DRAFT -- FOR DISCUSSION PURPOSES

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF SEVEN ORDERS RESTRAINING SPEECH

Case Nos. 20 Mag. 12614
20 Mag. 12623
21 Mag. 548
21 Mag. 992
21 Mag. 2537
21 Mag. 2711
21 Mag. 3884

SEALED FILING

MICROSOFT'S APPEAL OF AND REQUEST TO VACATE ORDER RESTRAINING SPEECH

DRAFT -- FOR DISCUSSION PURPOSES

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. INTRODUCTION

The Government has obtained secrecy orders under 18 U.S.C. § 2705(b) that prevent Microsoft from telling its customer—Project Veritas, a self-described "non-profit journalism enterprise" engaged in "undercover reporting"—that the Government has seized from Microsoft emails and other information associated with its customer's business. To justify its restraint of Microsoft's speech, the Government professes concern that its investigation would be jeopardized if its surreptitious seizure of Project Veritas documents stored in Microsoft's cloud were disclosed. To be blunt, the concern is specious. The Government's investigation is no secret; it has been the subject of widespread national media coverage ever since the Government conducted pre-dawn raids on the homes of Project Veritas's founder and two former employees in November 2021. The search warrants for those raids are public, and they disclose not only the subject of the investigation, but also the names of ten potential co-conspirators. On these facts, Microsoft should be free to notify its customer that the Government has seized the customer's information from Microsoft so the customer can, among other things, assert the same rights it has asserted in this Court with respect to the fruits of the November raids. Microsoft now appeals and asks the Court to either vacate the secrecy orders or, at a minimum, modify them to permit Microsoft to disclose the seizures to a trustworthy individual at Project Veritas.

Microsoft bases its request for relief on the First Amendment, which protects its right to speak about issues of public concern and to inform its customers of matters involving their data privacy. Non-disclosure orders ("NDOs"), 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). And by forbidding speech "because of the topic discussed"—here, the Government's demands for Project Veritas's information under 18

U.S.C. § 2703—NDOs like these are also content-based restrictions. *Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2226 (2015). Like prior restraints, content-based restrictions are "presumptively unconstitutional." *Id.* To survive strict scrutiny, they must be narrowly tailored to serve a compelling government interest, and must do so through the least restrictive means of achieving that interest. "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 publicly available information shows the secrecy orders here cannot satisfy the strict scrutiny test.

First, the Government lacks a compelling interest to support these secrecy orders. Project Veritas already knows it is the subject of the Government's investigation. Months ago, the Government served Project Veritas with a grand jury subpoena and then raided the homes of Project Veritas's founder and two former employees pursuant to search warrants now filed on the public docket. News media widely reported the raids and wrote follow-up stories on the investigation. Because the Government's collection of Project Veritas materials in the course of its investigation is now widely known, the Government has no compelling interest in silencing Microsoft from disclosing the orders to Project Veritas. "[O]ne cannot 'disclose' what is already in the public domain." *Bartnicki v. Vopper*, 532 U.S. 514, 546 (2001).

Second, even if the secrecy orders could be justified given the publicity surrounding the investigation, the Government made no attempt to narrowly tailor them to the facts of this case, as the law requires, or to show that notice to Project Veritas would result in any of the harms enumerated in § 2705(b), such as endangering life, risking destruction of evidence, or enabling

flight from prosecution. The Government has offered no reason to suggest that Project Veritas would undertake the sort of rash extra-judicial action identified in § 2705(b)—especially given that the organization has appeared *in this Court* to litigate its concerns with the raids on its employees' homes. Nor can the Government satisfy its burden of showing that a less restrictive alternative, i.e., notice to a trustworthy individual at Project Veritas, would lead to the harms enumerated in § 2705(b). That notice would afford the customer "the opportunity to interpose privilege and other objections . . . and parallels the approach that would be employed if [Project Veritas] maintained data on its own servers, rather than in the cloud." U.S. Dep't of Justice, Seeking Enterprise Data Held by Cloud Service Providers (Dec. 2017) ("DOJ Recommended Practices"), Decl. of James Garland ("Garland Decl."), Ex. M at 2. Preserving Project Veritas's right to object has particular importance here, as the Court has recognized that seizure of Project Veritas's information may implicate "potential First Amendment concerns." *In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mc-00813-AT (S.D.N.Y. Dec. 8, 2021), ECF No. 48 at 2 ("Order Appointing Special Master").

Third, the Government cannot rely on ex parte evidence to justify suppressing Microsoft's speech. "[D]ue process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other." *United States v. Abuhamra*, 389 F.3d 309, 322 (2d Cir. 2004). At the very least, the Government must provide Microsoft with redacted versions or summaries of any ex parte evidence on which it seeks to rely.

II. BACKGROUND

A. Impact of Cloud Computing on the Government's Seizure of Business Information

Cloud computing has fundamentally changed how companies store information. Twenty years ago, companies typically kept their emails and other business information on their physical

property. Today, they increasingly store this information in the "cloud"—i.e., on remote servers owned by companies like Microsoft—a migration that "reduce[s] information technology infrastructure costs, increase[s] resiliency, and improve[s] data availability for mobile workers." DOJ Recommended Practices at 1. Because of cloud computing, "prosecutors [now] have the legal authority to compel the enterprise or a cloud service provider to produce the [customer's] data." *Id.* In other words, cloud computing has made it possible for the Government to seize and search private records not just from the business itself, but also from its cloud provider.

