UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

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

Case No. 18-MJ-723 (PK)

ORDER

Peggy Kuo, United States Magistrate Judge

On-line service provider Microsoft Corporation ("Microsoft") challenges on First Amendment grounds a Non-Disclosure Order ("NDO") (Dkt. 3), compelling it not to disclose the existence of a search warrant (the "Search Warrant") to any person, including the subscriber of two e-mail accounts which are the subject of the Search Warrant. The subscriber of the accounts is a corporate Microsoft customer ("Customer"), and the two e-mails are assigned to two of its employees. Microsoft argues that the NDO is an overbroad prior restraint on its speech and requests that the NDO be modified to allow it to notify "an appropriate individual" at the Customer of the existence of the Search Warrant. (Microsoft's Mem. of Law at 12, Dkt. 14.) For the reasons stated herein, the "Motion to Modify Non-Disclosure Order" ("Motion") (Dkt. 12) is denied.

PROCEDURAL BACKGROUND

On August 3, 2018, Magistrate Judge Marilyn D. Go issued the Search Warrant, upon a showing of probable cause, for the search of information associated with two e-mail accounts "that is stored at premises owned, maintained, controlled, or operated by" Microsoft. (Search Warrant at 3, Dkt. 2.) It directs Microsoft, as the service provider for those accounts, to disclose certain information "within the possession, custody, or control of Microsoft" associated with these two

accounts, including usage records and data, as well as the contents of emails, text messages and voicemails. (*Id.*) In a detailed supporting affidavit, the Government asserts, among other things, that the individual users of the two e-mail accounts, along with others, committed violations of wire fraud (18 U.S.C. § 1343), money laundering (18 U.S.C. § 1956), and the International Emergency Economic Powers Act ("IEEPA") (50 U.S.C. §§ 1701-1705). (Affidavit in Support of an Application for Search Warrants ("SW Affidavit") at 3, ¶ 5, Dkt. 1.) It further states that the individual users are employed by a multinational corporation that has conspired with another multinational corporation "to violate IEEPA by sending and attempting to send U.S. origin goods to [a company] in [a foreign country], in contravention of U.S. sanctions." (*Id.* at 10-11, ¶ 25.) The affidavit provides details from e-mails which the Government obtained through prior search warrants, in which the individual user of one of the e-mail accounts — a customer service representative of a wholly owned subsidiary of the Customer — communicates with senior employees of the other company regarding the shipment of goods manufactured in the United States to a country where such goods would otherwise be banned from export. (*Id.* at 15-20, ¶¶ 35-47.) The individual user of the second e-mail account, also an employee of the Customer subsidiary, is copied on many of those e-mails. (*Id.*)

Along with the Search Warrant, the Government requested an order that Microsoft "not disclose the existence of the attached warrant, or this Order of the Court, to the listed subscriber or to any other person, for the period of one year from the date of this Order. . . ." (NDO at 1.) Judge Go concluded that "there is reason to believe that notification of the existence of the attached warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, and intimidate potential witnesses." (*Id.* at 1.) Accordingly, Judge Go issued the NDO pursuant to 18 U.S.C. § 2705(b). (*Id.*)

On September 7, 2018, Microsoft filed the Motion. The Government opposed the Motion (Govt.'s Mem. of Law, Dkt. 23.), and the Court heard oral argument from both parties.[1]

STATUTORY BACKGROUND

The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, was designed "to protect legitimate law enforcement needs while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers." 132 CONG. REC. S14449 (daily ed. Oct. 1, 1986) (statement of Sen. Leahy). In balancing these interests, Title II, the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* ("SCA"), generally precludes electronic communication services and remote computing services from disclosing certain information, while also empowering the Government to compel a service provider to disclose records, information and contents of such communications in specific circumstances, through use of a warrant, subpoena or court order. 18 U.S.C. § 2703 (a)-(c).

Furthermore, Section 2705(b) of the SCA permits the government to prevent a service provider from notifying any person of the existence of a such a warrant, subpoena or court order by obtaining a non-disclosure order, and directs that "[t]he court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in" one or more of the following harms: "(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." 18 U.S.C. § 2705(b).

[1] Microsoft also filed a Motion to Stay requesting that the Court stay Microsoft's compliance with the Search Warrant until the Motion was resolved. (Microsoft's Mot. to Stay, Dkt. 16.) On October 16, 2018, the Court denied Microsoft's Motion to Stay. (October 16, 2018 Order, Dkt. 31.)

