

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

**REPUBLIC OF THE GAMBIA,**

**Petitioner,**

**v.**

**FACEBOOK, INC.,**

**Respondent.**

**Miscellaneous Action No. 20-36 (JEB)**

**MEMORANDUM OPINION**

Republic of The Gambia is currently prosecuting in the International Court of Justice a case of genocide against Myanmar for its treatment of the Rohingya people. So how does this concern U.S. courts? The Gambia believes that critical evidence of the guilt of Myanmar officials lies in their posts and messages on Facebook, many of which the company took down in 2018 for contributing to the ethnic violence. Hoping to obtain the deleted material from these accounts to use in its prosecution of Myanmar, The Gambia filed an application under 28 U.S.C. § 1782 to take discovery from Facebook. While the company has agreed to turn over some of the desired records, it maintains that the Stored Communications Act prevents it from disclosing private accounts and associated content. Agreeing with Facebook, the Court will vacate the Magistrate Judge Order's requirement that it release the private communications.

**I. Background**

A. Factual Background

This case stems from an ongoing proceeding before the ICJ in which The Gambia seeks to hold Myanmar accountable for genocide against the Rohingya people, an ethnic and religious

minority in Myanmar. See ECF No. 27 (Pet. Response) at 3–4. As the details of that conflict are ably described in Magistrate Judge Zia Faruqui’s Order, see ECF No. 22 (MJ Order) at 2–6, the Court need not recount them in depth here. Instead, it will focus on the facts most relevant to The Gambia’s ancillary dispute with Facebook.

To aid its prosecution of Myanmar in the ICJ, The Gambia seeks to acquire information from several Facebook and Instagram accounts believed to have been run by Myanmar officials and used to spread “anti-Muslim, anti-Rohingya, and anti-activist sentiment” that contributed to the genocide. See Pet. Resp. at 4–5 (citation omitted). Facebook and its constituent apps (including Instagram) allow users to communicate through public and private postings, as well as through direct-messaging services like Facebook Messenger. See ECF No. 24 (Resp. Objections to MJ Order) at 8–9. “In countries like Myanmar, in particular, many users rely on Facebook for most of their personal communications.” Id. at 9 (citing U.N. Human Rights Council, Report of the Independent International Fact-Finding Mission on Myanmar, ¶ 74, U.N. Doc. A/HRC/39/64 (Sept. 12, 2018)).

Recognizing that its platform and apps had potentially played a role in ethnic violence against the Rohingya, Facebook removed numerous accounts and pages in 2018. For example, in August of that year, it announced the removal of “18 Facebook accounts, one Instagram account and 52 Facebook Pages, followed by almost 12 million people.” Id. at 10 (quoting Removing Myanmar Military Official from Facebook, Facebook (Aug. 18, 2018, last updated Dec. 18, 2018), <https://bit.ly/3G9IHWm> (Removal Post)). The company determined that several of these pages and accounts had engaged in “coordinated inauthentic behavior on Facebook, meaning they used seemingly independent news and opinion Pages to covertly push the messages of the Myanmar military.” Id. (citation and internal quotation marks omitted). In

October and December 2018, Facebook removed another 425 pages, 17 Facebook groups, 135 Facebook accounts, and 15 Instagram accounts for coordinated inauthentic behavior. Id. Many of these pages were inconspicuous — some of the most popular were titled “Beauty and Classic,” “Let’s Laugh Casually,” and “All About Myanmar”— but Facebook determined that they “were in-fact covert accounts linked to the Myanmar military.” Pet. Resp. at 5 (internal quotation marks and citation omitted). Critically, when Facebook removed these pages and accounts, it preserved the content it had deleted. Id. at 6; see Resp. Objections at 10.

Some of this content was maintained at the request of the Independent Investigative Mechanism for Myanmar (IIMM), a body created by the U.N. Human Rights Council to “collect evidence of the most serious international crimes and violations of international law and prepare files for criminal prosecution.” Resp. Objections at 11 (quoting U.N. Human Rights Council, Independent Investigative Mechanism for Myanmar, <https://bit.ly/31jHDjj>). Facebook has subsequently shared some of the content with the IIMM; to date, it has made 13 productions totaling approximately 1.5 million pages of documents and is engaged in ongoing dialogue to respond to additional requests. Id. at 12. The IIMM, however, “has no power to hold Myanmar accountable for the genocide of the Rohingya,” Pet. Resp. at 3 n.1, which brings the Court back to The Gambia’s request.