These same developments have made it possible for the Government to do its work in secret. In the past, if the Government wanted to obtain a company's private information, it almost invariably had to obtain that information from a filing cabinet or computer on physical property—meaning the company would know about the search (just as Project Veritas's founder and former employees knew when the FBI appeared at their homes last November).[1] In 1986, however, when the Internet was in its infancy, Congress enacted 18 U.S.C. § 2705(b) as part of the Electronic Communications Privacy Act ("ECPA"). *See, e.g.*, H.R. Rep. No. 99-647, at 21-23 (1986) (positing that email *might* replace paper letters). Under § 2705(b), courts may prohibit 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."

With the migration of enterprise data to the cloud, the Government now has a significant

[1] Even in the rare instances of so-called "sneak and peek" warrants, which permit surreptitious physical searches, the Government must notify the target "within a reasonable period not to exceed 30 days" unless "the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(b)(3).

and unprecedented power: the ability to obtain a company's information *without the company knowing about it.* This secrecy makes it impossible for the company to protect its interests—including its right to assert the attorney-client or journalistic privileges, and other protections—in connection with the investigation.

Microsoft is all too familiar with the Government's practice of obtaining secrecy orders to accompany demands for customer information. But that information belongs to the customer, not Microsoft. For that reason, when law enforcement demands enterprise customer information from Microsoft, it ordinarily asks the Government to redirect the request to the customer. And DOJ recognizes that the customer is generally better positioned than Microsoft to produce its own information. *See* DOJ Recommended Practices at 1-2.

B. Background on Secrecy Orders and DOJ's Commitment to Use Them Sparingly

In 2016, Microsoft challenged the constitutionality of § 2705(b) under the First and Fourth Amendments. *See Microsoft Corp. v. U.S. Dep't of Just.*, 233 F. Supp. 3d 887 (W.D. Wash. 2017). After the district court denied DOJ's motion to dismiss Microsoft's First Amendment claim, DOJ issued a binding policy limiting the cases in which federal prosecutors may seek secrecy orders. *See* U.S. Dep't of Justice, Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b) (Oct. 19, 2017) ("DOJ Policy"), Garland Decl., Ex. L. The DOJ Policy recognizes that notification to the entity whose information is obtained must be the rule, not the exception. *Id.* at 1. Accordingly, the DOJ Policy directs prosecutors to obtain § 2705(b) orders only after an "individualized and meaningful assessment regarding the need" for such an order, and requires that each application for a secrecy order 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.

Within a few weeks of issuing that policy, DOJ issued guidance addressing seizure of

enterprise customer data, i.e., information belonging to "a company, government agency, university, or other enterprise." DOJ Recommended Practices at 1. The Recommended Practices make clear that the federal government should not, as a default, obtain enterprise data from cloud providers. Instead, DOJ recommends that "prosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation." *Id.* "[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). In other cases, prosecutors "have justified reasons for not approaching the enterprise directly, at least initially. If an enterprise is essentially devoted to criminal activity—for example, a small medical practice suspected of engaging in massive Medicare fraud—there may not be a trustworthy individual to approach." *Id.* In these cases, "seeking disclosure directly from the cloud provider may be the only practical option." *Id.* at 2-3.

Notwithstanding this guidance, the Government has continued to resort to secrecy orders, prompting significant litigation. And at least some of those cases have been resolved through modification or withdrawal of the secrecy order. *See In re Microsoft Corporation's Appeal of Non-Disclosure Orders*, No. 20 Misc. 349 (S.D.N.Y.) (resolved when Government agreed to notify customer's outside counsel about demand); *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 19 Misc. 682 (D. Md.) (resolved

when Government agreed to withdraw secrecy order given publicity surrounding investigation); *see also Microsoft Corp. v. United States*, No. 20-1653 (2d Cir.) (resolved when government allowed secrecy order to expire); *United States v. Google*, No. 19-1891 (2d Cir.) (same).

C. DOJ's Limits on Compulsory Process Involving Records of the News Media

DOJ also has recognized the importance of protecting journalists' ability to investigate and report the news. In particular, DOJ has promulgated regulations that limit when it can seek information from—or regarding members of—the news media. *See* 28 C.F.R. § 50.10. The use of compulsory process "to seek information from, or records of, non-consenting members of the news media" is an "extraordinary measure[], not [a] standard investigatory practice[.]" *Id.* § 50.10(a)(3). In July 2021, the Attorney General further circumscribed the Government's ability to issue compulsory process against those engaged in newsgathering. *See* Memorandum from the Attorney General Re: Use of Compulsory Process to Obtain Information From, or Records of, Members of the News Media (July 19, 2021), Garland Decl., Ex. N. Under DOJ's revised policy, prosecutors may "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," except in certain "limited circumstances." *Id.* at 1.

D. The Customer's Use of Microsoft's Enterprise Cloud Services

Microsoft provides cloud-based services, including Microsoft 365 services, which provide email accounts and productivity software to a wide range of enterprise customers. When an enterprise customer signs up for Microsoft 365, it purchases end-user licenses, or "seats," each assigned to a user who receives account credentials and an individual email address. Email addresses hosted by Microsoft 365 incorporate the enterprise's chosen domain name, rather than a Microsoft domain name (*e.g.*, jane.smith@company.com, rather than jane.smith@outlook.com).

The customer here is Project Veritas, which describes itself as a non-profit organization engaged in investigative journalism, news and information gathering, and content publication.[2] As of January 2021, Project Veritas maintained 159 Microsoft 365 seats. Garland Decl. ¶ 2.

