



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

March 22, 2022

VIA CM/ECF

Honorable Analisa Torres
United States District Court
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: In re Search Warrant dated November 5, 2021, Case No. 21-MC-00813 (AT)

Dear Judge Torres:

We write to request preliminary relief from multiple government seizures of newsgathering, attorney-client privileged, and personal materials from Project Veritas and its journalists, separate and apart from the warrants that are the subject of this Court's December 8, 2021, Order. (Docket No. 48).

In pursuit of their investigation into President Biden's adult daughter's abandoned diary and personal belongings, the United States Attorney's Office for the Southern District of New York, and Assistant United States Attorneys Robert Sobelman, Mitzi Steiner, and Jacqueline Kelly have proceeded with total disregard for the First Amendment and with the utmost hostility towards the free press. The pre-dawn raids at the homes of James O'Keefe (the journalist who founded Project Veritas and continues to serve as its President) and two former Project Veritas journalists enabled the government to seize journalists' electronic devices filled with First Amendment-protected materials and attorney-client privileged information. Out of respect for "any First Amendment concerns, journalistic privileges, and attorney-client privileges," and to institute a process that would "not only be fair but also appear to be fair," this Court granted the aggrieved journalists' Motions to Appoint a Special Master to review the contents of the seized electronic devices before providing any materials to a government filter team, and ultimately to make privilege determinations following the aggrieved journalists' objections. (Docket No. 48) at 3 (citations omitted) and 4.

We have recently learned, however, that the government already had in place mechanisms for circumventing these protective processes and invading the First Amendment and attorney-client privileges of Project Veritas and its journalists, the existence of which the government concealed from counsel for Project Veritas and its journalists and, we believe, from this Court. We have discovered that from November 2020 to April 2021, the government used compulsory

demands, including secret warrants and 18 U.S.C. § 2703(d) orders, to obtain voluminous materials from Microsoft, the email services provider used by Project Veritas, spanning the email accounts of eight journalists and Project Veritas's Human Resources Manager. This means that by the time the undersigned filed the Motion to Appoint a Special Master on November 10, 2021, the government had already seized Project Veritas's journalistic and attorney-client privileged materials, without regard to topic or the aforementioned privileges and far outside the relevant time period.

Compounding the privilege violations arising from this invasion, the government also muzzled Microsoft with a series of non-disclosure orders, which the government sought to continue even after this Court ordered the appointment of a Special Master and after the government's diary investigation had long been a matter of public record such that any purported grounds for the non-disclosure orders became non-existent. It appears that the government misled this Court by omission, failing to disclose during the briefing and arguments over the appointment of a Special Master that the government had already obtained through these surreptitious actions many of the privileged communications this Court charged the Special Master with protecting. The government's clandestine invasions of journalist's communications corrode the rule of law.

The government apparently disdains the free press, and candor to the Court and opposing counsel. In light of the government's violations of Project Veritas's First Amendment, journalistic, and attorney-client privileges, as well as the government's attendant failure to disclose these matters before or during the litigation of our motion for appointment of a Special Master, Project Veritas requests that this Court, pursuant to its supervisory powers, inherent authority, and Fed. R. Crim. P. 41(g), enter an Order requiring the government to:

(1) immediately halt access, review, and investigative use of Project Veritas materials that the government obtained from Microsoft (*cf.* November 12, 2021 Order acknowledging pause in government extraction and review of James O'Keefe's mobile devices);

(2) inform this Court and counsel whether the government used a filter team to conduct a review of the data it seized from Microsoft on the basis of both attorney-client and journalistic privileges;

(3) inform this Court and counsel of the identities of any prosecutors, agents, or other members of the investigative team who have reviewed any data seized from Microsoft, what data they reviewed, and when they reviewed it; and

(4) disclose to the Court and counsel the identity of any other third party to which the government issued demands for Project Veritas data under the Electronic Communications Privacy Act ("ECPA") with or without a non-disclosure order.

This interim relief is necessary to avoid compounding the harm to Project Veritas caused by the government's violations of law and principles of candor and to enable Project Veritas to seek appropriate further relief.

**The Government Secretly Obtained Voluminous
Privileged Project Veritas Materials from Microsoft**

The government's failure to disclose its previous invasions of Project Veritas's privileges makes a mockery of these proceedings. While we conferred with the government and then moved for relief from the government's seizures of journalists' electronic devices, the government sat silent, failing to disclose that it had already obtained vast amounts of privileged materials from Microsoft. Nor, apparently, did the government inform this Court. We suspect that the government also withheld this information from Magistrate Judge Cave, from whom it obtained the search warrants to seize journalists' electronic devices (although we cannot know, as the search warrant affidavits remain unjustifiably sealed¹ at the time of this filing).

