

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

:

**IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
E-MAIL ACCOUNTS**

:

**MEMORANDUM DECISION  
AND ORDER**

:

1:18-MJ-723 (AMD)

:

----- X

**ANN M. DONNELLY**, United States District Judge:

Microsoft Corporation is currently subject to a nondisclosure order that prohibits it from informing one of its corporate customers about the existence of a search warrant targeting two employee email accounts. (ECF Nos. 4, 36.) Microsoft seeks review of Magistrate Judge Peggy Kuo’s July 31, 2019 order denying its motion to modify the nondisclosure order to permit disclosure to at least one person at the corporate customer.<sup>1</sup> (ECF Nos. 35, 52.) For the following reasons, Microsoft’s motion is denied.

**BACKGROUND**

**I. The Search Warrant**

The Government is investigating an alleged conspiracy among employees at various multinational companies to send United States goods to a foreign country in contravention of United States sanctions. (ECF No. 1 ¶¶ 25, 36.) One of the companies under investigation subscribes to Microsoft’s email service. (*Id.* ¶¶ 36, 70.)

On August 3, 2018, the Government applied for a search warrant directing Microsoft to produce information associated with two individual email accounts registered to the customer.

---

<sup>1</sup> The Court is also in receipt of the unopposed motion for leave to file brief of amici curiae in support of Microsoft’s objections to Judge Kuo’s order. (ECF No. 66.) The Court grants the motion and takes the amicus brief under advisement.

(ECF No. 2 at 2.) While the targeted email accounts are registered to Microsoft’s customer, the search warrant seeks information “stored at premises owned, maintained, controlled, or operated by Microsoft.” (*Id.*) According to the Government’s affidavit, Microsoft stores data associated with these accounts on its servers, and the data would help the Government’s investigation.

(ECF No. 1 ¶ 70.)

In the search warrant affidavit, the affiant details information about the targeted employees’ involvement in alleged shipments to a sanctioned country, and asserts that there is probable cause to believe that the employees violated 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1956 (money laundering), and 50 U.S.C. §§ 1701-1705 (International Emergency Economic Powers Act (“IEEPA”)). (ECF No. 1 ¶¶ 5, 36, 40.)

After reviewing the affidavit, Magistrate Judge Marilyn D. Go found that the Government established probable cause for the search and issued the warrant. (ECF No. 2.)

## **II. The Nondisclosure Order**

In addition to the search warrant, the Government applied for a nondisclosure order pursuant to 18 U.S.C. § 2705(b) of the Stored Communications Act (ECF No. 1 ¶ 77), which authorizes a court to prohibit a service provider like Microsoft from notifying any person of the existence of a search warrant if the court “determines that there is reason to believe that notification . . . w[ould] result in” one of the following: (1) danger to 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) jeopardization of an investigation or undue delay of a trial. 18 U.S.C. § 2705(b). The Government argued that premature disclosure would jeopardize its investigation. (ECF No. 1 ¶ 77.)

Judge Go issued the nondisclosure order, concluding that disclosure of the warrant to someone at the corporate customer would “seriously jeopardize the investigation or unduly delay a trial . . . .” (ECF No. 4 at 1-2.) The nondisclosure order prohibits Microsoft from “notify[ing] any person (including the subscribers and customers of the account(s) listed in the warrant) of the existence of the . . . warrant for [a] period of one year[.]” (*Id.*)

### **III. Judge Kuo’s Decision**

Microsoft subsequently moved to modify the nondisclosure order (ECF No. 12) so that it could “notify an appropriate individual” at the corporate customer about the warrant. (ECF No. 14 at 2.)<sup>2</sup> Microsoft argued that the customer’s status as “a major conglomerate with [thousands of] employees worldwide” meant that there had to be someone at the company “who c[ould] be notified of the warrant without compromising the Government’s investigation.” (*Id.*)