E. The Government's Secret Demands for Project Veritas's Information

Between November 2020 and April 2021, the Government served Microsoft with seven demands for Project Veritas's data, seeking information associated with nine email accounts. Each demand was accompanied by a non-disclosure order issued under 18 U.S.C. § 2705(b):

- **20 Mag. 12614:** Served November 24, 2020, this grand jury subpoena seeks basic subscriber information associated with the account j[redacted][at]projectveritas.com. The accompanying secrecy order prohibits Microsoft from disclosing the existence of the subpoena for one year, expiring November 23, 2021. *See* Garland Decl. Ex. A.

- **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. The order includes a one-year secrecy provision, expiring November 24, 2021. *See* Garland Decl. Ex. B.

- **21 Mag. 548:** Served January 15, 2021, this search warrant demands email content and other information associated with the same account at issue in 20 Mag. 12614 and 20 Mag. 12623 (but with the domain name misspelled as "j[redacted][at]projectvertias.com"), e[redacted][at]projectveritas.com, and s[redacted][at]projectveritas.com. The warrant contains a one-year secrecy provision, expiring January 14, 2022. *See* Garland Decl. Ex. C.

- **21 Mag. 992:** Served January 26, 2021, this search warrant demands email content and other information associated with [redacted][at]projectveritas.com. It contains a one-year secrecy provision, expiring January 26, 2022. *See* Garland Decl. Ex. D.

- **21 Mag. 2537:** Served March 5, 2021, this search warrant demands email content and other information associated with c[redacted][at]projectveritas.com, n[redacted][at]projectveritas.com, and s[redacted][at]projectveritas.com. It contains a one-year secrecy provision, expiring March 5, 2022. *See* Garland Decl. Ex. E.

- **21 Mag. 2711:** Served March 10, 2021, this this order, issued under 18 U.S.C. § 2703(d), requires Microsoft to produce information associated with e[redacted][at]projectveritas.com. It

[2] *See* Mot. to Appoint Special Master at 1 ("Special Master Mot."), *In re Search Warrant dated Nov. 5, 2021*, No. 21 Misc. 813 (AT) (S.D.N.Y. Nov. 15, 2021), ECF No. 10; Reply in Support of Mot. to Appoint a Special Master at 2-6, *In re Search Warrant dated Nov. 5, 2021*, No. 20 Mag. 10685 (AT) (S.D.N.Y. Nov. 22, 2021), ECF No. 38; *Project Veritas Action Fund v. Rollins*, 982 F.3d 813, 817 (1st Cir. 2020); *see also Overview*, Project Veritas, https://www.projectveritas.com/about/ (last visited Feb. 11, 2022).

includes a one-year secrecy provision, expiring March 9, 2022. *See* Garland Decl. Ex. F.

- **21 Mag. 3884:** Served April 9, 2021, this search warrant demands email content and other information associated with j[redacted][at]projectveritas.com. It contains a one-year secrecy provision, expiring April 9, 2022. *See* Garland Decl. Ex. G.

Three search warrants state that the seized information would be reviewed for evidence of crimes related to the transportation and possession of stolen goods, including the stolen property of Ashley Biden, daughter of President Biden.[3] *See* Garland Decl. Exs. C-E.

Consistent with its policies, *see supra* Part II.A, Microsoft responded to each request by asking the Government to redirect its legal process to Project Veritas. Garland Decl. ¶ 5. When the Government refused, Microsoft produced the requested information. *Id*. At the time, the Government's investigation was not public.

F. The Investigation Receives Wide Publicity.

On November 4 and 6, 2021, seven months after the Government's last demand to Microsoft, the FBI executed search warrants on the homes of two former Project Veritas employees, Eric Cochran and Spencer Meads, and that of Project Veritas's founder James O'Keefe. *See* Government's Mem. of Law in Opp'n to Mot. for Appointment of a Special Master ("Opposition to Special Master Mot.") at 2, *In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mc-00813-AT (S.D.N.Y. Dec. 8, 2021), ECF No. 29. During the searches, the Government seized cell phones, laptops, thumb drives, and other electronic storage devices. *In re Search Warrant*, No. 21 Misc. 825 (S.D.N.Y. Nov. 18, 2021), ECF No. 8 at 4-5; *In re Search Warrant*, No. 21 Misc. 819 (S.D.N.Y. Nov. 17, 2021), ECF No. 8 at 2. Like the warrants directed to Microsoft, these warrants state that the Government would review seized items for evidence of crimes related to the transportation and possession of stolen property, including

[3] The fourth warrant served on Microsoft appears to be missing two pages, and (at least as served on Microsoft) does not disclose details regarding the nature of the Government's investigation. *See* Garland Decl. Ex. G.

property belonging to Ashley Biden. *See In re Search Warrant*, No. 21 Misc. 825 (S.D.N.Y. Nov. 18, 2021), ECF No. 8-1; *In re Search Warrant*, No. 21 Misc. 819 (S.D.N.Y. Nov. 17, 2021), ECF No. 8-1; Special Master Mot. at 58 (Ex. F). The O'Keefe warrant names ten potential co-conspirators.[4]

The New York Times, Washington Post, and other major news outlets reported on the home searches, stating that the Government was investigating Project Veritas and O'Keefe for their alleged involvement in the theft of a diary belonging to Ashley Biden.[5] O'Keefe also publicly announced that Project Veritas had received a grand jury subpoena, and "acknowledged that Project Veritas had been involved in discussions with sources about the diary." Schmidt 11/5. A month later, the New York Times published a front-page story elaborating on the investigation, mentioning several people named in the warrants.[6]

G. Project Veritas's Motion for a Special Master

On November 6, 2021—the day the FBI executed a warrant on O'Keefe's home—counsel for Project Veritas and O'Keefe wrote to the Government, raising the concern that

[4] The potential co-conspirators are Jennifer Kiyak, Tyler Moore, Elaine Ber, Anthony Wray, Jackson Voynick, Leon Sculti, Robert Kurlander, Aimee Harris, Stephanie Walczak, and Elizabeth Fago. Special Master Mot. at 58 (Ex. F). The Cochran and Meads warrants also list potential co-conspirators, but publicly filed copies of those warrants redacted the names of those individuals. *See In re Search Warrant*, No. 21 Misc. 825 (S.D.N.Y. Nov. 18, 2021), ECF No. 8-1; *In re Search Warrant*, No. 21 Misc. 819 (S.D.N.Y. Nov. 17, 2021), ECF No. 8-1.