Each time the government compelled Microsoft to produce Project Veritas's material, it also served a non-disclosure order pursuant to 18 U.S.C. § 2705(b).² The government seized both content and non-content information from the Project Veritas email accounts of its Human Resources Manager, James O'Keefe, investigative journalists Spencer Meads and Eric Cochran, and other investigative journalists who were involved in investigating the potential news story about the Ashley Biden diary.

The government's demands to Microsoft were as follows:

¹ The Reporters Committee for Freedom of the Press has sought to unseal the search warrant affidavits, and its 12/20/21 Objection to the Magistrate's Order remains pending. The recent lifting of the government's 18 U.S.C. § 2705(b) Orders weighs in favor of unsealing the search warrant affidavits. *See* Obj. (Docket No. 49).

² Enacted as part of the ECPA, 18 U.S.C. § 2705(b) allows courts to prevent providers from notifying "any other person" of the existence of a warrant, subpoena, or other court order for customer data if the court finds notification "will result in" one of five adverse events: "(1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial." In practice, the government's boilerplate recitations are rarely scrutinized. As Microsoft Vice President of Customer Security & Trust testified before Congress, "Traditionally, secrecy was the exception. In recent years, law enforcement has turned that exception on its head, developing a practice of reflexively asking to keep even routine investigations secret. Providers, like Microsoft, regularly receive boilerplate secrecy orders unsupported by any meaningful legal or factual analysis." *The Need for Legislative Reform on Secrecy Orders*, available at https://blogs.microsoft.com/on-the-issues/2021/06/30/the-need-for-legislative-reform-on-secrecy-orders/#_ednref4 (June 30, 2021).

Date	Instrument Compelling Production	Project Veritas Personnel	Information Obtained	Time Period	Non-Disclosure Order
11/22/20 ³	Subpoena	Human Resources Manager	Subscriber Information, etc.	No time limitation	Initially one year, later extended 180 days
11/24/20	18 U.S.C. § 2703(d) 20 MAG 12623	Human Resources Manager	Email Headers and Timestamps	9/1/20 to present	Initially one year, later extended one year
1/14/21	Warrant 21 MAG 548	Eric Cochran, Spencer Meads, Human Resources Manager	All emails, Address Book, Subscriber Information	1/1/20 to present	Initially one year, later extended one year
1/26/21	Warrant 21 MAG 992	Additional Project Veritas Journalist	All emails, Address Book, Subscriber Information	1/1/20 to present	Initially one year, later extended one year
3/5/21	Warrant 21 MAG 2537	Three Additional Project Veritas Journalists	All emails, Address Book, Subscriber Information	9/1/20 to 12/1/20	One year
3/9/21	18 U.S.C. § 2703(d) 21 MAG 2711	Additional Project Veritas Journalist	Email Header and Timestamps	9/1/20-12/1/20	One year
4/9/21	Warrant 21 MAG 3384	James O'Keefe	All emails, Address Book, Subscriber Information	9/1/20-12/1/20	One year

See Composite Exhibit A (redacted copies).

³ Given the short time that elapsed between when Ashley Biden's lawyer vowed to refer Project Veritas to the United States Attorney's Office for the Southern District of New York in late October 2020, and the commencement of these compulsory demands, it is clear that the prosecutors never obtained the necessary DOJ approvals to seize records of the news media.

Because the government chose to seek *all emails* within the specified time periods, it obtained a significant volume of both attorney-client privileged emails (particularly from Mr. O’Keefe’s account) and First Amendment privileged materials, including constitutionally protected donor identities and communications as well as privileged newsgathering materials wholly unrelated to the potential reporting about the Ashley Biden diary (which was only one news story among many that Project Veritas investigated at the time).⁴ By seizing the contents of *all emails*, the government has also necessarily obtained hyperlinks to some internal Project Veritas cloud computing folders and various internal draft news reporting. We cannot yet know if the government followed these hyperlinks to rummage through Project Veritas’s internal digital files as well.

The government compounded its privilege violations by requiring production of email content from far outside the relevant time period of the news investigation into the Ashley Biden diary. Project Veritas first heard of the diary and what it alleged about now President Joe Biden in early September 2020. The government knew that this was the beginning of the relevant period, as evidenced by its 11/24/20 Order issued pursuant to 18 U.S.C. § 2703(d), which compelled production of records dated on or after 9/1/20. Nonetheless, its next two search warrants required that Microsoft produce emails for a period **beginning January 1, 2020 -- eight months before Project Veritas had ever heard of the Ashley Biden diary.** The fact that the government secretly obtained emails from three different Project Veritas journalists dating from eight months prior to the newsgathering conduct that the government is scrutinizing shocks the conscience. This was eight full months of journalist communications that have no bearing whatsoever on the non-crime that the government is investigating herein, but the government has presumably put its prying eyes on them anyway.