In a thorough and well-reasoned decision, Judge Kuo denied Microsoft’s motion, concluding that the nondisclosure order was narrowly tailored to protect the Government’s compelling interest in safeguarding the integrity of its investigation. (ECF Nos. 35 and 52 at 9, 12.) In particular, Judge Kuo found that disclosure of the warrant could result in witnesses and perpetrators changing or concealing their behavior and destroying evidence. (ECF No. 52 at 9.) Moreover, because the two employees used their corporate email accounts and did not attempt to hide their behavior, there was a “possibility that high-level employees at the Customer knew of or condoned th[e] activity.” (*Id.* at 10.) Accordingly, the nondisclosure order—limited in duration to one year—was proper. (*Id.* at 9.) Microsoft produced to the Government data responsive to the warrant and did not alert anyone at the corporate customer about the warrant. (ECF No. 45 at 15 n.9.)

---

<sup>2</sup> Microsoft also moved to stay compliance with the warrant pending the court’s decision on its motion for modification. (ECF No. 16.) Judge Kuo denied the motion. (ECF No. 31.)

#### IV. Current Status of the Nondisclosure Order

On August 3, 2019, the nondisclosure order's original expiration date, the Government moved to extend the order for an additional year. (ECF No. 36.) Magistrate Judge Steven Tiscione concluded that Microsoft's disclosure of the warrant to the subscriber company would "seriously jeopardize the investigation or unduly delay a trial . . . ." (ECF No. 36 at 4-5.) He extended the nondisclosure order for an additional year. (*Id.*)

The nondisclosure order is now due to expire on August 3, 2020. On September 13, 2019, Microsoft sought review of Judge Kuo's order denying its motion to modify the nondisclosure order. (ECF No. 45.) I heard oral argument on November 19, 2019 and requested additional information from the Government about its investigation. In January of 2020, the Government provided the requested update, and the parties provided supplemental authority. (ECF Nos. 69, 70, 71; *see also* ECF No. 72.) In its submission, filed *ex parte*, the Government argues that there should be no modification to the nondisclosure order because the investigation could result in criminal liability for the corporate customer. (ECF No. 69.)

#### STANDARD OF REVIEW

When a party submits a timely objection to a magistrate judge's ruling, the district court reviews *de novo* the parts of the ruling to which the party objected. Fed. R. Civ. P. 72; 28 U.S.C. § 636(b)(1)(C); *see also United States v. Romano*, 794 F.3d 317, 340 (2d Cir. 2015).

"[D]ispositive matters referred under the 'additional duties' provision in § 636(b)(3) are [also] subject to the *de novo* review standard in subsections (b)(1)(B) and (C)." *United States v.*

*Warshay*, No. 98-CV-1245, 1998 WL 767138, at \*3 (E.D.N.Y. Aug. 4, 1998). I apply a *de novo* standard of review.<sup>3</sup>

---

<sup>3</sup> The parties agree that the Court's review of the magistrate judge's ruling is *de novo*. (ECF No. 45 at 18 n.11; ECF No. 60 at 6.)

## DISCUSSION

Microsoft challenges the nondisclosure order as an unconstitutional prior restraint on its speech. (ECF No. 45 at 8.) It argues that a less restrictive alternative—notification of an appropriate officer, director, or employee of the corporate customer—will achieve the Government’s goal of maintaining the secrecy of the investigation while ensuring that the corporate “customer[] . . . maintain[s] the same level of control and privacy over [its] cloud-based information as when [it] store[s] that information on premises.” (*Id.* at 12-13.) The Government responds that the nondisclosure order is proper as it is, and that Microsoft’s proposed alternative would not sufficiently protect the Government’s investigation. (ECF No. 60 at 4, 12.)

### I. First Amendment

The First Amendment prohibits the enactment of laws abridging the freedom of speech. U.S. CONST., amend. I. Speech that is critical of the Government’s exercise of power is at the heart of the First Amendment. *See Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1034 (1991) (“There is no question that speech critical of the exercise of the State’s power lies at the very center of the First Amendment.”). At the same time, the Amendment “does not comprehend the right to speak on any subject at any time.” *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 31 (1984); *see also Zalaski v. City of Bridgeport Police Dep’t*, 613 F.3d 336, 341 (2d Cir. 2010) (The Amendment “does not guarantee the right to communicate one’s views at all times and places or in any manner that may be desired.”) (citation omitted).