[5] *See, e.g.*, Michael S. Schmidt et al., *People Tied to Project Veritas Scrutinized in Theft of Diary From Biden's Daughter*, N.Y. Times (Nov. 5, 2021) ("Schmidt 11/5"), https://www nytimes.com/2021/11/05/us/politics/project-veritas-investigation-ashley-biden-diary html; Amy B. Wang & Devlin Barrett, *FBI searches Project Veritas associates*, Wash. Post (Nov. 5, 2021), https://www.washingtonpost.com/politics/2021/11/05/fbi-searches-project-veritas-associates-probe-over-diary-purportedly-belonging-bidens-daughter/; Michael S. Schmidt et al., *F.B.I. Searches James O'Keefe's Home in Ashely Biden Diary Theft Inquiry*, N.Y. Times (Nov. 6, 2021), https://www.nytimes.com/2021/11/06/us/politics/james-okeefe-project-veritas-ashley-biden.html.

[6] *See* Adam Goldman and Michael S. Schmidt, *How Ashley Biden's Diary Made Its Way to Project Veritas*, N.Y. Times, Dec. 17, 2021 at A1, https://www.nytimes.com/2021/12/16/us/politics/ashley-biden-project-veritas-diary.html?searchResultPosition=4; *see also* Adam Goldman and Michael S. Schmidt, *Project Veritas Tells Judge It Was Assured Biden Diary Was Legally Obtained*, N.Y. Times, Nov. 13, 2021 at A16, https://www.nytimes.com/2021/11/12/us/politics/project-veritas-ashley-biden-diary.html?action=click&module=RelatedLinks&pgtype=Article.

O'Keefe's seized cell phones contain materials protected by the First Amendment and attorney-client privilege, and requesting that the Government sequester the seized phones, including from any DOJ filter team. Special Master Mot., Ex. A; *see also id.* Ex. B (Government's November 7 letter response). On November 10, 2021, Project Veritas and O'Keefe (later joined by Cochran and Meads) moved before Judge Analisa Torres for the appointment of a special master to review the electronic devices the Government had seized. They argued that the Government's review of these materials implicated the First Amendment (in part because of Project Veritas's journalistic activities) and certain other privileges and protections. *See* Order, *In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mc-00813-AT (S.D.N.Y. Nov. 12, 2021), ECF No. 2.[7]

On November 15, 2021, the Court publicly docketed the motion and related filings. Those filings confirm that key aspects of the Government's investigation are known to Project Veritas (and to the public), including, *inter alia*, the crimes under investigation, the connection to Ashley Biden's stolen property, and the identities of at least ten potential co-conspirators. *See, e.g.*, Special Master Mot. at 58 (Ex. F). Moreover, in its opposition to the motion, the Government acknowledged that "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." Opposition to Special Master Mot. at 20.[8]

On December 8, 2021, Judge Torres granted the motion and appointed the Honorable Barbara D. Jones (ret.) as special master. Order Appointing Special Master at 3. The Court's

[7] *See also* Special Master Mot.; Mot. to Appoint Special Master, *In Re: Search Warrant dated Nov. 3, 2021*, No. 1:21-mc-00819-AT (S.D.N.Y. Nov. 17, 2021), ECF No. 8; Letter re: Appointment of Special Master, *In re: Search Warrant dated Nov. 3, 2021*, No. 1:21-mc-00825-AT (S.D.N.Y. Nov. 18, 2021), ECF No. 8.

[8] On November 21, 2021, the Reporter's Committee for the Freedom of the Press ("RCFP") intervened to seek public disclosure of detailed affidavits containing evidence to support probable cause of unlawful conduct, citing the public nature of the investigation. Magistrate Judge Cave denied the request. RCFP's objections to the opinion are pending before Judge Torres. *See* Objections of the RCFP, *In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mj-10685-AT (S.D.N.Y. Dec. 20, 2021), ECF No. 49.

ruling cited "the potential First Amendment concerns that may be implicated by the review of the [seized] materials," and explained that "the appointment of a special master will help[] to protect the public's confidence in the administration of justice." *Id.* (quotation omitted).

H. The Government Obtains Renewed Secrecy Orders

Although Project Veritas was aware of the Government's investigation no later than November 4, 2021—and immediately objected to the Government's search and seizure of its information—the Government, between November 19, 2021, and January 13, 2022, sought and obtained renewed NDOs for four of the demands directed to Microsoft:[9]

- **20 Mag. 12614:** On November 19, 2021, the Government obtained a renewed NDO for the subpoena seeking data for j[redacted][at]projectveritas.com. The Government sought a year-long NDO, but Magistrate Judge Wang granted only a 180-day NDO. *See* Garland Decl. Ex. H.