There are also instances of the government obtaining Project Veritas journalists’ communications from months *after* the relevant time period. Its warrants for the emails of Eric Cochran, Spencer Meads, and an additional journalist (as well as Project Veritas’s Human Resources Manager) required Microsoft to produce emails from months after Project Veritas had made its final decision not to publish its reporting about the diary’s allegations about Joe Biden, and long after Project Veritas had provided the diary and other items to local law enforcement in Florida. The government had to know that nothing material could be learned by obtaining journalists’ communications from months after the Ashley Biden diary and her belongings were in the hands of the local police.

Notably, the government represented during the Special Master litigation that “the Government’s investigation is limited to a narrow course of conduct and the particular offenses listed in the search warrants, and therefore its scope does not include all of the Movants’ activities.” (Docket No. 29) at 15. This claim all but concedes the impropriety of the then-secret warrants and other compulsory process the government had already used to obtain Project Veritas email communications without regard to topic or relevant time frame. In fact, our current best estimate is that the government gained unsupervised access to as many as 150,000 emails and 1,000 contacts.

⁴ Unlike legacy corporate media, Project Veritas is a non-profit journalism organization. The compelled disclosure of donor information violates the First Amendment. *See Americans for Prosperity Foundation v. Bonta*, 594 U.S. ___, 141 S.Ct. 2373 (2021).

In addition to these seizures from Microsoft, Uber has also notified Project Veritas that it received some unspecified form of compulsory demand for records and a non-disclosure order. It produced unspecified “responsive information” on March 22, 2021. Former Project Veritas journalists Spencer Meads and Eric Cochran also received such notices from Uber. The aggrieved journalists do not yet know what other forms of compulsory process the government has used to invade the operations of a press organization whose very mission includes investigating government misconduct.

**The Government’s Secrecy Orders and Its Failure to Disclose That It Had Already
Obtained Project Veritas’s Privileged Material**

The government obtained 18 U.S.C. § 2705(b) secrecy orders that prevented Microsoft from disclosing the existence of the government’s demands, which in turn rendered Project Veritas unable to protect its privileges from the government’s prying eyes. To justify its extraordinary invasion of the rights of the free press, the government made boilerplate recitations that its diary investigation would be jeopardized – a specious concern, as it continued its non-disclosure orders long after Project Veritas was aware of the government’s bad faith investigation.

The government’s abuse of 18 U.S.C. § 2705(b) secrecy orders is consistent with the contempt for the First Amendment that it has demonstrated throughout its diary investigation. Non-disclosure orders, like all “court orders that actually forbid speech activities,” are prior restraints. *Alexander v. United States*, 509 U.S. 544, 550 (1993). Prior restraints are “the most serious and least tolerable infringement on First Amendment rights.” *Neb. Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976). By forbidding speech “because of the topic discussed” (*i.e.*, Microsoft could not inform Project Veritas of these government demands for Project Veritas’s newsgathering materials and privileged communications) these orders also operated as content-based restrictions. *See generally Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 163 (2015). Like prior restraints, content-based restrictions are “presumptively unconstitutional.” *Id.* Thus, courts have “almost uniformly” concluded, “nondisclosure orders pursuant to Section 2705(b) . . . are content-based prior restraints on speech, and subject to strict scrutiny.” *See In re Search Warrant for [Redacted].com*, 248 F. Supp. 3d 970, 980 (C.D. Ca. 2017) and *In re Search of Info. Associated with E-mail Accts.*, Case No. 1:18-MJ-723 (AMD), 2020 WL 5627261, at *3 (E.D.N.Y. May 22, 2020), respectively; *see also Microsoft Corp. v. Dep’t. of Justice*, 233 F. Supp. 3d 887, 906 (W.D. Wash. 2017) (orders under Section 2705(b) are prior restraints).

To survive strict scrutiny, government speech restraints like 18 U.S.C. § 2705(b) secrecy orders must be narrowly tailored to serve a compelling government interest and must do so through the least restrictive means of achieving that interest. The government bears the burden of proof under strict scrutiny. *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971). “If a less restrictive alternative would serve the Government’s purpose, the [government] *must* use that alternative.” *United States v. Playboy Entm’t Grp., Inc.*, 529 U.S. 803, 813 (2000) (emphasis added). “When a plausible, less restrictive alternative is offered to a content-based speech restriction, it is the Government’s obligation to prove that the alternative will be ineffective to achieve its goals.” *Id.* at 816. The government “must present substantial supporting evidence,” *Eclipse Enters. v. Gulotta*, 134 F.3d 63, 67 (2d Cir. 1997), “demonstrat[ing] that the recited harms

are real, not merely conjectural, and that the [restraint] will in fact alleviate these harms in a direct and material way,” *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 664 (1994).

