

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

v.

**CONCORD CONSULTING AND
MANAGEMENT, LLC,**

Defendant

Crim. No. 18-cr-32-2 (DLF)

**GOVERNMENT’S MOTION FOR A PROTECTIVE ORDER
UNDER FEDERAL RULE OF CRIMINAL PROCEDURE 16(d)(1)**

The United States of America, by and through Special Counsel Robert S. Mueller, III, submits this motion for a protective order pursuant to Federal Rule of Criminal Procedure 16(d)(1) and 18 U.S.C. § 3771(a)(8).

BACKGROUND

On February 16, 2018, a federal grand jury returned an eight-count indictment against sixteen defendants, arising out of their efforts to interfere with the U.S. political process, including the 2016 presidential election. (ECF No. 1). Count One of the indictment charges all defendants, including defendant Concord Management and Consulting LLC (“Concord Management”), with conspiring to defraud the United States. The indictment charges that in order to carry out their activities to interfere in the U.S. political and electoral processes without detection of their Russian affiliation, the defendants conspired to obstruct the lawful functions of the United States government through fraud and deceit.

The government anticipates that voluminous discovery will be involved in this case. As described in previous filings, the government estimates that it currently possesses documentary evidence related to the investigation that totals somewhere between 1.5 and 2 terabytes of data.

The evidence includes data related to hundreds of social media accounts, as well as evidence obtained from email providers, internet service providers, financial institutions, and other sources. Additionally, the need to produce much of the data in its original format (formats that include, for example, Excel and HTML files) makes it infeasible to make certain redactions without compromising expeditious review of the data. The evidence in this case will also include numerous reports and affidavits filed in connection with this investigation that describe investigative steps, identify uncharged co-conspirators, and disclose various law enforcement and intelligence collection techniques.

On May 17, 2018, the government and defense counsel met and conferred to discuss the discovery, as well as the considerations that warrant a protective order. On May 25, 2018, the government sent defense counsel a proposed protective order that reflected the considerations discussed by the parties. On June 1, 2018, defense counsel sent the government proposed revisions and comments to the draft. After the parties conferred telephonically on June 4, 2018, the government sent defense counsel a revised protective order on June 6, 2018 to address their concerns. On June 7, 2018, defense counsel informed the government it would not agree to the revised protective order.

The government and defense counsel have agreed on many procedures designed to enable the government to turn over discovery expeditiously and without redactions while protecting information that affects government interests involved in this case, as well as privacy interests of victims and uncharged third parties. Defense counsel also agrees that discovery is only to be used for the defense of the case. The parties also agree to limit review of discovery to authorized parties (but disagree on who should be permitted to be designated an authorized party). Defense counsel also agrees that for certain discovery designated as sensitive, defense counsel will maintain

discovery at their U.S. offices and agrees not to physically or electronically transport any such materials outside the United States.

The government and Concord Management, however, have not been able to reach agreement on two key provisions. First, due to the number of co-defendants who have chosen not to appear in the United States and are beyond the reach of U.S. legal process, the government seeks, in the first instance, not to allow any co-defendant charged in this criminal case to review discovery until the co-defendant appears before this Court. (Proposed Order, ¶ 2). The proposed protective order provides that if defense counsel, after reviewing discovery in this matter, believes it necessary to seek to disclose or discuss any material with a co-defendant who has not appeared before this Court, counsel must first seek permission from this Court and a modification of this Order. (Proposed Order, ¶ 2).

Second, to avoid unnecessarily undermining ongoing law enforcement and national security investigations, the proposed protective order outlines a mechanism to regulate disclosure of particularly sensitive material to foreign nationals. Disclosure of sensitive discovery would initially be limited to domestic defense counsel. (Proposed Order, ¶ 11). After review of the materials, defense counsel could seek permission from the Court to make additional disclosures (subject to the other provisions in the protective order). (Proposed Order, ¶ 11). For any foreign national to whom defense counsel wishes to disclose sensitive materials, defense counsel would provide a firewall counsel for the government (separate from the prosecution team) with the name of any such individual contemporaneous to its request for Court approval.¹ If needed, firewall

¹ If approved, the government would identify Firewall Counsel to counsel and the Court.

counsel would alert the Court to any concerns or considerations about such disclosures.² (Proposed Order, ¶ 11).