- **20 Mag. 12623:** On November 29, 2021, the Government obtained a one-year renewal of the NDO for the D Order seeking data on the same account. *See* Garland Decl. Ex. I.

- **21 Mag. 548:** On January 11, 2022, the Government obtained a one-year renewal of the NDO for the warrant seeking data on j[redacted][at]projectvertias.com, eric[at]projectveritas.com, and spencer[at]projectveritas.com. *See* Garland Decl. Ex. J.

- **21 Mag. 992:** On January 13, 2022, the Government obtained a one-year renewal of the NDO for the warrant seeking data on l[redacted][at]projectveritas.com. *See* Garland Decl. Ex. K.

The foregoing renewals were all obtained from Magistrate Judges, not Judge Torres. Microsoft does not know whether the Government has informed Judge Torres about the existence of the legal process issued to Microsoft, or about the NDO renewals obtained during the pendency of the Special Master proceedings.

I. Microsoft Seeks Modification of the Secrecy Orders

Microsoft has asked the Government to vacate the secrecy orders, which would allow

[9] The NDOs accompanying the other three demands Microsoft received—bearing case nos. 21 Mag. 2537, 21 Mag. 2711, and 21 Mag. 3884—have not yet expired. *See supra* Part II.B.

Microsoft to notify an appropriate individual at its customer about the demands. Garland Decl. ¶ 10-11. Microsoft explained that the Government cannot prove a compelling interest in secrecy in this case, given the public nature of the investigation. Microsoft further explained that notification is particularly appropriate given Judge Torres's recognition that the Government's search of Project Veritas's electronic devices potentially implicates the First Amendment and reporter's privilege. The Government has refused Microsoft's requests. *Id.*

III. ARGUMENT

As prior restraints and content-based restrictions on speech, the secrecy orders here are "presumptively unconstitutional" and may be sustained "only if the Government proves that [they are] narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2226 (2015). The Government cannot make such a showing given the public disclosure of the investigation, the media coverage of the Government's activities, and the public identification of ten potential co-conspirators, who appear to substantially overlap with the individuals targeted in the demands to Microsoft. The Court should vacate the orders. But even if the secrecy orders were otherwise justifiable, Microsoft has proposed a less restrictive alternative to an outright ban on its speech: notification of an appropriate individual at Project Veritas who already knows about the Government's investigation. Because the Government has not met its heavy burden of establishing that this alternative would fail to protect its interests, the Court should at least modify the secrecy orders to allow this alternative.

A. The Secrecy Orders Are Subject to Strict Scrutiny under the First Amendment.

1. The secrecy orders are prior restraints on speech and content-based speech restrictions, and presumptively unconstitutional.

As courts have "almost uniformly" concluded, *In re Search Warrant for [Redacted].com*, 248 F. Supp. 3d 970, 980 (C.D. Cal. 2017), "nondisclosure orders pursuant to Section 2705(b)—

like the one here—are content-based prior restraints on speech, and subject to strict scrutiny," *In re Search of Info. Associated with E-mail Accts.*, No. 1:18-MJ-723 (AMD), 2020 WL 5627261, at *3 (E.D.N.Y. May 22, 2020).

First, the secrecy orders are prior restraints. A prior restraint "forbid[s] certain communications when issued in advance of the time that such communications are to occur." *Alexander v. United States*, 509 U.S. 544, 550 (1993) (emphasis and quotations omitted). Here, the secrecy orders prohibit Microsoft from disclosing the existence of the process and orders to Project Veritas or any other person. This restriction is a presumptively invalid prior restraint, as it "suppresses speech . . . on the basis of the speech's content and in advance of its actual expression." *United States v. Quattrone*, 402 F.3d 304, 309 (2d Cir. 2005); *see also Microsoft*, 233 F. Supp. 3d at 906 (orders under Section 2705(b) are prior restraints). "[S]uch restraints constitute the most serious and the least tolerable infringement on our freedoms of speech and press." *Quattrone*, 402 F.3d at 309 (quotations omitted). Any prior restraint bears "a heavy presumption against its constitutional validity," and the Government "carries a heavy burden of showing justification for the imposition of such a restraint." *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 558 (1976) (quotations omitted).

Second, the secrecy orders are content-based restrictions on Microsoft's speech. "Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed." *Reed*, 576 U.S. at 163. By singling out speech about the legal process served on Microsoft, the orders "target speech based on its communicative content" and restrict speech based on its "function or purpose." *Id.* This content-based restriction is "presumptively unconstitutional." *Id.* "It is rare that a regulation restricting speech because of its content will ever be permissible." *Playboy*, 529 U.S. at 818.

2. The secrecy orders are subject to strict scrutiny.

Because the secrecy orders are both a prior restraint and content-based restriction, strict scrutiny applies. 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." *Playboy*, 529 U.S. at 813 (emphasis added). The Government must prove it has narrowly tailored the restraint to promote a compelling government interest while treading as lightly as possible on the right to speak. *Id.* at 814. 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).

The perceived value of the speech restrained has no relevance to the strict scrutiny analysis. *See United States v. Stevens*, 559 U.S. 460, 470 (2010). Here, there is no question about the First Amendment value of Microsoft's interest in notifying its customer about the Government's demand for the customer's private information. Secrecy orders such as this one chill the free discussion of public affairs—i.e., the exercise of the Government's (surreptitious) investigative powers. 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 h[ie]rarchy 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). More fundamentally, Project Veritas has the right to know—just as it would in the pre-cloud era—that the Government has

seized its data so that it can communicate directly with the Government and the Court about the demands and ensure that the Government investigation takes its rights and interests into account.