THE PARTIES' ARGUMENTS

Microsoft argues that the NDO constitutes a prior restraint under the First Amendment and, therefore, must satisfy strict scrutiny in order to be valid. (Microsoft's Mem. of Law at 1.) It contends that the NDO fails strict scrutiny because it is not the "least restrictive means" of achieving the Government's interest. (*Id.*) A "less restrictive alternative," in its view, would be notifying an appropriate individual at the Customer (other than the individual users whose e-mail accounts are to be searched) of the Search Warrant. (*Id.* at 11.) It argues there are good reasons for exercising this alternative. (*Id.*) Microsoft has made commitments to its customers, embodied in its customer contracts, that, "if compelled to disclose customer data to law enforcement, Microsoft will promptly notify the [customer] and provide a copy of the demand, unless legally prohibited from doing so." (*Id.* at 6-7.) In addition, working with a person within the Customer to respond to the Search Warrant could help identify documents subject to privilege and assist Microsoft in its compliance with the law of the foreign jurisdiction where the Customer and its subsidiary are located.[2]

In support of this proposed notification, Microsoft cites the document entitled *Seeking Enterprise Customer Data Held by Cloud Service Providers*, issued by the U.S. Department of Justice Criminal Division Computer Crime and Intellectual Property Section, dated December 2017 ("DOJ Recommended Practices"), available at: https://www.justice.gov/criminal-ccips/file/1017511/download). (Microsoft's Mem. of Law at 2, 4; *see also* Ex. 1 to Joachim Decl., Dkt. 15.) This document identifies "recommended practices" for seeking information belonging to a subscriber which is an organization rather than an individual. (DOJ Recommended Practices at 1.)

[2] Foreign law imposes certain obligations on service providers, depending on the specific data being disclosed. (Oral Argument Transcript at 58, Dkt. 34.) Because it "doesn't peek inside [the customer's] cloud...," Microsoft does not have a detailed understanding of the content of the data and therefore cannot know whether its disclosure is valid under foreign law. (*Id.*)

It encourages prosecutors to "seek data directly from the enterprise, rather than its cloud-storage provider if doing so will not compromise the investigation." (Microsoft's Mem. of Law at 2, citing DOJ Recommended Practices at 1.)

Microsoft suggests that someone in executive management at the Customer, a member of its Board of Directors, or the General Counsel would be "plausible candidates for notification." (Microsoft's Mem. of Law at 6, 11.) Conceding that it does not know who that person might be, since it is not privy to the details of the Government's investigation, it proposes that the parties confer and jointly identify that person. (*Id.* at 12.) Microsoft finds it "implausible" that in "a major conglomerate with [thousands of] employees worldwide," there is not one individual who can be notified "without compromising the Government's investigation," especially since the two users of the e-mails are employed by a "discrete business unit" of the Customer. (*Id.* at 7, 11.) It argues that the Government has failed to show that this alternative will be ineffective to achieve the Government's goals. (*Id.* at 11-12.)

The Government questions whether strict scrutiny should be applied to the NDO. Citing language in *John Doe, Inc. v. Mukasey,* 549 F.3d 861, 878 (2d Cir. 2008), it argues that restrictions on this type of speech may not "raise the same specter of government censorship" as in other situations. (Govt.'s Mem. of Law at 7.) Nevertheless, it contends that the NDO "survives even strict scrutiny" since it is already narrowly tailored to achieve the Government's "compelling interest in protecting the integrity of its ongoing investigation." (*Id.* at 7.) It notes that the First Amendment requirement of "narrowly tailored" does not mean it must prove that there is "*no* person employed by Microsoft's subscriber who could be notified" without resulting harm.[3] (*Id.* at 9 (emphasis in original).)