Here, the government apparently did not attempt to employ a less restrictive alternative to blanket secrecy. Rather, it used a proverbial bludgeon, not a scalpel, when directing its secret government snooping against fragile First Amendment interests. It then performed its sleight of hand when it launched public search warrants and subpoenas against Project Veritas and its journalists. As noted below, the government ignored guidelines and rules requiring it to respect press freedoms. The government’s flouting of its own rules signals that this irregular investigation was likely undertaken in bad faith—retribution for daring to investigate Joe Biden’s family. This sort of content-based discrimination has no place in First Amendment caselaw. Instead, it demonstrates that the government’s investigation may simply be an “instrument for stifling liberty of expression.” *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1965). And efforts to stifle newsgathering deserve an adequate and prompt remedy by this Court. *Branzburg v. Hayes*, 408 U.S. 665, 709-10 (1972) (Powell, J., concurring) (“the courts will be available to newsmen under circumstances where legitimate First Amendment interests require protection”).

Because a core purpose of the First Amendment is to “protect the free discussion of governmental affairs,” *Mills v. Alabama*, 384 U.S. 214, 218 (1966), speech about this government activity “is entitled to special protection” and rests on “the highest rung of the hierarchy of First Amendment values,” *Connick v. Myers*, 461 U.S. 138, 145 (1983) (citations and quotations omitted); *see also In re Application and Affidavit for a Search Warrant*, 923 F.2d 324, 331 (4th Cir. 1991) (recognizing society’s interest “in law enforcement systems and how well they work,” including the conduct of criminal investigations). Project Veritas had the right to know of these government infringements and to obtain relief against them. But it was precluded from doing so because of the government’s abuse of 18 U.S.C. § 2705(b) secrecy orders. But for the resistance of Microsoft, the government would have extended those restraints on free speech into 2023, despite the government making its investigation public in 2021.

The Government Sought and Successfully Obtained Extensions of Four 18 U.S.C. § 2705(b) Secrecy Orders Even After Its Diary Investigation Was Public

The government also kept these 18 U.S.C. § 2705(b) secrecy orders in place long past the expiration of any arguable justification, such that the government could never have met a standard for strict scrutiny for its First Amendment restraints. The government maintained these secrecy orders for months after lead counsel for Project Veritas and James O’Keefe contacted the government and provided an attorney proffer, months after lead counsel called the government’s attention to the applicable DOJ regulations for obtaining information from the news media, and months after lead counsel stated that he was authorized to accept service of a grand jury subpoena. ***Worse, while the parties conferred about the appointment of a Special Master to protect Project Veritas’s privileged materials seized from journalists’ homes, and while the government argued that the appointment of a Special Master was unnecessary, the government misled Project Veritas and, apparently, the Court by not disclosing that it had already obtained privileged***

*materials.*⁵ The government's decision to withhold this information multiplied these proceedings, forcing Project Veritas to again seek relief from the Court.

This was not a matter of the government passively allowing secrecy orders to remain in place. Rather, the government affirmatively sought and obtained four extensions of its secrecy orders even after its diary investigation was public and the Special Master litigation began. In fact, the government made two of its four requests *after* this Court's order granting the aggrieved journalists' motions. An abbreviated chronology makes the government's utter lack of justification for continued secrecy patent:

10/27/21	<p>Lead counsel for Project Veritas calls the United States Attorney's Office for the Southern District of New York to speak about the investigation and is connected to AUSA Steiner, who asks how counsel had obtained her name and whether counsel had learned any other information before saying she could not speak to counsel, thanking counsel for his time, and hanging up.</p> <p>Lead counsel subsequently sends a letter to the Criminal Division Chief, the new incoming Criminal Division Chief, and Ms. Steiner asking for the opportunity to provide an attorney proffer to correct any misapprehensions the government may have formed and calling the government's attention to the applicable regulations and DOJ guidance for obtaining information from the news media, 28 C.F.R. § 50.10 and Justice Manual 9-13.400. <i>See</i> (Docket No. 10-4).</p>
11/1/21	<p>During a phone conference with AUSAs Steiner, Sobelman, and Kelly, counsel for Project Veritas provides an attorney proffer regarding Project Veritas's news investigation and ultimate decision not to publish its reporting on Ashley Biden's abandoned diary. The government provides no information, and simply listens.</p>
11/4/21	<p>The government raids the homes of former Project Veritas journalists Spencer Meads and Eric Cochran, and seizes electronic devices.</p> <p>Having been fed information by the government, New York Times reporters seek comment while, or immediately after, the government raids the journalist's homes.</p> <p>Lead counsel for Project Veritas accepts service of a grand jury subpoena via email.</p>

⁵ The government had previously refused our request to pause its review of materials seized in its pre-dawn raids on journalists' homes, requiring the undersigned to seek relief from this Court. When the aggrieved journalists did so, the government took the position that Project Veritas was not engaged in journalism. (The absurdity of that argument is now further highlighted by the fact that the government had obtained and reviewed materials from Microsoft indisputably showing that Project Veritas was engaged in newsgathering when it lawfully received the Biden diary from a source and investigated its authenticity and the veracity of its contents.) This underscores the necessity for relief - the government argued that Project Veritas' privileges should not be honored when this Court was looking; what was the government doing before the undersigned and the Court were aware of its secret actions?