3. This case presents unique circumstances that heighten the Government's First Amendment burden.

The Government bears an even greater burden here because the Court has recognized "the potential First Amendment concerns that may be implicated by the review of the [seized] materials." Order Appointing Special Master at 3. The Government has demanded information belonging to an entity that describes itself as a "non-profit journalism enterprise," Special Master Motion at 6-14; Project Veritas Homepage, https://www.projectveritas.com/about/, which is "primarily engaged in undercover journalism." *Project Veritas Action Fund v. Conley*, 270 F. Supp. 3d 337, 339 (D. Mass. 2017).

Project Veritas has argued that the electronic materials the Government seized in its physical searches "contain vast amounts of information protected by the First Amendment, including materials related to on-going news investigations, whistleblower information, and donor information that implicates freedom of speech and association guarantees." Special Master Mot. at 1. Project Veritas has further asserted that these materials "contain a vast amount of attorney-client privileged material" relating to the Government's investigation and "many unrelated matters." *Id.* The information on Microsoft's servers is likely substantially similar—if not identical—to information on the devices the Government seized, and likely implicates the same First Amendment, journalistic, and attorney-client privilege concerns. And to the extent the information seized from Microsoft *does* overlap with the information now before the Special Master, allowing the Government to retain that information free from scrutiny will undermine the efficacy of the Court's Order providing for the Special Master's review.

Accordingly, unlike a case involving the mere *possibility* that a customer would assert

privilege and protections over its data, here, Project Veritas has clearly asserted that these protections apply. And the Government has acknowledged that Project Veritas might qualify for protection under the DOJ's news media procedures. *See* Special Master Mot., Ex. B (Government's assertion of compliance "with all applicable regulations and policies regarding potential members of the news media in the course of this investigation"). Without notice of the Government's legal demands to Microsoft, however, Project Veritas cannot assert privileges as to the materials Microsoft provided in response to those demands, and the Special Master cannot review them. Nor can Microsoft: as a steward of its customer's data, Microsoft does not review the content, and even if it did, it could not assess (or assert) its customer's potential privileges.

Again, Judge Torres has already *recognized* that the Government's search and seizure of Project Veritas's data may implicate "potential First Amendment concerns." Order Appointing Special Master at 2. These same concerns apply equally to the information the Government demanded from Microsoft.

B. The Secrecy Orders Fail to Serve a Compelling Interest.

Strict scrutiny requires the Government to demonstrate a compelling interest that the restriction "will in fact alleviate . . . in a direct and material way." *Turner Broad.*, 512 U.S. at 664. Because the Government cannot meet that test, the Court should vacate the secrecy orders.

The Government's justification for suppressing Microsoft's speech turns on the supposed fear that, if Project Veritas and its associates knew about the investigation, evidence might disappear, witnesses might flee, or the investigation might otherwise be jeopardized. But that fear makes no sense here. Months ago, the Government served Project Veritas with a grand jury subpoena and executed physical search warrants on the homes of Project Veritas's founder and two former employees, seizing cell phones, laptops, thumb drives, and other electronic storage devices. Special Master Mot. at 2-4 & Exs. E-F; *In re Search Warrant dated Nov. 3, 2021*, No.

1:21-mc-00819-AT, Dkt. 8 at 2 (S.D.N.Y. Nov. 17, 2021); *In re Search Warrant dated Nov. 3, 2021*, No. 1:21-mc-00819-AT, Dkt. 8 at 4-5 (S.D.N.Y. Nov. 18, 2021). The search warrants—now filed on the public docket—authorized the Government to review substantial amounts of ESI on the devices. *See, e.g.*, Special Master Mot. at 35-37 (Ex. F). And the publicly available warrants identify ten individuals as "potential co-conspirators." *In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mc-00813-AT (S.D.N.Y. Nov. 15, 2021), ECF No. 10-6 at 5. Through this process, it appears the Government has *publicly identified* at least seven (and possibly all) of the nine individuals targeted in the demands issued to Microsoft.[10] And anyone who did *not* learn of the investigation from the Government's pre-dawn searches (and the accompanying warrants) would have read about it in the news, which reported on both the grand jury subpoena and the searches, and identified individuals the Government named as potential co-conspirators. *See supra* Part II.F.

The investigation's public nature defeats any claim that disclosure of these various demands to Microsoft's client would actually risk the Government's purported harms—and thus defeats the claim of a compelling government interest. "[O]ne cannot 'disclose' what is already in the public domain." *Bartnicki v. Vopper*, 532 U.S. 514, 546 (2001); *see also Wash. Post v. Robinson*, 935 F.2d 282, 291-92 (D.C. Cir. 1991) (similar). The Government's searches of three

[10] The Government executed physical search warrants on the homes of James O'Keefe, Eric Cochran, and Spencer Meads—presumably the accountholders of j[redacted][at]projectveritas.com, e[redacted][at]projectveritas.com, and s[redacted][at]projectveritas.com, respectively. Three of the "potential co-conspirators" identified in the warrants, i.e., Jennifer Kiyak, Elaine Ber, and Leon Sculti, are likely the accountholders of j[redacted][at]projectveritas.com, e[redacted][at]projectveritas.com, and l[redacted][at]projectveritas.com. *See In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mc-00813-AT (S.D.N.Y. Nov. 15, 2021), Dkt. 10-6 at 5. And it has been widely reported that another named "potential co-conspirator[]"—Jackson Voynick—uses the moniker "S[redacted]," which corresponds to another targeted account, s[redacted][at]projectveritas.com. *See* Will Sommer, *Proud Boy Named in Feds' James O'Keefe Search Warrant*, The Daily Beast (Dec. 28, 2021), https://www.thedailybeast.com/proud-boy-named-in-department-of-justices-james-okeefe-search-warrant. The remaining two targeted accounts—r[redacted][at]projectveritas.com and c[redacted][at]projectveritas.com—plausibly correspond to the other two potential co-conspirators identified in the physical search warrants.