#### B. Procedural History

The Gambia filed an Application to take discovery from Facebook under 28 U.S.C. § 1782 on June 8, 2020. See ECF No. 1 (Pet. Application). That section empowers district courts to order an individual or entity to “give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal . . . upon the application of any interested person.” 28 U.S.C. § 1782(a). The Gambia’s Application sought to

obtain “evidence indicating the involvement of Myanmar State officials and entities, or those affiliated with State officials and entities, in spreading anti-Rohingya hate speech on Facebook, including the content of related Facebook accounts and evidence of coordinated activity,” which Petitioner could then submit to the ICJ in support of its claims against Myanmar. See Pet. App. at 14. Specifically, The Gambia requested 12 discrete categories of documents and communications associated with pages and accounts linked to Myanmar government officials. Id. at 14–17. It also requested documents relating to Facebook’s investigation that led to its conclusion that the removed accounts had engaged in coordinated inauthentic behavior, as well as a Fed. R. Civ. P. 30(b)(6) deposition. Id. at 17. This Court referred the Application to Magistrate Judge Faruqui for full case management on June 9, 2020. See ECF No. 2 (Order Referring to MJ).

After briefing and a six-hour hearing, Magistrate Judge Faruqui issued a well-written and thorough Order granting in part and denying in part The Gambia’s Application on September 22, 2021. See MJ Order. He rejected Facebook’s arguments that the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*, prohibited it from releasing much of the requested content. See MJ Order at 7–19. A subsequent weighing of the § 1782 factors, additionally, led him to conclude that discovery was appropriate. Id. at 23–28. He also ordered Facebook to produce any non-privileged documentation relating to its internal investigation. Id. at 28–29. The Order declined to grant The Gambia’s request for a Rule 30(b)(6) deposition, however, finding it “unduly burdensome.” Id. at 29.

Facebook filed its Objections to the Magistrate Judge Order on October 13, 2021. See Resp. Objections. After receiving a Response from The Gambia and a further Reply from Facebook, see ECF Nos. 27 & 28 (Repl.), this Court held a hearing to clarify what remains in

dispute. See Minute Entry of November 12, 2021. Given that Facebook has now committed to produce public postings — *e.g.*, postings that anyone on Facebook can view — and associated metadata, the parties there agreed that the Court should address at this juncture only the question of whether private pages and communications — *e.g.*, direct messages between users — may be disclosed to The Gambia pursuant to a § 1782 subpoena.

## **II. Legal Standard**

A district court’s review of objections to a magistrate judge order is governed by Fed. R. Civ. P. 72. When reviewing non-dispositive orders, a court must “set aside any part of the order that is clearly erroneous or is contrary to law.” Fed. R. Civ. P. 72(a). The “clearly erroneous” standard provides for deferential review of factual findings, but the “contrary to law” standard “permits *de novo* review of a magistrate judge’s legal conclusions.” American Center for Civil Justice v. Ambush, 794 F. Supp. 2d 123, 129 (D.D.C. 2011) (citations omitted). Review of objections to dispositive motions, conversely, is governed by Rule 72(b), which provides that courts should conduct *de novo* review of any part of a magistrate judge’s order to which a party has objected. See Fed. R. Civ. P. 72(b)(3). Since the Court now confronts only objections to the Order’s legal conclusions, whether such Order is considered non-dispositive or dispositive — a question that appears to remain open in this district — is of no consequence. The Court will thus apply *de novo* review.

## **III. Analysis**

Facebook proffers two types of objections to the Order’s determination that The Gambia may obtain the private pages and communications pursuant to a § 1782 subpoena: 1) the SCA prohibits Facebook from disclosing these communications, even if it wishes to do so, and 2) the

Magistrate Judge abused his discretion in granting the § 1782 subpoena if the SCA does not block disclosure. See Resp. Objections at 19–37. The Court need take up only the first here.

A. Stored Communications Act

In challenging the Order, Facebook’s primary contention is that the SCA prohibits its disclosure of the deleted private pages and communications stored on its servers. The Court provides a brief overview of the Act’s statutory framework before assessing its applicability to the communications at issue.

