, 3, 4, 371, 2314, 2315

and not to depart the Grand Jury without leave thereof, or of the United States Attorney, and that you bring with you and produce at the above time and place the following:

SEE ATTACHED RIDER

Failure to attend and produce any items hereby demanded will constitute contempt of court and will subject you to civil sanctions and criminal penalties, in addition to other penalties of the Law.

DATED: New York, New York
November 4, 2021

Damian Williams

DAMIAN WILLIAMS
*United States Attorney for the
Southern District of New York*

Mitzi Steiner

Mitzi Steiner
Assistant United States Attorney
One St. Andrew's Plaza
New York, New York 10007
Telephone: 212-637-2284



The seal of the United States District Court for the Southern District of New York is visible, featuring an eagle with wings spread, perched on a shield, surrounded by the text "UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK". A large, stylized handwritten signature in black ink is written over the seal.

RIDER

Grand Jury Subpoena dated November 4, 2021
Reference #2020R01153

Instructions and Definitions:

1. “Documents” refers to any and all documents and records within your possession, custody, or control, in whatever form kept (*e.g.*, paper and electronic form) and wherever they may be found (*e.g.*, on computers, tablets, email accounts, iCloud accounts, servers, personal or company-issued cellphones, and other electronic devices), including, but not limited to, correspondence, writings, emails, text messages, messages sent through “apps” or social media accounts, drawings, graphs, charts, calendar entries, photographs, audio or visual recordings, images, and other data or data compilations.
2. All electronically stored information responsive to this subpoena should be produced in accordance with the “Document and ESI Production Specifications” set forth below.
3. The term “Project Veritas” refers to a corporate entity bearing that name and a corporate entity bearing the name “Project Veritas Action Fund,” and includes both entities’s officers, directors, employees, or agents.
4. This subpoena does not call for the production of any documents protected by a valid claim of privilege, although any responsive document over which privilege is being asserted must be preserved. Any documents withheld on grounds of privilege must be specifically identified on a privilege log with descriptions sufficient to identify their dates, authors, recipients, and general subject matter.

Materials to be Produced:

1. For the time period of August 1, 2020, through the present, any and all documents relating to any personal property or tangible items provided to Project Veritas by [REDACTED]
2. For the time period of August 1, 2020, through the present, any and all documents relating to [REDACTED], including, but not limited to, communications, draft or executed written agreements, travel records, and financial documents reflecting funds transferred by Project Veritas to any of the aforementioned individuals or their agents.

Document and ESI Production Specifications:

I. Electronically Stored Information (ESI)

- a. Electronically stored information (ESI) should be produced in accordance with these specifications. If compliance with these specifications would cause undue burden, please contact the United States Attorney’s Office for the Southern District of New York to discuss. Please do not vary from these standards without prior approval.
- b. *All ESI must be produced both in native file format, and in electronically converted TIFF image format including extracted text and load files.*

II. Transactional and Database Records

- a. Transactional records extracted from a database shall be produced in delimited ASCII text data format or in another easily computer-importable non-proprietary file format that does not incur a loss of data. Field headers shall be included for each column of data, and a data dictionary or other explanation of the contents of each column shall be provided.
- b. Images of items associated with transactions, such as checks, shall be produced in graphic data files in a commonly readable, non-proprietary format, such as TIFF or JPEG, with the highest image quality maintained, and named in a manner that uniquely associates them with the relevant transaction record(s).
- c. Where responsive ESI is contained in a complex relational or proprietary database (*e.g.*, Oracle, SAP, SQL, MySQL, QuickBooks) from which records cannot readily be exported without loss of related data, please call the Assistant U.S. Attorney to arrange a meet-and-confer. Identify the database type and version number, and provide the database dictionary and user manuals or other documentation sufficient to describe the structure and content of the database. The meet-and-confer will evaluate, for example, production of a backup of the database (*e.g.*, an .SDF file for a SQL implementation), or other alternatives, such as delimited ASCII exports of custom queries.

III. Native File Format for ESI

- a. All documents must be provided in the original file or “native” format in which the document was created.
- b. System and executable files should not be produced unless specifically requested.
- c. Email files must be delivered in their native format (*e.g.*, Outlook .PST or .msg, Lotus .NSF, etc.).
- d. Relevant information stored in database applications (*e.g.*, Oracle, Sybase, or MSSQL) should only be produced after first consulting with the SDNY attorney to determine method and format of delivery.
- d. Files must be copied and produced in such a manner as to preserve all associated document and file system metadata. See list of required metadata fields below.
- f. Note: a PDF file is *not* considered a native file unless the document was initially created as a PDF.