targets' homes pursuant to a publicly disclosed warrant identifying ten potential co-conspirators have, by this time, been highly publicized in the press and actively litigated in the public domain. If anyone connected with the events at issue were likely to flee, tamper with evidence, threaten a witness, or otherwise jeopardize the Government's investigation, they already have had ample time (and incentive) to do so. Indeed, by now common sense would have led Project Veritas and its associates to suspect, if not assume, the Government has sought its email and other records by going not only to the homes of Project Veritas's founder and former employees, but also to the organization's cloud service provider.

In these circumstances, the secrecy orders serve no legitimate government purpose, much less a compelling one. Indeed, the Government has previously agreed to withdraw a non-disclosure order associated with a public investigation, for the same reasons. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 19 Misc. 682 (D. Md.). Here, the orders do nothing more than nullify Project Veritas's right to interpose objections with respect to the information already seized, and abrogate Microsoft's ability to engage in protected speech.

Vacating the secrecy orders implicates none of the concerns Magistrate Judge Cave identified in declining to unseal materials related to the search warrant for Mr. O'Keefe's devices—a decision now on appeal to Judge Torres. *See In re Search Warrant dated Nov. 5, 2021*, 2021 WL 5830728, at *5-8 (S.D.N.Y. Dec. 7, 2021). Judge Cave found that unsealing those materials would jeopardize the investigation's integrity because they contained information about the full range of potential criminal violations being investigated, evidence the Government obtained before the searches, and individuals who had already provided information to the Government. *Id.* at *6. Judge Cave also found that the privacy interests of third parties

identified in the materials—including confidential informants, cooperating witnesses, and the President's daughter—weighed heavily against disclosure. *Id.* at *7-8. But here, Microsoft does not seek to disclose the information that raised concerns for Judge Cave; indeed, Microsoft lacks access to that information. Microsoft asks only for relief from the restraints that prevent it from telling its customer that the Government has demanded information that Project Veritas stored with Microsoft. Disclosure would do nothing more than confirm to Project Veritas (and its counsel) what everyone likely assumes, i.e., that the Government has demanded information Project Veritas stored on Microsoft's servers, just as it has seized information Project Veritas employees kept in their homes. Knowing this, Project Veritas would have the opportunity to protect its interests in this Court, just as it is doing in connection with the November warrants.

C. The Government Cannot Show that the Secrecy Orders Are Narrowly Tailored.

Even if the Government could demonstrate a compelling interest justifying some restraint on Microsoft's speech, it has failed to show the ineffectiveness of alternatives less restrictive than the existing bans.

1. Microsoft has proposed a plausible less restrictive alternative.

Microsoft has proposed a less restrictive alternative to the secrecy orders' complete speech restriction: notifying an appropriate individual at Project Veritas of the Government's demands to Microsoft, but otherwise maintaining the demands' confidentiality. This limited notification would relax the ban on Microsoft's speech and enable Project Veritas to protect its interests through counsel. Microsoft will work with the Government to identify a "trustworthy candidate" for notice. DOJ Recommended Practices at 2.

There is no reason to assume that the person notified would resort to unlawful means. To the contrary, Project Veritas has asserted its rights before Judge Torres on issues related to the warrants for the November 2021 raids through lawful means. In those proceedings, Project

Veritas's counsel have successfully advanced arguments to protect Project Veritas's interests.[11] *See generally In re Search Warrant dated Nov. 5, 2021*, No. 1:21-mc-00813-AT (S.D.N.Y.). On these facts, the Government cannot plausibly identify any reason to believe notice of the demands to a responsible individual at Project Veritas would lead to extra-judicial action jeopardizing the investigation—especially given the widespread publicity already surrounding the Government's inquiry and the ongoing proceedings before Judge Torres.

2. The Government cannot prove that Microsoft's less restrictive alternative will be ineffective.

Once Microsoft proposed a plausible less restrictive alternative to the secrecy orders' ban on speech, the burden shifted to the Government to "prove that the alternative will be ineffective to achieve its goals." *Playboy*, 529 U.S. at 816; *see also Boos v. Barry*, 485 U.S. 312, 329 (1988) (if "less restrictive alternative is readily available," restraint "is not narrowly tailored"). No information available to Microsoft suggests the Government can meet its burden.

As discussed, the Government has provided no reason to believe that allowing Microsoft to notify its customer of these demands would lead Project Veritas to improperly interfere with the investigation—particularly given that Project Veritas is engaging with the Court concerning the materials seized in the November searches. And the Government cannot justify banning Microsoft's speech based on speculation that a notified individual *might* do so. "Mere conjecture" about the harms of disclosure is inadequate "to carry a First Amendment burden."