1. *Statutory Background*

One of the difficulties this case presents is the interpretation of a communications statute enacted before the arrival of social media, smartphones, and the modern Internet. Passed in 1986, the SCA “creates a set of Fourth Amendment-like protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private information.” Orin S. Kerr, A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1212 (2004). It does so by limiting service providers’ knowing disclosure of stored electronic communications, see 18 U.S.C. § 2702, and imposing procedural requirements on the Government’s attempts to compel disclosure from these providers. See 18 U.S.C. § 2703. Its protections apply to content held by two types of service providers: providers of an “electronic communication service” (ECS), defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications,” 18 U.S.C. § 2510(15), and providers of a “remote computing service” (RCS), which “means the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

The Act prohibits both ECS and RCS providers from “knowingly divulg[ing] to any person or entity” certain communications. See 18 U.S.C. § 2702(a). ECS providers may not disclose any communication held “in electronic storage.” 18 U.S.C. § 2702(a)(1). “Electronic storage” is defined as:

- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
- (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]

18 U.S.C. § 2510(17). RCS providers, similarly, may not divulge communications maintained on their service “on behalf of . . . a subscriber or customer . . . solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents” for any other purpose. See 18 U.S.C. § 2702(a)(2)(A)–(B). Two distinctions are thus critical here in determining whether a communication is protected by the SCA’s disclosure prohibition: first, whether the possessing provider is an ECS or RCS (or neither), and, second, if the former, whether the communication is in “electronic storage.”

## *2. Application to Provider-Deleted Private Communications*

In their briefing before this Court, the parties seem to agree both that Facebook is an ECS with respect to the content at issue (setting aside whether it may also be an RCS) and that this content does not fall within the “temporary storage” category (subsection A) of “electronic storage,” and they also do not contest that “electronic storage” includes two discrete types of protected communications. See Pet. Resp. at 19; Resp. Objections at 20; Hately v. Watts, 917 F.3d 770, 784 (4th Cir. 2019) (noting majority of courts have found that subsections (A) and (B) identify “two discrete types” of protected communications). Their squabble thus boils down to one basic question: whether the deleted private pages and communications are stored “for

purposes of backup protection” (subsection B). See 18 U.S.C. § 2510(17). To frame the question narrowly, however, does little to aid its resolution. Indeed, it raises a matter of first impression in both this district and elsewhere, at least as far as the Court and parties are aware.

Facebook argues that the content it possesses consists of copies of pages and messages retained to protect the communications from destruction, which fits squarely within the plain meaning of “for purposes of backup protection,” and that a contrary holding would undermine the SCA’s purpose and have grave implications for electronic privacy. See Resp. Objections at 19–27. The Gambia, agreeing with the Magistrate Judge’s Order, rejoins that deleted content stored on Facebook’s servers cannot be a “backup” when the original no longer exists, and that a narrow definition of SCA-protected communications is in line with the Act’s intent to provide only a limited set of protections. See Pet. Resp. at 18–23.

The SCA does not define “backup protection,” and so the Court turns, as it must, to the plain meaning of the text. See Ross v. Blake, 578 U.S. 632, 638 (2016); Blackman v. District of Columbia, 456 F.3d 167, 176 (D.C. Cir. 2006). “The most relevant definition of ‘backup’ is ‘a copy of computer data.’” Hately, 917 F.3d at 791 (emphasis in original) (quoting Backup, Merriam-Webster.com (last visited Feb. 26, 2019)). “Backup” is also defined as “[a] reserve or substitute.” Backup, The American Heritage Dictionary of the English Language (3d ed. 1992) (published six years after SCA’s passage). “Protection” is “the act of protecting,” which is defined, in turn, as “keep[ing] from being damaged, attacked, stolen, or injured.” Protection, id.; Protect, id. A communication is stored “for purposes of backup protection,” then, when it is a “copy” or “reserve” held to prevent it being “damaged” or lost. See Hately, 917 F.3d at 791.