Courts apply varying levels of scrutiny when reviewing government restrictions on speech. Content-based restrictions are subject to strict scrutiny, while content-neutral restrictions are subject to intermediate scrutiny. *See Time Warner Cable Inc. v. F.C.C.*, 727 F.3d 137, 155

(2d Cir. 2013). A prior restraint on speech such as the one at issue here carries “a heavy presumption against” its constitutionality. *Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 582-83 (1976). “A judicial order forbidding certain communications when issued in advance of the time that such communications are to occur is generally regarded as a prior restraint” on speech. *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 871 (2d Cir. 2008) (citing *Alexander v. United States*, 509 U.S. 544, 550 (1993) (emphasis and internal quotation marks omitted)).

The Second Circuit has not ruled definitively on the appropriate level of scrutiny for nondisclosure orders like the one at issue here. *See Doe*, 549 F.3d at 876 (noting that a similar provision in 18 U.S.C. § 2709 was not a “typical example” of a prior restraint, and that the “panel [was] not in agreement” about the applicable standard of scrutiny). However, courts in other circuits have held that nondisclosure orders pursuant to Section 2705(b)—like the one here—are content-based prior restraints on speech, and subject to strict scrutiny. *See, e.g., Matter of Subpoena 2018R00776*, 947 F.3d 148, 156 (3d Cir. 2020) (“Because the [nondisclosure orders] are content-based restrictions and presumptively unconstitutional prior restraints, we apply strict scrutiny to determine whether they are constitutionally inform.”); *see also Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d 970, 980 (C.D. Cal. 2017) (collecting cases). I conclude that strict scrutiny is the appropriate standard of review.

## **II. Strict Scrutiny Standard**

Application of strict scrutiny requires the Government to show that “the nondisclosure requirement is ‘narrowly tailored to promote a compelling government interest.’” *Doe*, 549 F.3d at 878 (citing *United States v. Playboy Entm’t Group, Inc.*, 529 U.S. 803, 813 (2000)). “Mere conjecture” about the harms of disclosure is inadequate “to carry a First Amendment burden.” *Nixon v. Shrink Missouri Gov. PAC*, 528 U.S. 377, 379 (2000). The Government must prove

“that there are no less restrictive alternatives that would be at least as effective in achieving” the government’s compelling interest. *Doe*, 549 F.3d at 878 (citing *Reno v. ACLU*, 521 U.S. 844 (1977) (internal alteration omitted)).

Maintaining the integrity of an ongoing criminal investigation is a compelling governmental interest. *See United States v. Smith*, 985 F. Supp. 3d 506, 545 (S.D.N.Y. 2013) (government has a compelling interest in the secrecy of an ongoing investigation); *see also Matter of Subpoena 2018R00776*, 947 F.3d at 156 (“The government’s interest is particularly acute where, as here, the investigation is ongoing.”). That is especially true when national security is implicated. “No government interest is more compelling than the security of the Nation.” *United States v. Aref*, 533 F.3d 72, 83 (2d Cir. 2008) (citing *Haig v. Agee*, 453 U.S. 280, 307 (1981)).

Nevertheless, determining whether the government has met its burden is “a delicate task” for a district court. *Doe*, 549 F.3d at 881. In considering the constitutionality of 18 U.S.C. § 2709, a similar nondisclosure requirement prohibiting electronic service providers from disclosing FBI-authorized administrative subpoenas related to international terrorism and clandestine intelligence investigations, the Second Circuit explained:

While the court will normally defer to the Government’s considered assessment of *why* disclosure in a particular case may result in an enumerated harm related to such grave matters as international terrorism . . . , it cannot, consistent with strict scrutiny standards, uphold a nondisclosure requirement on a conclusory assurance that such a likelihood exists . . . . [A] court must receive some indication that the [Executive Branch’s] judgment has been soundly reached.