[11] Project Veritas has hired experienced counsel. Lead counsel Paul Calli has been a member of the Florida Bar for nearly three decades and has served as Chair of the Florida Bar Grievance Committee for Miami-Dade County. *See* https://www.floridabar.org/directories/find-mbr/profile/?num=994121; https://calli-law.com/paul-a-calli-appointed-chair-of-florida-bar-grievance-committee/. Benjamin Barr has been a member of the Illinois Bar for over two decades, http://iardc.org/Lawyer/PrintableDetails/85c18c15-aa64-eb11-b810-000d3a9f4eeb, and Stephen Klein is a member of the District of Columbia, Michigan, and Illinois Bars. *See* https://barrklein.com/attorney-profiles/. Both Barr and Klein are members of the U.S. Supreme Court Bar and have been admitted to practice in numerous U.S. Courts of Appeal. *Id.* Microsoft can find no indication that Project Veritas's counsel have been subjected to bar discipline or judicial sanctions, and all are currently before the Court and subject to its authority.

Nixon v. Shrink Missouri Gov. PAC, 528 U.S. 377, 379 (2000). The Government "must specifically identify an 'actual problem' in need of solving," *Brown v. Entm't Merchants Ass'n*, 564 U.S. 786, 799 (2011) (quoting *Playboy*, 529 U.S. at 822), and offer "proof" that the proposed less restrictive alternative is unworkable, *Playboy*, 529 U.S. at 822 ("anecdote and supposition" are not enough).

Even if the notification Microsoft proposes would be incrementally riskier than a complete ban on Microsoft's speech, that "marginal degree of protection" does not justify rejecting Microsoft's proposal. *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983) (striking down law prohibiting unsolicited mail about contraceptives as "a restriction of this scope is more extensive than the Constitution permits"). Where "a less restrictive means is available for the Government to achieve its goals, the Government *must* use it." *Playboy*, 529 U.S. at 815 (emphasis added). The law does not require a less restrictive alternative to be a "perfect solution," *Ashcroft v. ACLU*, 542 U.S. 656, 668 (2004); if it did, speech bans would always be constitutional (because a complete suppression of speech always provides the Government greater protection than any alternative). The Government therefore cannot reject a less restrictive alternative here simply because it does not offer a complete assurance of secrecy.

Nor can the Government reject Microsoft's proposed alternative on the ground that blanket secrecy orders are more efficient. It is bedrock law that "the First Amendment does not permit the State to sacrifice speech for efficiency." *Riley v. Natl. Fedn. of the Blind of N. Carolina, Inc.*, 487 U.S. 781, 795 (1988); *see also Natl. Inst. of Fam. and Life Advocates v. Becerra*, 138 S. Ct. 2361, 2376 (2018). Further, requiring the Government to work with Microsoft to identify an appropriate individual to notify is consistent with DOJ's own guidance, as well as the Government's investigative approach in the pre-cloud era. *See* DOJ

Recommended Practices at 2 ("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."). Before cloud computing, the Government needed to (and did) routinely obtain enterprise documents directly from target companies—including in investigations where the company itself might be liable. *See id.* at 1. It would run counter to the First Amendment if the Government were now permitted to capitalize on administrative *efficiencies* made possible by new technologies to obtain information directly from cloud providers, while simultaneously invoking the administrative *burdens* of finding an appropriate individual to notify to justify a ban on the providers' speech.

3. The Government cannot carry its burden by relying on *ex parte* evidence to which Microsoft does not have access.

The Government may attempt to justify its suppression of Microsoft's speech by relying on its *ex parte* application for the secrecy orders. The Court cannot rely on this evidence—which Microsoft has never seen—in assessing the First Amendment issues. "It 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." *Abourezk v. Reagan*, 785 F.2d 1043, 1060–61 (D.C. Cir. 1986), *aff'd*, 484 U.S. 1 (1987). "[D]ue process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other." *Abuhamra*, 389 F.3d at 322.

This rule against *ex parte* evidence means the government ordinarily "must either apprise the defendant of the substance of its sealed submission or forego the court's consideration of the evidence." *Id.* at 331; *see also Abourezk*, 785 F.2d at 1061 (either "the other side must be given access to the [classified] information," or "the court may not rely upon [it]"). And even in the "rare circumstances" where reliance on *ex parte* information is appropriate, the government must provide a "substitute disclosure" explaining the "gist or substance of the government's [entire]

ex parte submission." *Abuhamra*, 389 F.3d at 322, 329; *see also, e.g.*, *Cabral v. Strada*, 513 F. App'x 99, 102-03 (2d Cir. 2013) (consideration of ex parte evidence permissible because government "disclos[ed] the substance of the evidence" to pre-trial detainees).[12]

Microsoft therefore must be given access to any evidence on which the Government asks the Court to rely. The robust strict scrutiny analysis—which requires the Government to provide "specific evidence" supporting its position, *Playboy*, 529 U.S. at 819—cannot function unless the parties can test that evidence through the adversarial process. *See, e.g.*, *Freedman v. State of Md.*, 380 U.S. 51, 58 (1965) ("only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression."). Microsoft's attorneys would be willing to sign a protective order to limit disclosure of any *ex parte* information. At a minimum, Microsoft is entitled to a redacted version or summary of any submission on which the Government relies.

IV. CONCLUSION

The Court should vacate the secrecy orders, or at a minimum modify them to allow Microsoft to notify an appropriate individual at Project Veritas about the demands.

Dated: February ____, 2022

[12] Statutes that contemplate consideration of *ex parte* evidence typically provide for some substitute disclosure of the substance of the material. For example, the Classified Information Procedures Act ("CIPA"), the law governing the use of classified information in criminal proceedings, contemplates the provision of summaries or substitute submissions. *See* 18 U.S.C. app. 3 § 4; *see also Abuhamra*, 389 F.3d at 331 (discussing CIPA). Similarly, the law that governs terrorism-related removal proceedings requires the government to provide unclassified summaries of any classified information on which it relies. *See* 8 U.S.C. § 1534(e)(3).