[3] The Government also argues that Microsoft has forfeited its rights by failing to "comply with or object to the warrant within the 14-day period in which this Court ordered Microsoft to respond to the warrant." (Govt.'s Mem. of Law at 14.) However, waivers of constitutional rights must be made "voluntarily,

DISCUSSION AND ANALYSIS

The First Amendment to the United States Constitution prohibits the enactment of laws "abridging the freedom of speech." *Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2226, 192 L. Ed. 2d 236 (2015) (quoting U.S. Const., Amdt. 1). In general, it precludes the government "from proscribing speech, or even expressive conduct, because of disapproval of the ideas expressed." *R.A.V. v. City of St. Paul, Minn.*, 505 U.S. 377, 382, 112 S. Ct. 2538, 120 L. Ed. 2d 305 (1992) (internal quotations omitted). Courts apply different levels of scrutiny to First Amendment controversies, depending on whether the regulation is content-neutral or content-based. Content-based regulations are subject to strict scrutiny, *see, e.g., United States v. Playboy Entm't Grp.*, Inc., 529 U.S. 803, 813, 120 S. Ct. 1878, 1885, 146 L. Ed. 2d 865 (2000), while content-neutral regulations are subject to intermediate scrutiny, *see, e.g., Turner Broad. Sys., Inc. v. F.C.C.*, 520 U.S. 180, 213–14, 117 S. Ct. 1174, 1198, 137 L. Ed. 2d 369 (1997). Administrative or judicial orders forbidding certain communications issued in advance of the time such communications are to occur constitute prior restraints, which bear a "heavy presumption against their constitutionality." *Microsoft Corporation v. U.S. Department of Justice*, 233 F. Supp. 3d 887, 905 (W.D. Wash. 2017) (citing *Alexander v. United States*, 509 U.S. 544, 550, 113 S.Ct. 2766, 125 L.Ed.2d 441 (1993); *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 225, 110 S.Ct. 596, 107 L.Ed.2d 603 (1990)).

A non-disclosure order issued pursuant to Section 2705(b) of the Stored Communications Act imposes a speech restriction which courts have generally construed as a content-based prior restraint subject to strict scrutiny under the First Amendment. *See, e.g., Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d 970, 980 (C.D. Cal. 2017) (indicating that courts "have almost

---

knowingly, and intelligently," and must be established by "clear and compelling evidence." *Legal Aid Society v. City of New York*, 114 F. Supp. 2d 204, 226 (S.D.N.Y. 2000). The waiver of a fundamental right "can neither be presumed nor may it be lightly inferred." *Id.* (quoting *Doe v. Marsh*, 105 F.3d 106, 222 (2d Cir. 1997)). Here, absent clear and compelling evidence of waiver, the Court finds that Microsoft did not waive its First Amendment rights.

uniformly found" that non-disclosure orders under Section 2705(b) and analogous statutes "are prior restraints and/or content-based restrictions") (citing *Microsoft Corporation,* 233 F. Supp. 3d at 905-06; *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 881-83 (D. Tex. 2008); *Matter of Grand Jury Subpoena*, 79 F. Supp. 3d 1091 (N.D. Cal. 2015); *In re Application of the United States of Am. for Nondisclosure Order Pursuant to 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014032122836*, No. MC 14-480 (JMF), 2014 WL 1775601, at *2 (D.D.C. Mar. 31, 2014)).

Constitutional challenges to Section 2705(b) non-disclosure orders have focused, to date, on indefinite non-disclosure orders, which lack any time limitation. For example, the Court in *Microsoft Corporation* denied the Government's motion to dismiss Microsoft's action for declaratory judgment that indefinite non-disclosure orders under Section 2705(b) violate the First Amendment. *Microsoft Corporation,* 233 F. Supp. 3d at 887. It found that such non-disclosure orders "restrain Microsoft from speaking about government investigations without any time limit on that restraint," and thus constituted a prior restraint on speech. *Id.* at 905-06. It concluded that sufficient facts were alleged to "state a claim that certain provisions of Section 2705(b) fail strict scrutiny review and violate the First Amendment." *Id.* at 908; *see also In re Search Warrant Issued to Google,* 269 F. Supp. 3d 1205 (N.D. Ala. 2017) (finding that indefinite nondisclosure order did not satisfy strict scrutiny and imposing 180-day limit); *Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d at 970 (same).

The Government acknowledges that the First Amendment applies to the NDO, but questions whether the NDO should be considered a content-based prior restraint subject to strict scrutiny. It cites the Second Circuit's decision in *Doe v. Mukasey,* 549 F.3d at 861, raising the possibility that a "less exacting standard may be appropriate" for a limited restraint in the "analogous" situation of a National Security Letter ("NSL"). (Govt.'s Mem. of Law at 6.) *Doe v. Mukasey* opines that the non-disclosure requirement imposed on NSLs is not "a typical example" of a prior restraint because "it is not a restraint imposed on those who customarily wish to exercise