ARGUMENT

A. District Courts Have Significant Discretion to Enter Protective Orders Governing Discovery

Federal Rule of Criminal Procedure 16(d)(1) provides that “[a]t any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief.” Fed. R. Crim. P. 16(d)(1). The advisory committee further clarified that “[a]mong the considerations to be taken into account by the court will be the safety of witnesses and others, a particular danger or perjury or witness intimidation, the protection of information vital to the national security, and the protection of business enterprises from economic reprisals.” Fed. R. Crim. P. 16 advisory committee’s note (1966 amendment). The government may also establish “good cause by a written statement that the court will inspect ex parte,” Fed. R. Crim. P. 16(d)(1), which the advisory committee recognized would be most appropriate “where matters of national security are involved.” Fed. R. Crim. P. 16 advisory committee’s note (1966 amendment).

In *United States v. Alderman*, 394 U.S. 165 (1969), the Supreme Court directed that “the trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect.” *Id.* at 185. The entry of a protective order is a common and valid exercise of the Court’s discretion under Rule 16(d)(1). See, e.g., *United States v. O’Keefe*, No. 06-cr-0249 (PLF), 2007 WL 1239204, at *2 (D.D.C. Apr. 27, 2007) (“Protective orders in criminal cases are not uncommon, and the Federal Rules of Criminal Procedure provide that ‘[a]t any time the court may, for good cause,

² This approach was adopted from the approach in *United States v. Loera*, No. 1:09-cr-466 (E.D.N.Y. Apr. 3, 2017) (D.E. 51).

deny, restrict, or defer discovery or inspection, or *grant other appropriate relief.*”) (quoting Fed. R. Crim. P. 16(d)) (court’s emphasis). This authority is commonly used to protect information related to national security investigations. *See, e.g., United States v. Lindh*, 198 F. Supp. 2d 739, 742 (E.D. Va. 2002) (“protective orders regarding unclassified, but sensitive material ‘vital to national security.’”); *United States v. Moussaoui*, No. 01-cr-455 (E.D. Va. Feb. 5, 2002) (ECF No. 64) (“Protective Order for Unclassified But Sensitive Material as to Zacarias Moussaoui”); *United States v. Bin Laden*, 58 F. Supp. 2d 113, 121 (S.D.N.Y. 1999) (similar)

Protective orders are also frequently entered pursuant to Rule 16(d)(1) to promote the timely, and expeditious production of voluminous discovery information while preventing inadvertent dissemination of the information. *See, e.g., United States v. Bundy*, No. 2:16-CR-046-GMN-PAL, 2016 WL 7030431, at *4 (D. Nev. Nov. 30, 2016) (“The current Protective Order will promote the timely, efficient, and expeditious production of voluminous discovery information while preventing inadvertent dissemination of the information.”). Where a case involves voluminous discovery, such that identification of all sensitive information is infeasible, courts recognize that protective orders may be entered to cover the entirety of discovery produced by the government to defendants. *See, e.g., United States v. Luchko*, No. CRIM. A. 06-319, 2006 WL 3060985, at *5 (E.D. Pa. Oct. 27, 2006) (noting an “umbrella” protective order appropriate “where an action is complex or involves large-scale discovery and, potentially, where there is a stronger showing of good cause”).

Separately, the Crime Victims’ Rights Act (“CVRA”) provides that crime victims have the right, *inter alia*, “to be treated with fairness and with respect for the victim’s dignity and privacy.” 18 U.S.C. § 3771(a)(8). Courts have referred to the victims’ rights under the CVRA in identifying “good cause” for the imposition of protective orders or otherwise regulating discovery pursuant to

Rule 16. *See, e.g., United States v. Patkar*, No. CR. 06-00250-JMS, 2008 WL 233062, at *4–6 (D. Haw. Jan. 28, 2008) (referring to CVRA in denying modification of protective order); *United States v. Robinson*, No. CR 08-10309-MLW, 2009 WL 137319, at *3 (D. Mass. Jan. 20, 2009) (referring to CVRA in denying motion for pretrial public disclosure of victim’s identity).

B. The Government’s Discovery Contains Information that Could Be Detrimental to National Security and Law Enforcement Interests if Released

As described further in the government’s *ex parte* affidavit, the discovery in this case contains unclassified but sensitive information that remains relevant to ongoing national security investigations and efforts to protect the integrity of future U.S. elections. At a high level, the sensitive-but-unclassified discovery in this case includes information describing the government’s investigative steps taken to identify foreign parties responsible for interfering in U.S. elections; the techniques used by foreign parties to mask their true identities while conducting operations online; the relationships of charged and uncharged parties to other uncharged foreign entities and governments; the government’s evidence-collection capabilities related to online conduct; and the identities of cooperating individuals and, or companies. Discovery in this case contains sensitive information about investigative techniques and cooperating witnesses that goes well beyond the information that will be disclosed at trial.