IV. Electronically Converted TIFF Format for ESI

- a. In addition to the native format, you must also provide an electronically-produced (*i.e.*, not a printed and scanned) TIFF image version, including extracted text and load files, and available metadata, for each document produced in native format.
- b. The electronically converted TIFF production must comply with the TIFF Image Production and Cross Reference File Specifications set forth below.
- c. The electronically converted TIFF production must be provided in a Concordance .dat load,

together with images and the necessary image cross-reference file. *See* the Delivered Fields Specifications below.

V. Custodian, ESI Source Location, and Path—Naming Conventions

- a. For each document that is produced, the custodian; the ESI source location (*e.g.*, network server, network hard drive, media); and the network or folder path, must be specified in a .dat file.
- b. All ESI provided must be broken down in the following folder structure: by custodian, then by data category (*e.g.*, JohnDoe/Mailfiles/datafiles/desktopfiles).

VI. Production of Paper Records

- a. Paper records should be produced in ASCII delimited format, as detailed below.

ASCII delimited text file (.dat) format

- i. The first line of the text file must contain the field names.
 - ii. In most instances, the StartBates should be the Image Key field unless another field has been designated the key field by the Government.
 - iii. The delimiters used should be the default values used by Concordance: comma (ASCII value 20); quote (ASCII value 254); and newline (ASCII value 174).
 - iv. Produce a page header indicator in the following format, <<**batesno**>>, on a separate line for every page of OCR.
- b. If there will be more than one production, please confirm the database fields and structure remain consistent between data deliveries.

VII. Delivered Fields Specifications

The database and load file provided must contain, at minimum, the first and last Bates number for each document, and all applicable OCR text. The .dat file should contain a path to the OCR. The OCR of the documents should be on a document level.

VIII. TIFF Image Production and Cross Reference File Specifications

- a. Documents should be electronically converted or, if need be, scanned (at 300 dpi) into single-page CCITT Group IV TIFF files. TIFF file names should match the assigned Bates number of the underlying document page, should be unique, and sequentially numbered. Searchable PDF files will be accepted only after a consultation between the provider and USAO technical support staff. Multi-page TIFF files are strongly discouraged.
- b. Bates numbers should be electronically “endorsed” onto images. The file name assigned to the image should match the underlying document’s Bates number. Bates numbers should be alpha-numeric, with the numeric portion of the stamp being “zero-filled”. As an example, as assigned Bates numbered series of documents such as “ABC1”, “ABC2”, “ABC3” would be unacceptable, whereas “ABC000001”, “ABC000002”, “ABC000003” is preferred.
- c. Images should be placed on delivered media in a master folder named **XIMAGES**.
- d. Cross-reference File. TIFF files must be accompanied with an image cross-reference file, preferably an Opticon .opt file, otherwise an IPRO .lfp file will be acceptable. *See* below.

This file must associate each Bates number with the corresponding single-page TIFF file name and indicate its location on the media provided. The file should contain one line for every page in the collection, and must contain the document Bates number and the fully qualified path to the image, beginning with the media volume.

Below is a sample for an Opticon .opt file

```
XYZCO_00663941,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663941.tif,Y,,,1
XYZCO_00663942,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663942.tif,Y,,,1
XYZCO_00663943,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663943.tif,Y,,,2
XYZCO_00663944,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663944.tif,,,,
XYZCO_00663945,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663945.tif,Y,,,1
XYZCO_00663946,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663946.tif,Y,,,2
XYZCO_00663947,,D:\Company\Doe
Production\AUTO0003\XYZCO_00663947.tif,,,,
```

Below is a sample for an IPRO .lfp file:

```
IM,ABC-000001,D,0,@VOL01;IMG_0000001;ABC-000001.tif;2,0
IM,ABC-000002,,0,@VOL01;IMG_0000001;ABC-000002.tif;2,0
IM,3542-S-000001,D,0,@VOL01;IMG_0000001;3542-S-
000001.tif;2,0
IM,3542-S-000002,,0,@VOL01;IMG_0000001;3542-S-
000002.tif;2,0
IM,3542-S-000003,,0,@VOL01;IMG_0000001;3542-S-
000003.tif;2,0
```

IX. Delivery Media

- a. All data and image deliveries must be made through a file-sharing site approved by this Office (*i.e.* USAfx), thumb drive, or USB 3.0 external hard drive, depending on data volume.