*Id.* at 881-882. The Second Circuit remanded the case for further proceedings, finding that the FBI’s certification—which said only that “disclosure . . . may endanger the national security of the United States”—was unacceptably conclusory. *Id.* at 881, 885.

**A. The Case Before Judge Kuo**

As explained above, 18 U.S.C. § 2705(b) authorizes a court to prohibit a service provider from notifying any person of the existence of a search warrant if “there is reason to believe that notification w[ould] result in” any one of five enumerated harms: (1) danger to 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) jeopardization of an investigation or undue delay of a trial. *Id.*

Microsoft argued to Judge Kuo that the Government “relied on unfounded assumptions regarding the risks of notification” to support the issuance of the nondisclosure order, and that “uncertainty at this stage of the investigation as to who can be trusted with knowledge of the search warrant” is insufficient to meet strict scrutiny.<sup>4</sup> (ECF No. 34 at 18, 21.) The company contended that there had to be a “*single . . . person*” at its corporate customer to whom the warrant’s disclosure would be appropriate. (*Id.* at 20.)

The Government replied that protecting the integrity of ongoing criminal investigations is a well-established and compelling governmental interest, and that Microsoft’s single “person[] standard would effectively preclude the use of [nondisclosure orders] to protect the integrity of criminal investigations.” (*Id.* at 6-7, 11.)

Judge Kuo’s decision rejecting Microsoft’s position was correct in all respects. The Government established good reason to believe that disclosing the search warrant to Microsoft’s customer would jeopardize its investigation.<sup>5</sup> The search warrant application describes in detail

---

<sup>4</sup> Microsoft’s request for access to the Government’s *ex parte* affidavit in support of the warrant so that it can “refute or explain why” the underlying facts “have no bearing on the strict scrutiny analysis” (ECF No. 45 at 24-25) is denied.

<sup>5</sup> Section 2705(b) requires that the Court find “reason to believe” that notification would result in one of several harms, 18 U.S.C. 2705(b), a standard that the Second Circuit has interpreted in a similar statute to

a conspiracy among employees at different multinational companies to send United States goods to a foreign country, sanctioned for its support of international terrorism, in contravention of United States sanctions. (ECF No. 1 ¶¶ 15, 16, 25, 36.) Maintaining the secrecy of this ongoing criminal investigation, which involves matters of national security, is a compelling governmental interest.

The Government also demonstrated that the nondisclosure order was narrowly tailored to achieve its compelling interest. At the time it was entered, the nondisclosure order was limited to one year. (ECF No. 4 at 1.) Moreover, there was a risk that other employees, including higher-ups, were involved in the conspiracy. As detailed in the search warrant affidavit, the targeted employees did not attempt to conceal their conduct; they used their company email addresses, and interacted with high-level employees at the co-conspirator company. Additionally, the criminal conduct under investigation—wire fraud, money laundering and IEEPA violations—was allegedly carried out in the company’s financial interest.<sup>6</sup>

Judge Kuo’s decision to reject Microsoft’s proposal—that they should be permitted to notify someone at the company, like a senior official or a lawyer in its United States office, of the warrant (ECF No. 45 at 15-16, 23)—was correct, because Microsoft’s proposal was not as effective as the nondisclosure order in achieving the Government’s purpose.<sup>7</sup> *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 874 (1997) (the less restrictive alternative must “be at least

---

mean “good reason to believe.” *Doe*, 549 F.3d at 881. This standard avoids the prospect of district courts “blindly credit[ing]” the government’s finding of “any conceivable . . . reason” to support nondisclosure. *Id.*

<sup>6</sup> Microsoft argues that “[a]ll manner of corporate misconduct serves a corporation’s financial interests.” (ECF No. 45 at 21-22.) As Judge Kuo observed, this is not always the case. “[T]he alleged criminal conduct by the two individual employees implicates the Customer directly, unlike a more individualized crime, such as child pornography[.]” (ECF No. 52 at 10.)

