UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
NEW YORK REGIONAL OFFICE
BROOKFIELD PLACE
200 VESEY STREET, ROOM 400
NEW YORK, NY 10281-1022

Jorge G. Tenreiro
WRITER'S DIRECT DIAL
TELEPHONE: (212) 336-9145
TenreiroJ@sec.gov

January 10, 2020

Via ECF, Email, and Overnight Delivery

Hon. P. Kevin Castel
United States District Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: SEC v. Telegram Group Inc. & TON Foundation Inc., No. 19 Civ. 9439 (PKC)

Dear Judge Castel:

Plaintiff Securities and Exchange Commission ("SEC") respectfully renews its motion to compel Defendants to produce certain bank records. On January 6, 2020, the Court denied without prejudice the SEC's first such motion of December 26, 2019 (D.E. 52) (the "Motion"), but ordered Defendants to file a declaration setting forth a proposed schedule for a review of the requested records to ensure that production of such records complies with foreign data privacy laws (D.E. 58) (the "Order"). Defendants have since filed a vague affidavit that makes it impossible for the SEC or, we submit, the Court to weigh the true nature of the supposed burden of complying with foreign data privacy laws. These vague assertions of burden are, moreover, insufficient to rebut the presumption in favor of discovery that applies in federal courts even in the face of an assertion that foreign blocking statutes impede production. Telegram's vague submission reveals Telegram's broad, amorphous invocation of "data privacy" for what it is—a smokescreen aimed at improperly withholding relevant, responsive documents from the SEC.

I. There Is a Strong Presumption of Discoverability in U.S. Courts—Even of Evidence Otherwise Subject to Foreign Data Privacy Laws.

Over thirty years ago, the Supreme Court explained that "[i]t is well settled that [foreign data privacy] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." *Société Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, 482 U.S. 522, 544 n.29 (1987) ("*Aerospatiale*"). Instead, to successfully block discovery based on the applicability of a foreign data privacy statute, "the party resisting discovery must provide the Court with information of sufficient particularity and specificity to allow the Court to determine whether the discovery sought is indeed prohibited by foreign law." *Alfadda v. Fenn*, 149 F.R.D. 28, 34 (S.D.N.Y. 1993); *see also SEC v. Gib. Global Sec., Inc.*, 13 Civ. 2575, 2015 WL 1514746, at *2 (S.D.N.Y. Apr. 1, 2015) ("Where the alleged obstacle to production [of

documents] is foreign law, the burden of proving what that law is and demonstrating why it impedes production falls on the party resisting discovery.") (collecting Southern District of New York cases); *accord Laydon v. Mizuho Bank, Ltd.*, 183 F. Supp. 3d 409, 413 (S.D.N.Y 2016).

If the party opposing discovery actually shows a conflict with foreign privacy laws, a district court should then engage in the comity analysis set forth by the Supreme Court in *Aerospatiale*. Specifically, a court should then look to "(1) the importance to the litigation of the information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the relative interests of the United States and the foreign nation." *Gib. Global Sec.*, 2015 WL 1514746, at *4 (citing *Aerospatiale*, 482 U.S. at 544 n.28). "Courts in the Second Circuit also consider: (6) the hardship of compliance on the party or witness from whom discovery is sought; and (7) the good faith of the party resisting discovery." *Id.* (citing *Wultz v. Bank of China Ltd.*, 298 F.R.D. 91, 96 (S.D.N.Y. 2014)).

"The fifth-factor—the balancing of national interests—is the most important, as it directly addresses the relations between sovereign nations." *Gib. Global Sec.*, 2015 WL 1514746, at *5. This interest weighs in favor of the SEC in cases like this, because the United States has a strong interest in ensuring the integrity of its financial markets by enforcing the federal securities laws. *Mizuho Bank*, 183 F. Supp. 3d at 423.

II. Telegram's Vague Submission Prevents an Assessment of the *Aerospatiale* Factors.

Telegram's vague submission makes it impossible to assess any of the relevant factors and is thus insufficient to meet Telegram's burden. Telegram first asserts, generally, "that there are foreign persons identified in the [requested banking records]" and that producing them in this action "*may* implicate applicable foreign data privacy laws." Decl. of Eytan J. Fisch, dated Jan. 9, 2010, at ¶ 5 (D.E. 61) ("Fisch Decl.") (emphasis added). Defendants then complain that the analysis would include "determining the jurisdiction of each of the approximately 770 entities or individuals identified in the Records, and the nature of the relationship with each, to assess the extent to which foreign data privacy laws *may* be implicated." *Id.* at ¶ 6 (emphasis added). Defendants next state that fourteen jurisdictions are implicated for the 76 out of 770 entities or individuals whose jurisdiction they have already identified, that they have "already . . . performed" the data privacy analysis with respect to twelve of those jurisdictions, and that they have not done that work for the other two. *Id.* at ¶ 7. Defendants further conclude that they "*may* need to engage local counsel to conduct legal analysis of related data privacy issues" with respect to these jurisdictions. *Id.* (emphasis added).