rights of free expression, such as speakers in public fora, distributors of literature, or exhibitors of movies." *Doe v. Mukasey,* 549 F.3d at 876 (citations omitted). It also states that the category of information "is far more limited than the broad categories of information that have been at issue with respect to typical content-based restrictions." *Id.* (citations omitted.) However, the Second Circuit in *Doe v. Mukasey* expressly did not hold that a standard less stringent than strict scrutiny should apply to NSLs. It noted that the appeals panel "is not in agreement" on the matter, and, in any event, the Government in that case "conceded that strict scrutiny is the applicable standard." *Id.* at 878. Therefore, the Second Circuit actually applied the strict scrutiny standard, *id.* at 876, and the Government can find no analogy or support for applying a lower standard here. Furthermore, despite raising the issue, the Government does not articulate what "less exacting standard" should apply, simply falling back on the argument that the NDO "survives even strict scrutiny" because of its narrow tailoring. (Govt.'s Mem. of Law at 6.)

Given the uniformity in how other courts have analyzed Section 2705(b) non-disclosure orders under the First Amendment, and the lack of an articulated lower standard for content-based prior restraints in cases such as this, the Court applies strict scrutiny here.[4]

In order to satisfy strict scrutiny, the Government must demonstrate that the restriction of non-disclosure is "narrowly tailored to promote a compelling Government interest and that there are no less restrictive alternatives to achieve the Government's purpose." *Doe v. Mukasey,* 549 F.3d at 878 (quoting *Playboy,* 529 U.S. at 813 and *Reno v. ACLU,* 521 U.S. 844, 874, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997) (quotation marks omitted)). The Government must show that there are no

[4] In *Microsoft Corporation,* 233 F. Supp. 3d at 908, the court also applied, in the alternative, a lower standard of review, finding that, "even if a lesser standard of review applies to Microsoft's First Amendment claim" and a balancing approach were applied, Microsoft's "rights may outweigh the state's interest such that indefinite [non]disclosure orders impermissibly burden Microsoft's rights." *Id.* (citing *In re § 2703(d),* 787 F. Supp. 2d 430, 438 (E.D. Va. 2011)). The Court here does not find it necessary to apply an analysis under a lower standard of review.

"less restrictive alternatives [that] would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve." *Reno,* 521 U.S. at 874; *see also, Green Party of Connecticut v. Garfield*, 616 F.3d 189, 208-09 (2d Cir. 2010); *Doe v. Mukasey,* 549 F.3d at 878. "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." *Playboy*, 529 U.S. at 816.

The Court finds that the Government has demonstrated a compelling interest in safeguarding the integrity of its ongoing investigation. The affidavit submitted *ex parte* to the Court in support of the Search Warrant details the ongoing criminal conduct under investigation. The Government is investigating a conspiracy among several individuals, including high-ranking employees of a company doing business with the Customer, to violate U.S. laws and regulations banning exports to a foreign country which, according to a series of Executive Orders, supports terrorism, among other actions. (SW Affidavit at 7, ¶¶ 15-16.) Because the criminal conduct is ongoing, there is a danger that if witnesses and perpetrators learn of the Search Warrant, they will flee, alter or conceal their behavior, and destroy evidence. Secrecy of such an ongoing criminal investigation thus constitutes a compelling Government interest. *See, e.g., U.S. v. Smith*, 985 F. Supp. 2d 506 (S.D.N.Y. 2013) (finding, in the context of the right to access judicial documents, that the government has a "compelling interest in ongoing investigations into potentially serious criminal conduct."); *United States v. Armstrong,* 185 F. Supp. 3d 332, 336 (E.D.N.Y. 2016) ("Unquestionably, there is a government interest in the secrecy of ongoing investigations.").

The Court next examines whether the NDO is narrowly tailored to achieve the Government's compelling interest. At the outset, the Court notes that, unlike the indefinite non-disclosure orders at issue in *Microsoft Corporation,* 233 F. Supp. 3d at 887 and *In re Search Warrant Issued to Google,* 269 F. Supp. 3d at 1205, the NDO is limited in duration to one year from the date of the

order. Of course, a "prior restraint is not constitutionally inoffensive merely because it is temporary." *U.S. v. Quattrone,* 402 F.3d 304, 310 (2d Cir. 2005).

The question is whether Microsoft's proposed less restrictive alternative of identifying and notifying an appropriate person inside the Customer would serve the Government's purpose as effectively as the NDO now stands. If it does, then the NDO would not be narrowly tailored and would run afoul of the First Amendment.