In *Snepp v. United States*, 444 U.S. 507 (1980), the Supreme Court recognized “publication of . . . material relating to intelligence activities can be detrimental to vital national interests even if the published information is unclassified.” *Id.* at 511–12; *see also Kaplan v. Conyers*, 733 F.3d 1148, 1157–58 (Fed. Cir. 2013) (“Courts have long recognized that sensitive but unclassified material can be vital to national security. . . [Disclosures of] unclassified information can have

detrimental effects on national security the same way as classified information.”).³ Publication of such information can be particularly detrimental in the hands of sophisticated foreign intelligence services. *See United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) (“[M]uch of the government's security interest in the conversation lies not so much in the contents of the conversations, as in the time, place, and nature of the government's ability to intercept the conversations at all. Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods.”).

Public or unauthorized disclosure of this case's discovery would result in the release of information that would assist foreign intelligence services, particularly those of the Russian Federation, and other foreign actors in future operations against the United States. First, the substance of the government's evidence identifies uncharged individuals and entities that the government believes are continuing to engage in interference operations like those charged in the present indictment. Second, information within this case's discovery identifies sources, methods, and techniques used to identify the foreign actors behind these interference operations, and

³ In *CIA v. Sims*, the Supreme Court gave an example of the probative value of unclassified information in the hands of a foreign intelligence service:

A foreign government can learn a great deal about the [Central Intelligence Agency's] activities by knowing the public sources of information that interest the Agency. The inquiries pursued by the Agency can often tell our adversaries something that is of value to them. For example, disclosure of the fact that the Agency subscribes to an obscure but publicly available Eastern European technical journal could thwart the Agency's efforts to exploit its value as a source of intelligence information.

471 U.S. 159, 176–77 (1985) (internal citation omitted).

disclosure of such information will allow foreign actors to learn of these techniques and adjust their conduct, thus undermining ongoing and future national security investigations.⁴ *See Lindh*, 198 F. Supp. 2d at 742 (“[G]iven the nature of al Qaeda and its activities, and the ongoing federal law enforcement investigation into al Qaeda . . . the questions asked and the techniques employed by law enforcement agents in the interviews are highly sensitive and confidential.”).

As described in its *ex parte* filing submitted pursuant to Rule 16(d)(1), the government has particularized concerns about discovery in this case being disclosed to Russian intelligence services.⁵ These heightened concerns inform the government’s proposed protective order. *See Lindh*, 198 F. Supp. 2d at 742 (noting protective order will “serve to prevent members of

⁴ The U.S. government has publicly identified multiple ongoing efforts to protect the integrity of future elections from unlawful foreign interference, including the Justice Department’s Cyber-Digital Task Force and the FBI’s Foreign Influence Task Force. *See* Memorandum of Attorney General Jeffrey B. Sessions, “Cyber-Digital Task Force,” Feb. 16, 2018, *available at* <https://www.justice.gov/opa/press-release/file/1035457/download>; Testimony of FBI Director Christopher Wray, House Homeland Security Committee, Nov. 30, 2017, *available at* <https://www.c-span.org/video/?437873-1/senior-homeland-security-officials-testify-global-terrorist-threats&start=3834> (describing efforts to investigate and interdict Russian interference campaigns in U.S. elections).

⁵ Additionally, Prigozhin and both charged Concord entities were sanctioned by the United States in 2016 pursuant to Executive Order 13,661, which authorizes sanctions based on “the actions and policies of the Government of the Russian Federation with respect to Ukraine—including the [] deployment of Russian Federation military forces in the Crimea region of Ukraine.” 79 Fed. Reg. 15,535 (Mar. 16, 2014). Concurrent with that designation, the Treasury Department explained that Prigozhin was being designated for “having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, senior officials of the Russian Federation,” including “extensive business dealings with the Russian Federation Ministry of Defense.” Press Release, “Treasury Sanctions Individuals and Entities In Connection with Russia’s Occupation of Crimea and the Conflict in Ukraine,” *available at* <https://www.treasury.gov/press-center/press-releases/Pages/jl0688.aspx>. On March 15, 2018, the Treasury Department designated Prigozhin and both Concord entities for another set of sanctions pursuant to Executive Order 13,694, which authorizes sanctions based on “malicious cyber-enabled activities.” 80 Fed. Reg. 18,077 (Apr. 1, 2015); *see also* Press Release, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks, *available at* <https://home.treasury.gov/news/press-releases/sm0312>.

international terrorist organizations . . . from learning, from publicly available sources, the status of, the methods used in, and the information obtained from the ongoing investigation of the detainees”).