11/6/21	<p>Government raids James O’Keefe’s home, seizing his current cell phone and an older cell phone.</p> <p>Lead counsel for Project Veritas sends AUSAs Steiner, Sobelmen, and Kelly a letter requesting that the government not access the seized devices given the privileged materials contained therein and calling their attention to the government’s violation of the Privacy Protection Act (42 U.S.C. § 2000aa), 28 C.F.R. § 50.10, and Justice Manual 9-13.400. <i>See</i> (Docket No. 10-4).</p>
11/7/21	<p>Government sends a letter to Project Veritas counsel in which it “hereby confirms that it has 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 warrant at issue.” <i>See</i> (Docket No. 10-2).</p>
11/10/21	<p>Project Veritas and James O’Keefe move for the appointment of a Special Master (Docket No. 10).</p>
11/15/21	<p>Motion for Appointment of Special Master is publicly docketed. (Docket No. 10).</p>
11/19/21	<p>Government acknowledges in its effort to oppose the Special Master appointment motion that Mr. “O’Keefe and Project Veritas well know” that “the Government approached multiple individuals as part of the investigation prior to the execution of the search warrants.” (Docket No. 29) at 20.</p> <p>That same day, the government seeks a year-long extension of the secrecy order for its subpoena to Microsoft for the Human Resources Manager’s email account. Magistrate Judge Wang grants a 180-day extension instead.</p>
11/24/21	<p>The government previously refused to extend the deadline for a response to its grand jury subpoena. Because the subpoena included no option for responding other than in-person, a Project Veritas corporate representative accompanied by counsel appear at the grand jury room to provide an initial privilege log. In fact, no grand jury was sitting, and no prosecutor was present.</p>
11/29/21	<p>Five days after the Project Veritas corporate representative appears as directed for a grand jury that was not actually sitting, the government obtains a year-long extension of the secrecy order for its 18 U.S.C. § 2703(d) Order to Microsoft for the Human Resources Manager’s email account.</p>
12/8/21	<p>This Court grants the motions filed by James O’Keefe, Project Veritas, and the aggrieved former journalists, appointing The Honorable Barbara D. Jones (Ret.) as Special Master. (Docket No. 48).</p>
1/11/22	<p>The government obtains a year-long extension of its secrecy order for its warrant seeking content for the Human Resources Manager’s email account.</p>

1/13/22	The government obtains a year-long extension of its secrecy order for its warrant seeking content from a Project Veritas journalist's email account.
---------	---

It is impossible for us to understand how the government convinced multiple Magistrate Judges to extend non-disclosure orders for an investigation that was already public and widely-reported upon, including drawing the attention of press advocates like the Reporters Committee for Freedom of the Press and the American Civil Liberties Union. We can only hypothesize that the government omitted material facts from the Magistrates it successfully asked to extend its secrecy orders.

There was no genuine reason for the government to continue abusing these secrecy orders and no excuse for the government's failure to disclose that it had already obtained voluminous privileged Project Veritas communications. The government's only purpose for concealing these measures was to keep Project Veritas and this Court from grappling with the full scope of the threat to Project Veritas's privileges while the Special Master litigation was on-going. This was improper.

The Government Violated Its Own Guidance on Obtaining Materials from Providers, Just as It Previously Violated Its Own Regulations and Guidance on Obtaining Information from Non-Consenting Members of the Media

The government's abuse of 18 U.S.C. § 2703(b) orders in its diary investigation is yet another example of the United States Attorney's Office for the Southern District of New York ignoring DOJ policy, just as it ignored DOJ regulations and policy when it raided journalists' homes. *See* (Docket No. 10) at 8-9 and (Docket No. 38) at 10-11 (discussing how the government's raids on the Project Veritas journalists' homes violated 28 C.F.R. § 50.10, Justice Manual 9-13.400, and the Privacy Protection Act, 42 U.S.C. § 2000aa).