<sup>7</sup> Significantly, Microsoft’s proposal does not extinguish the burden on speech. It simply shifts it to others—employees at the targeted company—who presumably owe a duty of loyalty to the company.

as effective in achieving the legitimate purpose that the statute was enacted to serve.”). The Third Circuit recently rejected a similar proposal as “impractical” and “ineffective in maintaining grand jury secrecy.” *Matter of Subpoena 2018R00776*, 947 F.3d at 158. After all, the Government cannot be expected simply to accept whatever person Microsoft selects. And it would be unduly burdensome to require the Government to open a side investigation into a person’s background, and then decide whether the person could be trusted to maintain the secrecy of the investigation. “Neither courts nor the government can be expected to vet individuals selected by service providers and determine their risk of subverting an ongoing investigation. Strict scrutiny does not demand that sort of prognostication.” *Id.* at 159.

In view of the nature of the investigation into ongoing conduct and the attendant national security concerns, and the significant possibility that senior-level employees participated in the conspiracy, the nondisclosure order met strict scrutiny.<sup>8</sup>

### **B. The Current Status of the Investigation**

Judge Kuo ordered that the Government “must again satisfy strict scrutiny based on the information it presents at that point in time, including details of any developments in its investigation” if it seeks to extend the nondisclosure order. (ECF No. 52 at 12.) The case before me is in a different posture than it was when Judge Kuo made her decision; over a year has passed since the issuance of the original nondisclosure order, and Judge Tiscione subsequently granted the Government’s request for a one-year extension of the order on August 1, 2019. (ECF

---

<sup>8</sup> *Facebook v. Pepe*, No. 19-SS-1024, 2020 WL 1870591 (D.C. Apr. 15, 2020), which Microsoft cites, does not compel a different result. Pepe, a criminal defendant in a local prosecution for the shooting of a man, subpoenaed Facebook for Instagram content of one of its subscribers in an effort to establish self-defense. The D.C. Court of Appeals held that Pepe did not establish a substantial risk of prejudice or spoliation under the particular facts of that case, and that there were less restrictive means available to protect Pepe’s interests. *Id.* at 10-11. There are no such similar means available in this case.

No. 36.) Accordingly, at the November 2019 oral argument, I directed the Government to submit an update on its investigation.

The Government's *ex parte* application demonstrates the continued need for the nondisclosure order. The Government continues to have a compelling interest in safeguarding its investigation into a multinational conspiracy with national security implications. Moreover, the investigation has uncovered the possible involvement of additional employees, including employees at a different corporate office than the original targets, and one of whom is in a senior position. Given the broader employee involvement and possible corporate criminal liability, there is a significant risk that disclosure of the search warrant to anyone at the customer would jeopardize the Government's entire investigation. Accordingly, the nondisclosure order continues to meet strict scrutiny.

It is undoubtedly the case that litigants seeking to vindicate their rights often slow the progress of an investigation. Nevertheless, the Government will have to satisfy strict scrutiny should it seek to extend the nondisclosure order. To require anything less would “cast Article III judges in the role of petty functionaries, persons required to enter as a court judgment an executive officer's decision, but stripped of capacity to evaluate independently whether the executive's decision is correct.” *Doe*, 549 F.3d at 881 (citing *Gutierrez de Martinez v. Lamagno*, 515 U.S. 417, 426 (1995)).

**CONCLUSION**

Microsoft's motion to modify the nondisclosure order is denied. Portions of Judge Kuo's July 31, 2019 order remain under seal. By May 22, 2020, the parties must identify the portions of this document, if any, that they wish to redact and maintain under seal, and explain the need for such continued secrecy. The portions of this document as to which there is no such showing of need will then be unsealed.

**SO ORDERED.**

s/Ann M. Donnelly

---

Ann M. Donnelly  
United States District Judge

Dated: Brooklyn, New York  
May 8, 2020  
As modified May 22, 2020