C. The Government’s Discovery Contains Information that Could Be Damaging to Victims, Uncharged Parties, and Unwitting U.S. Persons if Released

Other considerations constitute good cause for the imposition of the government’s proposed protective order. The evidence in the government’s possession includes a significant amount of personal identifying information (“PII”) related to U.S. persons who were victims of identity theft (as alleged in the indictment, particularly in count two, and the related case of *United States v. Pinedo*, No. 1:18-cr-0024 (DLF)). Evidence related to these victims includes names, addresses, dates of birth, social security numbers, and other sensitive information, as well as the account numbers for bank accounts and other financial accounts opened in their names. This PII appears in hundreds if not thousands of pages of documents throughout the discovery, making document-by-document redaction impossible. *See United States v. Johnson*, 191 F. Supp. 3d 363, 372 (M.D. Pa. 2016) (“[T]he volume of materials precludes detailed, document-by-document redaction of sensitive information and personal identification information and in conjunction with the showing of good cause, warranted implementation of the [protective] order.” (internal quotation marks omitted)).

The discovery in the present case also contains thousands of communications and documents involving uncharged U.S. persons who were, as alleged in the indictment, unwittingly recruited by certain defendants and co-conspirators to engage in political activity inside the United States, such as attending Russian-organized rallies inside the United States. In certain cases the discovery includes PII such as telephone numbers, addresses, and other indicators that were collected by defendants and their co-conspirators during their operations. The government also

believes that if statements of these individuals were indiscriminately released, the result would be unnecessary embarrassment to these individuals who believed they were communicating about U.S. political activities with other U.S. persons. *See United States v. Luchko*, No. CRIM.A. 06-319, 2007 WL 1651139, at *7–8 (E.D. Pa. June 6, 2007) (imposing protective order in criminal case because disclosure would result “private and embarrassing activity concerning third parties, which I find would cause unnecessary or serious pain on parties . . . entitled to such protection” (internal quotation marks omitted)).

D. The Proposed Discovery Order Balances the Aforementioned Interests While Making Discovery Available to the Defense

The proposed protective order establishes rules for handling all discovery, as well as additional procedures related to sensitive but unclassified discovery that will be produced by the government to the defense.

1. Defendant Concord Management Should Be Prohibited from Providing or Discussing Discovery with any Co-Defendant Not Before this Court

In its initial proposed protective order, the government proposed a complete prohibition on sharing discovery with any co-defendant charged in this criminal case, whether individual or organizational. Defense counsel proposed that they be permitted to share discovery with a co-defendant if that co-defendant is an officer or employee of Concord Management. To the government’s knowledge, the only charged defendant in this category is Yevgeniy Viktorovich Prigozhin, who was charged individually for conspiring to defraud the United States, in violation of 18 U.S.C. § 371. (ECF NO. 1).

Prigozhin is alleged in the indictment to have approved and supported the operations of the Internet Research Agency, including those aimed at interfering in the 2016 U.S. elections. (ECF NO. 1, at 7). Prigozhin was indicted by the grand jury on February 16, 2018, and he has publicly

acknowledged that he is aware of his indictment, tell the public media, “I am not at all disappointed that I appear in this list [*i.e.*, the indictment]. If they want to see the devil — let them.” See “The Rise of ‘Putin’s chef,’ the Russian Oligarch Accused of Manipulating the U.S. Election,” *Washington Post*, Feb. 17, 2018; “Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as ‘Putin’s Cook,’” *N.Y. Times*, Feb. 16, 2018. Prigozhin is believed to be in Russia at this time, and he has not appeared before this Court to date.