Telegram has not provided sufficient information for the Court to determine whether a review for compliance with foreign data privacy laws is necessary. As the foregoing case law shows, to evaluate whether United States law should defer to foreign law and allow the withholding of otherwise relevant evidence, the Court should first engage in a conflicts-of-law analysis, which is multi-factored and requires specific facts. Here, Telegram has failed to provide information regarding the current location of the records, the original location of the records, and the original, intervening, and current custodian(s) of those records, all of which is necessary to the conflict-of-law analysis. Notably, Telegram does not even mention the names

of the foreign countries whose laws might apply, nor does it cite any specific data privacy laws. At his deposition two days ago, Mr. Durov, the CEO of a company holding approximately $1.3 billion of investor assets, similarly claimed [redacted] *See* Ex. A (Excerpts of Dep. of Pavel Durov, dated Jan. 7-8, 2020) at 283:17—284:9. The Court therefore cannot assess the threshold question of which country's data privacy laws may even apply to Telegram's handling of the data based on Telegram's vague submission.

The importance of identifying the location of the records is more than academic. The crux of the present dispute concerns the SEC's request for information about *payments Telegram made* from its bank accounts *to third parties.* Telegram's submission—insofar as it refers to the number of individuals and jurisdictions at issue—implies that the data privacy laws of every country *into which* Telegram made a payment, not the laws of the country *where the records reside*, controls the data privacy question or otherwise prohibits disclosure of that information. Telegram cites no legal principle, case, or international treaty to back this sweeping and broad interpretation of foreign data privacy statutes.

Moreover, even if the laws of recipient countries controlled, it is not clear why such payment information would be protectable. British blocking statutes, for example, do not prohibit the disclosure of personal data if "the disclosure is required by . . . any rule of law or by the order of a court or where the disclosure is necessary . . . for the purpose of, or in connection with, any legal proceedings . . . or for the purposes of establishing, exercising or defending legal rights." *Mizuho Bank*, 183 F. Supp. 3d at 415 (internal quotation marks omitted). German law appears to provide similar exceptions. *See BrightEdge Tech., Inc. v. Searchmetrics, GmbH*, No. 14 Civ. 01009, 2014 WL 3965062, at *4 (N.D. Cal. Aug. 13, 2014). Europe's General Data Protection Regulation ("GDPR"), *see* Regulation (EU) 2016/679, Apr. 27, 2016, 2016 O.J. (L119)1, appears to provide similar exceptions, *see* GDRP, Arts. 6(1)(c), 49(1), 49(1)(e), as well as an exception for information "necessary for important reasons of public interest." Br. of the European Comm'n on Behalf of the European Union as *Amicus Curiae* in *United States v. Microsoft Corp.*, No. 17-2, 2017 WL 6383224, at *15 (U.S. Dec. 13, 2017) (citing GDPR art. 49(1)(d)).[1] Finally, if the documents are already in the United States, as they appear to be given counsel's representations during the January 6 conference that Skadden "had" the records—confirmed by the statements of Mr. Fisch, Fisch Decl. ¶ 4—then this exercise is moot. Applying an *Aerospatiale* analysis to German and Swiss privacy protections, one district court has held "there is no question that the Federal Rules supply the correct procedure for obtaining evidence held by [the Defendant's U.S. entity]." *St. Jude Med. S.C. v. Janssen-Counotte*, 104 F. Supp. 3d 1150, 1167 (D. Or. 2015).

---

[1] The SEC understands that Switzerland (where Telegram banked before it switched its banking relationship after the filing of this suit) has privacy laws that are like the GDPR, but that it also affords privacy rights to legal entities like corporations. The SEC also understands that the Russian Federation's data privacy laws, particularly the Data Protection Act No. 152 FZ dated 27 July 2006, are similar, but that those contain exceptions for use for law enforcement purposes. *See* https://www.kramerlevin.com/en/perspectives-search/increased-fines-for-violations-of-russian-localization-law.html.

The *Aerospatiale* analysis therefore weighs unequivocally in favor of disclosure. The first factor weighs in favor of disclosure, because there is no question that Telegram's bank records are of critical relevance to this litigation. Defendants are correct that *Howey* mandates an objective test to determine whether investors in Grams had reasonable expectations of profits from their purchase. But it is equally true that post-investment actions by the parties "can serve as evidence" of the parties' expectations. *SEC v. Merchant Cap., LLC*, 483 F.3d 747, 760 (11th Cir. 2007); *see also SEC v. Arcturus*, 928 F.3d 400, 411 n.13 (5th Cir. 2019) (describing as "unpersuasive" contention that district court could not consider evidence of post-investment conduct to determine *Howey* analysis and collecting cases). Thus, how much Telegram may have *actually* spent on developing the TON Blockchain is relevant evidence that could support (or refute) the SEC's contention that Grams purchasers reasonably expected to profit based on Telegram's efforts. And, as the SEC has explained, whether Telegram made payments to third-parties to continue Telegram's own efforts in support of Grams after launch of the TON Blockchain would undermine Telegram's claims that secondary market purchasers of Grams have no reasonable expectation that they can profit based on Telegram's efforts through its subcontractors or proxies. As Telegram's own expert explained, "it is not uncommon for issuers and ecosystem foundations to remain involved in core protocol development and funding for external developers." *See* Ex. D (Excerpts of Expert Rep. of Stephen McKeon, dated Dec. 27, 2019) at ¶ 134. The record already shows evidence that Telegram has facilitated efforts with respect to the TON Blockchain by third parties. Such evidence includes a trademark license agreement with a particular entity, *see* Ex. B, whose principals have also been working as a [redacted] on pitches to third-party asset trading platforms to list Grams. *See* Ex. C.