The information which the Government has developed thus far in its investigation shows that certain employees of a wholly owned subsidiary of the Customer used their work e-mails to communicate with senior employees of another company about committing illegal activity. (SW Affidavit at 15, ¶ 36.) It also appears that the individuals under investigation acted on behalf of the Customer, to its financial benefit. (Govt.'s Mem. of Law at 2.) The fact that the two employees used the Customer's e-mail accounts to facilitate the illegal activity, without apparent attempts to hide it from their employer, raises the possibility that high-level employees at the Customer knew of or condoned that activity. In addition, as the Government pointed out at oral argument, the nature of the alleged criminal conduct by the two individual employees implicates the Customer directly, unlike a more individualized crime, such as child pornography, for which the Government could carve out corporate representatives unrelated to the criminal allegations. (*See* Oral Argument Transcript at 39.)

The Government emphasizes that at this stage in its investigation, it does not know exactly who else at the Customer was aware of or may be involved in the illegal activities. (*Id.* at 25.) In the absence of this information, disclosing the Search Warrant to anyone in the Customer "including specifically the CEO or the CSO" will jeopardize the investigation and leave the Government "with no assurance of the secrecy of its investigation." (Govt.'s Mem. of Law at 12; Oral Argument Transcript at 37.)

The DOJ Recommended Practices, on which Microsoft relies, recognize that circumstances may arise in which the recommended practice of notifying the subscriber rather than the service provider is not feasible, stating, "[i]f law enforcement has developed reasons to believe that the enterprise will be unwilling to comply or if the enterprise itself is principally devoted to criminal conduct, seeking disclosure directly from the cloud provider may be the only practical option." DOJ Recommended Practices at 2-3. While it has not been alleged that the Customer itself is "*principally* devoted to criminal conduct," there is uncertainty at this stage of the investigation as to who can be trusted with knowledge of the Search Warrant. The DOJ Recommended Practices also posit other circumstances for departing from its recommended practice,

> Other practical considerations might also leave the government with no choice but to seek disclosure directly from the provider. . . . Law enforcement might be unable to find a trustworthy point of contact (or, perhaps, any point of contact) at the enterprise. Disclosure of the investigation at a sensitive stage might put a cooperating witness in danger. DOJ Recommended Practices at 3.

There is, thus, a recognition that the particular circumstances of each situation can play a role even in applying the DOJ's recommendations. Microsoft suggests that measures could be taken to ensure that any point of contact within the Customer maintains the secrecy of the Search Warrant. For example, a protective order prohibiting any person inside the Customer from disclosing the Search Warrant to anyone else would put them within the contempt power of the Court. However, both the Customer and its fully owned subsidiary are headquartered outside the United States, potentially placing them outside the contempt jurisdiction of the Court. Similarly, while the Customer's legal department might provide candidates for notification, the General Counsel would have a professional duty to advise its client of the Search Warrant, thus making it impossible to maintain secrecy. (*See* Govt.'s Mem. of Law at 12.)

Given these particular circumstances, notification of the Search Warrant to someone at the Customer would not be effective in achieving the Government's interest in protecting the integrity

of its ongoing investigation. (*See* Oral Argument Transcript at 26.) The First Amendment "requires that [the speech restriction] be narrowly tailored, not that it be 'perfectly tailored.'" *Williams-Yulee v. Fla. Bar*, 135 S. Ct. 1656, 1671, 191 L. Ed. 2d 570 (2015) (quoting *Burson v. Freeman*, 504 U.S. 191, 112 S. Ct. 1846, 119 L. Ed. 2d 5 (1992)).

Accordingly, the Court finds that, applying strict scrutiny, the NDO does not violate Microsoft's First Amendment rights.

In reaching this conclusion, the Court notes that the NDO expires one year from the date of the order. At that time, if no application for extension of the NDO is sought, Microsoft will be free to notify the Customer, and anyone else, of the Search Warrant. If the Government seeks to extend the non-disclosure ban on Microsoft, it must again satisfy strict scrutiny based on the information it presents at that point in time, including details of any developments in its investigation.

CONCLUSION

For the foregoing reasons, Microsoft's Motion to Modify Non-Disclosure Order is denied.

No later than August 30, 2019, 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.

Dated: Brooklyn, New York
July 31, 2019
As modified September 24, 2019

SO ORDERED:

Peggy Kuo
PEGGY KUO
United States Magistrate Judge