As long as Prigozhin chooses not to appear personally in front of this Court, he is not entitled to review any discovery in this case. Courts generally do not allow a charged defendant to seek benefits from the judicial system whose authority he or she evades. See *Degen v. United States*, 517 U.S. 820, 824 (1996); see, e.g., *In re Assets of Martin*, 1 F.3d 1351, 1356 (3d Cir. 1993) (noting the “principle of mutuality” that “if a defendant is not willing to suffer the penalties of the crime,” the court “should not afford the defendant an opportunity to improve his or her position”); *Williams v. Holbrook*, 691 F.2d 3, 14 (1st Cir. 1982) (noting the impropriety of allowing an absent defendant to “opt in” if a matter “is decided favorably”). Courts have rejected motions for discovery and similar relief by defendants who refused to submit themselves to the Court. As one district court explained,

Upon learning charges have been brought for a crime in the United States, the fugitive, through counsel, could then request discovery from the government. This would allow the fugitive to preview or test the strength of the government’s evidence without being subject to the court’s jurisdiction.

United States v. Nabepanha, 200 F.R.D. 480, 483 (S.D. Fla. 2001); see also *United States v. Gorcyca*, No. 08-CR-9 (FB), 2008 WL 4610297, at *2 (E.D.N.Y. Oct. 16, 2008).

Courts have recognized that the presence of absent co-defendants can require the need to regulate discovery. In *United States v. Lorenzana-Cordon*, no. 1:03-cr-331 (CKK) (D.D.C. Mar.

19, 2015), the Court provided established discovery procedures that limited discovery to a “single-copy of discovery in electronic format on compact discs (‘CDs’), redacted as appropriate, and the CDs shall not be copied, duplicated, or replicated in whole or in part,” absent certain enumerated exceptions. (ECF No. 551, at 1–2). The Court required also that “discovery must remain in the custody of defense counsel or the defense team” and only be reviewed by the defendant in the presence of counsel. (*Id.*, at 2). In subsequent orders, the Court permitted additional redactions to account for overseas fugitive co-defendants, including redactions to the indictment itself, and prohibited defense counsel from further distribution of a partially unsealed indictment and other protected materials. *United States v. Lorenzana-Cordon*, 197 F. Supp. 3d 1, 3 (D.D.C. 2016).

While the government believes that defendant Concord Management should be fully barred from sharing information with defendant Prigozhin while he until he appears before this Court, in order to expedite discovery the proposed protective order explicitly allows defense counsel to seek to modify the order after counsel reviews discovery materials. Likewise, if Prigozhin appears before this Court, the protective order would not bar providing discovery to him as an authorized party.

2. Use of a Firewall Attorney to Address Disclosures of Sensitive Discovery to Foreign Nationals Is Appropriate

The parties agree that the particularly sensitive discovery in this case will physically remain in defense counsel’s U.S. offices. The government also anticipates that defense counsel may desire to have foreign nationals—such as Concord Management employees or officers—designated as authorized parties in order to review such materials. The government’s countervailing interest is that certain foreign individuals may try use that avenue as a way to obtain sensitive materials as part of an intelligence collection effort.

The government recognizes that names of proposed authorized persons may implicate

defense strategy information. In order to address this concern, the proposed protective order provides that, if defense counsel wishes to disclose sensitive material to a foreign national, the defense counsel notify the Court and a designated firewall counsel for the government. Firewall counsel would then raise any subsequent issues with such proposals with the Court and defense counsel without involvement of the prosecution team. A similar approach was put in place in *United States v. Loera*, No. 1:09-cr-044 (E.D.N.Y. 2017) (ECF No. 57), which has similar considerations and foreign nexuses. In that case, the Court restricted access to law-enforcement sensitive materials; required such materials to be kept by defense counsel; prohibited sensitive discovery's removal from the United States; and regulated foreign nationals' participation as part of the defense team through a firewall attorney from the government separate from the prosecution team. *Id.* A similar approach would be appropriate here.

CONCLUSION

For the reasons stated above, and to facilitate the availability of the discovery of this case while protecting the government's aforementioned interests as well as the privacy interests of third parties, the government requests the Court grant its motion and institute the proposed protective order.

Respectfully submitted,

ROBERT S. MUELLER III
Special Counsel

Dated: June 12, 2018

By: /s/ L. Rush Atkinson
Jeannie S. Rhee
L. Rush Atkinson
Ryan K. Dickey
U.S. Department of Justice
Special Counsel's Office
950 Pennsylvania Avenue NW

Washington, D.C. 20530
Telephone: (202) 616-0800

Attorneys for the United States of America