The second *Aerospatiale* factor also weighs in favor of disclosure because the request is specific and narrow: it seeks only bank statements for a two-year period relating to three bank accounts. *See* Fisch Decl. ¶ 4 n.1. The fourth factor—the availability, or lack thereof, of alternative means to obtain the information—also weighs in favor of the SEC. For example, in Telegram's CEO's deposition, the SEC tried to obtain a breakdown of what expenses Telegram had made since the filing of this action. He answered: "I think I can try and extract this information from our bank records." Ex. A at 63:12—64:7. The fifth factor, the public interest of the United States, also weighs heavily in favor of disclosure in this civil action to enforce the federal securities laws. *See Gib. Global Sec.*, 2015 WL 1514746, at *5.

The seventh factor, the good faith of the party resisting discovery, may also weigh in favor of the SEC in view of the history of discovery in the litigation. For example, Telegram's expenses included a $1.2 million dollar payment in approximately August 2018 to a third-party, *see* Ex. E (Excerpts of Bank Wire Information, converted into PDF from original records) which appears to have engaged in an effort to sell Grams into the secondary market in 2019, as Telegram was aware. *See* Ex. F (Official translation of Russian originals procured by SEC). The SEC saw this payment only because it cleared through U.S. financial institutions. Even though in October the SEC had requested from Defendants all third-party agreements relating to the TON Blockchain, Defendants did not produce until today—only after the SEC had asked Mr. Durov about it at his deposition and on the eve of summary judgment—the relevant agreement between Telegram and that entity. *See* Ex. G.

Of the remaining *Aerospatiale* factors, the Court cannot assess the weight of the sixth factor—the level of hardship Telegram would suffer from compliance. In *Mizuho Bank*, however, the Court noted that because the Defendants had provided no instances in "which a UK enforcement action was taken against an entity for violating [their blocking statute] by complying with discovery demands in the United States; nor have they provided an instance where a UK financial institution was found liable for damages for producing otherwise confidential customer information pursuant to an order by a United States court." 183 F. Supp. 3d at 425. Nor can the Court weigh the third *Aerospatiale* factor, whether the information was generated in the United States, because even though the Court may assume for these purposes that some of the information was generated in Switzerland, Ex. A at 165:3-5, it is equally clear that Defendants cleared some of their third-party payments through the United States. *See* Ex. E.

United States federal courts routinely reject blanket assertions that materials are protected from production in discovery by European privacy laws. *See, e.g.*, *Knight Capital Partners Corp. v. Henkel AG & Co.*, 290 F. Supp.3d 681, 690-91 (E.D. Mich. 2017) ("It is well settled that [foreign 'blocking'] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute.") (*citing Aerospatiale,* 482 U.S. at 544).[2] Here, Telegram has not made even a threshold showing. Invoking the words "foreign data privacy" is not a talisman that exempts Telegram from its discovery obligations under the Federal Rules of Civil Procedure.

III. Telegram's Submission Does Not Establish A Disproportionate Burden.

Even if Telegram's approach to the foreign data privacy question were complete, its submission and the record make clear that the burden at issue is not insurmountable. As Telegram recognizes, it has already performed the analysis of foreign data privacy laws with respect to 12 of the 14 (or 85%) of the jurisdictions it identified. Defendants further contend that approximately 40% of its expenses are on "equipment," *see* Ex. H, but concede [redacted] Ex. A at 278:24—280:12; *see also id.* at 67:19-21 [redacted] Another 10% of Telegram's expenses consists of "colocation" fees, Ex. H, but Telegram's CEO explained that [redacted]. Ex. A at 282:24—283:16.

For these reasons, the SEC respectfully requests that the Court grant the motion to compel. The SEC does not object to a rolling production of records from Defendants or to excluding from the requested records payments by Telegram below a *de minimis* amount, such as $10,000.

Respectfully submitted,

Jorge G. Tenreiro

---

2 *See also Royal Park Investments SA/NV v. HSBC Bank USA, N.A.*, 2018 WL 745994, at *2 (S.D.N.Y. Feb. 6, 2018).