These demands to Microsoft were not routine investigative steps -- 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); *see also* 28 C.F.R. § 50.10(c)(1) (default rule that "members of the Department must obtain the authorization of the Attorney General to issue a subpoena to a member of the news media; or to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party communications records or business records of a member of the news media."). In fact, the DOJ regulations forbid the use of warrants to seize newsgathering information.

Similarly, DOJ policy regarding 18 U.S.C. § 2705(b) orders recognizes that notification to the entity whose information is obtained is the rule, not the exception. *See* U.S. DEP'T OF JUSTICE, *Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b)* (Oct. 19, 2017), *available at* <https://www.documentcloud.org/documents/4116081-Policy-Regarding-Applications-for-Protective>. This policy requires prosecutors seeking to obtain 18 U.S.C. § 2705(b) orders to first make an "individualized and meaningful assessment regarding the need" for such an order. *Id.* at 2. Each application for an 18 U.S.C. § 2705(b) secrecy order must be

“tailor[ed] . . . to include the available facts of the specific case and/or concerns attendant to the particular type of investigation.” *Id.* at 2.

In related guidance, DOJ policy makes clear that the government should not default to obtaining customer data from providers, instead recommending, “[P]rosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation.” COMPUT. CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP’T OF JUSTICE, *Seeking Enterprise Customer Data Held by Cloud Service Providers* at 1 (2017), available at <https://www.justice.gov/criminal-ccips/file/1017511/download>. “[I]dentifying an individual within the enterprise who is an appropriate contact for securing the data is often the first step. In many enterprises, this will be the general counsel or legal representative.” *Id.* at 2. “Working with counsel and the enterprise’s information technology staff, law enforcement can identify and seek disclosure of relevant information. This approach also gives the counsel ***the opportunity to interpose privilege and other objections to disclosure*** for appropriate resolution, and parallels the approach that would be employed if the enterprise maintained data on its own servers, rather than in the cloud.” *Id.* (emphasis added). Moreover, DOJ’s guidance explains, “If an investigation requires only a subset of data . . . approaching the enterprise will often be the best way to get the information or data sought.” *Id.*

Even if the government had been reticent to contact Project Veritas’s in-house general counsel (such reticence would have been unjustifiable), the government has been aware since October 27, 2021, that it could discuss document issues with undersigned lead counsel. Instead, the government waited in the weeds. This is consistent with its all-out assault on the First Amendment and free press.

Conclusion

Because Project Veritas researched a potential news story about what Ashley Biden’s diary recounted about her father, the United States Attorney’s Office for the Southern District of New York has launched a retributive campaign that does violence to the First Amendment. As far as we know, federal law enforcement has never before investigated an abandoned diary. Moreover, the government’s diary investigation has included extreme measures that violate the First Amendment and corrode freedom of the press. The litigation before this Court began when the government searched journalists’ homes and seized electronic devices containing privileged materials. While the Special Master litigation proceeded, the government apparently misled the Court by omission, failing to inform it, and failing to inform the aggrieved journalists, that it had already obtained the contents of privileged emails from Microsoft. The government concealed its past privilege invasions through unjustified 18 U.S.C. § 2705(b) Orders, which it moved to extend even while the Special Master litigation was pending. These abuses of power must not go unpunished. The free press must not go unprotected.

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

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

cc: All Counsel of Record (via ECF)

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In Re Grand Jury Subpoena to
Microsoft Corporation, USA, dated
November 22, 2020, USAO
Reference No. 2020R01153

20 Mag. 12614

§ 2705(b)
Non-Disclosure Order
to Service Provider

SEALED

Upon the application of the United States pursuant to 18 U.S.C. § 2705(b):

1. The Court hereby determines that there is reason to believe that notification of the existence of the attached subpoena will result in one or more of the following consequences, namely, destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Accordingly, it is hereby ORDERED:

2. Microsoft Corporation, USA (the "Provider") shall not, for a period of ~~one year~~ ^{180 days/OTW} from the date of this Order (and any extensions thereof), disclose the existence of this Order or the attached subpoena, to the listed subscribers of the accounts referenced in the subpoena, or to any other person, except that the Provider may disclose the attached subpoena to an attorney for the Provider for the purpose of receiving legal advice.

3. This Order and the Application upon which it was granted are to be filed under seal until otherwise ordered by the Court, except that the Government may without further order provide copies of the Application and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter, and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York
November 19, 2021



UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

EXHIBIT A

20 MAG 12614

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In Re Grand Jury Subpoena to Microsoft
Corporation, USA, dated November 22,
2020, USAO Reference No. 2020R01153

**§ 2705(b)
Non-Disclosure Order
to Service Provider**

SEALED

Upon the application of the United States pursuant to 18 U.S.C. § 2705(b):

1. The Court hereby determines that there is reason to believe that notification of the existence of the attached subpoena will result in one or more of the following consequences, namely, endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Accordingly, it is hereby ORDERED:

2. Microsoft Corporation, USA (the “Provider”) shall not, for a period of one year from the date of this Order (and any extensions thereof), disclose the existence of this Order or the attached subpoena, to the listed subscriber of the account referenced in the subpoena, or to any other person, except that the Provider may disclose the attached subpoena to an attorney for the Provider for the purpose of receiving legal advice.