X. Metadata Fields

The production should include the following metadata fields:

```
Prodbeg
Prodend
Prodbegattach
Prodendattach
From
To
CC
BCC
Subject
```


Date sent
Time Sent
Author
Date Created
Time Created
Date last Modified
Time Last Modified
File Name/Document Name
File Extension
Document Type/Record Type
MD5 Hash
Custodian
Page Count
File Size
Original Folder Path

EXHIBIT I



CALLI LAW, LLC
One Flagler Building, Suite 1100
14 Northeast 1st Avenue
Miami, Florida 33132
T. 786.504.0911
F. 786.504.0912
www.calli-law.com

November 26, 2021

Mitzi Steiner, Esq.
Assistant United States Attorney
United States Attorney's Office
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007

Via PDF email: Mitzi.Steiner@usdoj.gov

Re: In re November 4, 2021 Grand Jury Subpoena

Dear Ms. Steiner:

We write to confirm the events of Wednesday, November 24, 2021 when Project Veritas appeared at 10:00 am as directed in the attached November 4, 2021 Grand Jury Subpoena (the "Subpoena"). Before doing so, however, we note several background events that provide appropriate context.

Project Veritas had requested your consent to an extension of the Subpoena return date until a date after Judge Torres adjudicated several pending motions. The government declined our request, and then successfully opposed our motion seeking such an extension. In particular, the government argued that Judge Torres lacked the authority to extend the Subpoena return date because of the Grand Jury's "unique role and carefully protected province." [DE 37] at 3.

On Wednesday, November 24, 2021 Project Veritas appeared at 10:00 am in Room 220 of the United States Courthouse as commanded by the Subpoena. Specifically, a witness designated by Project Veritas brought a written submission addressed to the Grand Jury Foreperson that provided information called for by the two Subpoena categories of "Materials to be Produced." That witness was accompanied by Harlan Protass, Esq., co-counsel for Project Veritas.

Mr. Protass and the witness were surprised to find that there was *no grand jury* sitting that morning and that no one from your Office was present. Nevertheless, Mr. Protass presented a copy of the Subpoena to the clerk on duty in Room 220 and agreed to wait while the clerk notified you of the witness's presence. Mr. Protass and the witness waited for *over an hour* before you called the clerk and he was able to speak with you.

You expressed "surprise" that Project Veritas had designated a representative who traveled to the courthouse to appear before the Grand Jury. Mr. Protass pointed out that the Subpoena

commanded the personal appearance of Project Veritas to testify and give evidence and that the Subpoena had not afforded Project Veritas the option of delivering its response to the government. You appeared to question Mr. Protass' description of the Subpoena but, after reviewing a copy, confirmed that it did not afford for any such "delivery" option. You expressed regret for any "confusion" about the Subpoena and stated that the Project Veritas' submission brought by its witness and addressed to the Grand Jury Foreperson be delivered to you in lieu of the Grand Jury Foreperson.

Given your express direction to Mr. Protass, we enclose Project Veritas' November 24, 2021 response to the Subpoena. Project Veritas, however, reserves all objections to these irregular procedures.

Respectfully,

CALLI LAW, LLC

/s/

By: _____

Paul A. Calli
Charles P. Short

14 NE 1st Avenue
Suite 1100
Miami, FL 33132
T. 786-504-0911
F. 786-504-0912
pcalli@calli-law.com
cshort@calli-law.com

Admitted Pro Hac Vice

Harlan Protass
PROTASS LAW PLLC
260 Madison Avenue
22nd Floor
New York, NY 10016
T. 212-455-0335
F. 646-607-0760
hprotass@protasslaw.com

Benjamin Barr
BARR & KLEIN PLLC
444 N. Michigan Avenue
Suite 1200
Chicago, IL 60611
T. 202-595-4671
ben@barrklein.com

Stephen R. Klein
BARR & KLEIN
1629 K. Street, NW
Suite 300
Washington, DC 20006
T. 202-804-6676
steve@barrklein.com

*Counsel for James O'Keefe,
Project Veritas and Project
Veritas Action Fund*

Enclosures