3. This Order and the Application upon which it was granted are to be filed under seal until otherwise ordered by the Court, except that the Government may without further order provide copies of the Application and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter, and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

November 23, 2020



UNITED STATES MAGISTRATE JUDGE

United States District Court
SOUTHERN DISTRICT OF NEW YORK

TO: Law Enforcement National Security
Microsoft Corporation, USA
1 Microsoft Way
Redmond, WA 98052

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 30, 2020 Appearance Time: 10:00 a.m.

to testify and give evidence in regard to an alleged violation of :

18 U.S.C. §§ 371, 873, 1952, 2314, 2315, 2261A

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

N.B.: Personal appearance is not required if the requested documents are: (1) produced on or before the return date to Special Agent John Vourderis, Federal Bureau of Investigation, 26 Federal Plaza, New York, New York 10278, jvourderis@fbi.gov, 212-384-2890; and (2) accompanied by an executed copy of the attached

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 22, 2020

Audrey Strauss / RBS
AUDREY STRAUSS
*Acting United States Attorney for the
Southern District of New York*

Robert B. Sobelman
Robert B. Sobelman

Assistant United States Attorney
One St. Andrew's Plaza
New York, New York 10007
Telephone: 212-637-2616



RIDER

Grand Jury Subpoena dated November 22, 2020

Reference # 2020R01153

1. All subscriber identifying information, including, but not limited to:
 - a. name
 - b. username or other subscriber identity or number
 - c. address
 - d. primary and alternate telephone numbers
 - e. primary and alternate email addresses
 - f. date of birth
 - g. social security number
 - h. any temporarily assigned network address
 - i. MAC address
 - j. Browser and operating system information
2. Records of session times and durations and any IP addresses used by the subscriber at the beginning, end, and at any time during these sessions;
3. Length of service (including start date) and types of service utilized; and
4. Means and source of payment for services (including any credit card or bank account number).
5. Account notes and logs, including any customer-service communications or other correspondence with the subscriber;
6. Investigative files or user complaints concerning the subscriber.

For any accounts associated with one or more of the following:

■@projectveritas.com

20 MAG 12623

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Orders to Disclose Non-Content
Information Associated with
████@projectveritas.com, Pursuant to 18 U.S.C.
§ 2703(d), USAO Reference No. 2020R001153

TO BE FILED UNDER SEAL

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Microsoft Corporation, USA (the “Provider”), to disclose certain records and other information, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation,

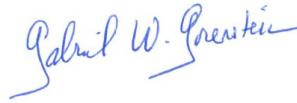
IT IS ORDERED, pursuant to Title 18, United States Code, Section 2703(d), that the Provider will, within ten days of the date of this Order, turn over to federal law enforcement agents the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Application and this Order be sealed until otherwise ordered by the Court, and that the Provider shall not disclose the existence of this Application and/or Order of the Court, or the existence of the investigation, to the listed subscriber or to any

other person (except as necessary to carry out this Order), for a period of one year from the date of this Order.

SO ORDERED:

New York, New York
November 24, 2020

A handwritten signature in blue ink, reading "Gabriel W. Gorenstein". The signature is written in a cursive style with a horizontal line extending from the end.

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

ATTACHMENT A

You are to provide the following non-content information in electronic format to Special Agent John Vourderis of the Federal Bureau of Investigation:

- any header information reflecting the names, usernames, or IP addresses of any sender(s) or recipient(s) of communications, for the time period of September 1, 2020, until the date of this Order; and
- time/date stamps, for the time period of September 1, 2020, until the date of this Order

For the following e-mail account:

■@projectveritas.com

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All
Content and Other Information
Associated with the Email Accounts
[REDACTED]@projectveritas.com,
[REDACTED]@projectvertias.com, and
[REDACTED]@projectveritas.com,
Maintained at Premises Controlled by
Microsoft Corporation, USA, USAO
Reference No. 2020R001153

21 MAG 548

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [REDACTED]@projectveritas.com, [REDACTED]@projectvertias.com, and [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 3 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for the Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

January 14, 2021.

Date Issued

10:22pm

Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the accounts [REDACTED]@projectveritas.com, [REDACTED]@projectvertias.com, and [REDACTED]@projectveritas.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between January 1, 2020, and the date of this warrant, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Microsoft Locator IDs GCC-1552941-K4N8V4 and GCC-1595762-L5Y8J1.

III. Review of Information by the Government

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 records produced by the Provider in order to locate any evidence, fruits, and instrumentalities 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), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Accounts at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the

true identity of the user 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 regarding Ashley Biden, President-Elect Joseph R. Biden, Jr. (and representatives thereof), and/or Ashley Biden's associates regarding 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 and locations of potential co-conspirators, such as communications with other individuals 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-Elect 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 emails reflecting registration of other online accounts potentially containing relevant evidence of the scheme.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Account
[REDACTED]@projectveritas.com, USAO
Reference No. 2020R001153

21 MAG 992

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 3 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that the Provider may disclose this Warrant and Order to an attorney for the Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

1/26/2021
Date Issued

9:56 a.m.
Time Issued

UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the account [REDACTED]@projectveritas.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between January 1, 2020, and the date of this warrant, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Microsoft Locator ID GCC-1605213-K2V7L0.

III. Review of Information by the Government

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 records produced by the Provider in order to locate any evidence, fruits, and instrumentalities 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), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Account at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user 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 regarding Ashley Biden, President Joseph R. Biden, Jr. (and representatives thereof), and/or Ashley Biden's associates regarding her stolen property.

c. Evidence of the location of Ashley Biden's property and the location of the user of the Subject Account 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 and locations of potential co-conspirators, such as communications with other individuals 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 emails reflecting registration of other online accounts potentially containing relevant evidence of the scheme.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Accounts
[REDACTED]@projectveritas.com,
[REDACTED]@projectveritas.com, and
[REDACTED]@projectveritas.com,
Maintained at Premises Controlled by
Microsoft Corporation, USA, USAO
Reference No. 2020R001153

21 MAG 2537

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [REDACTED]@projectveritas.com, [REDACTED]@projectveritas.com, and [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 3 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

March 5, 2021
Date Issued

8:53 am
Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email accounts [REDACTED]@projectveritas.com, [REDACTED]@projectveritas.com, and [REDACTED]@projectveritas.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between September 1, 2020, and December 1, 2020, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Microsoft Locator ID GCC-1627882-J5F7J1.

III. Review of Information by the Government

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 records produced by the Provider in order to locate any evidence, fruits, and instrumentalities 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), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Accounts at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the

true identity of the user 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 regarding Ashley Biden, President Joseph R. Biden, Jr. (and representatives thereof), and/or Ashley Biden's associates regarding 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 and locations of potential co-conspirators, such as communications with other individuals 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 emails reflecting registration of other online accounts potentially containing relevant evidence of the scheme.

21 MAG 2711

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of an Order to Disclose Non-Content
Information Associated with
[REDACTED]@projectveritas.com, Pursuant to 18 U.S.C.
§ 2703(d), USAO Reference No. 2020R001153

TO BE FILED UNDER SEAL

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Microsoft Corporation, USA (the “Provider”) to disclose certain records and other information, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person (including the account subscribers, the owners of any enterprise domain, and any agent, attorney, or affiliate of the foregoing) of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation,

IT IS ORDERED, pursuant to Title 18, United States Code, Section 2703(d), that the Provider will, within ten days of the date of this Order, turn over to federal law enforcement agents the records and other information as set forth in Attachment A-1 to this Order.

IT IS FURTHER ORDERED that the Application and this Order be sealed until otherwise ordered by the Court, and that the Provider shall not disclose the existence of this Application and/or Order of the Court, or the existence of the investigation, to the listed subscriber or to any

other person (except as necessary to carry out this Order), for a period of one year from the date of this Order.

SO ORDERED:

New York, New York
March 9, 2021

A handwritten signature in blue ink, appearing to read "Barbara Moses", is written above a horizontal line.

HON. BARBARA MOSES
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

ATTACHMENT A-1

You are to provide the following non-content information in electronic format to Special Agent John Vourderis of the Federal Bureau of Investigation:

- any header information reflecting the names, usernames, or IP addresses of any sender(s) or recipient(s) of communications, for the time period of September 1, 2020, until December 1, 2020; and
- time/date stamps, for the time period of September 1, 2020, until December 1, 2020

For the following email account:

██████@projectveritas.com

21 MAG 3884

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Account
[REDACTED]@projectveritas.com, Maintained
at Premises Controlled by Microsoft
Corporation, USA, USAO Reference
No. 2020R001153

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within one day of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

4/9/2021
Date Issued

7:17 a.m.
Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email account [REDACTED]@projectveritas.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between September 1, 2020, and December 1, 2020, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Apple Reference ID 21396344.

III. Review of Information by the Government

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 records produced by the Provider in order to locate any evidence, fruits, and instrumentalities 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), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Account at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user such as their name, address, telephone number, email address, payment information, and other personally identifiable information.