Copies of the deleted private accounts and pages, and the communications associated with them, fall within this definition. When it deleted these pages and accounts, Facebook



“preserv[ed] data, including content, on the accounts and Pages [it] . . . removed.” Removal Post. “Facebook stored a duplicate of these communications, among other reasons, in case it was lawfully called upon to produce them by an international body like the United Nations after their removal.” Resp. Objections at 20 (citing ECF No. 19 (Hearing Transcript) at 80:17–81:25). Such storage was not unusual, as Facebook routinely stores removed communications “in case a user petitions Facebook successfully to restore their account to the platform.” Id. at 20–21 (citing Hearing Transcript at 151:3–15). These duplicates “exist[] on the same servers, in the same place, in the same format, . . . in exactly the same manner” as they did before the accounts and pages were removed. See Hearing Transcript at 76:4–11. That constitutes a “copy” or “reserve” of communications stored to prevent their loss or destruction. As a result, Facebook’s storage of these communications “literally falls within the statutory definition” of “for purposes of backup protection.” Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004).

The Gambia protests that the common understanding of “backup” requires the existence of an original; in other words, if the original is deleted, the backup then becomes the primary. See Pet. Resp. at 18–23; see also Jennings v. Jennings, 736 S.E. 2d 242, 245 (S.C. 2012) (“Congress’s use of ‘backup’ necessarily presupposes the existence of another copy to which this e-mail would serve as a substitute or support.”). But dictionary definitions of “backup” require no such thing; indeed, the idea that a backup is a copy or reserve seems to contemplate the potential loss of any “original.” The statute also imposes no requirement that there be an original copy of the communication in order for other material to qualify as backup. See 18 U.S.C. § 2510(17)(B). Indeed, as the Fourth Circuit has noted, “[R]elying on definitions of ‘backup’ that define the term relative to an ‘original’ makes little sense in the context of messages stored by electronic communication services.” Hately, 917 F.3d at 796. In this context, “the ‘original’

would seem to be most readily understood as the copy of a message that a sender types into his email client,” and even the recipient receives only a copy of that message. Id. (emphasis in original). “Put differently, all copies of an email held by a recipient’s email service . . . are ‘copies,’ rather than ‘originals.’” Id. The same appears true for copies of the private communications at issue here.

This reading of “backup purposes,” moreover, comports with the SCA’s legislative context. Congress enacted the SCA to fill a gap in privacy protections for electronic stored communications, which were not protected by either existing federal statutes or the Fourth Amendment. Id. at 782 (citing H.R. Rep. No. 99-647, at 18 (1986) and S. Rep. No. 99-541, at 2 (1986)); see also Kerr, 72 Geo. Wash. L. Rev., at 1209–13. The uncertainty associated with this gap generated three problems Congress sought to address: 1) “it may unnecessarily discourage potential customers from using such [innovative communications] systems”; 2) it might “encourage unauthorized users to obtain access to communications to which they are not a party”; and 3) “most important,” it may lead to “the gradual erosion of a precious right [to privacy].” H.R. Rep. No. 99-647, at 19; see also S. Rep. No. 99-541, at 5. In enacting the SCA, “Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards,” Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002), in order to avoid hindering the adoption of new communications technologies.

Interpreting Congress’s definition of “for purposes of backup protection” to include provider-deleted communications is in keeping with these objectives. The counterfactual illustrates the point. Under a definition of “electronic storage” that excluded provider-deleted communications, an ECS like Facebook could avoid the SCA’s disclosure prohibition simply by

deactivating a user’s account. That would hand Facebook the SCA-on/off switch: it could remove an account or page (which Facebook does without government supervision) and distribute the associated content freely — *e.g.*, to the government or even to other private parties. See Resp. Objections at 26; see also Orin Kerr (@OrinKerr), Twitter (Sept. 24, 2021, 1:32 AM), <https://bit.ly/31k2Lpg>. Such a scheme would surely “discourage” individuals from using electronic-communications systems and risk “the gradual erosion of [the] precious right [to privacy].” H.R. Rep. No. 99-647, at 19; S. Rep. No. 99-541, at 5. It would also “lead[] to an arbitrary and untenable ‘gap’ in the legal protection of electronic communications,” Hately, 917 F.3d at 798 (citing S. Rep. No. 99-541, at 5), and the Court “do[es] not believe Congress intended such an absurd result when it enacted a statute intended to fill in the gaps in the then-existing privacy protections for electronic communications.” Id.

The House Report, furthermore, reveals that Congress intended the SCA’s protections to extend to backup copies not unlike those at issue in this case. Discussing § 2702 and other provisions, the Report contemplates the SCA’s application to copies of communications stored by service providers, separate and apart from those a user elects to store:

Even if the subscriber reads the message and discards or deletes it, the system maintains it as a backup copy for system maintenance and integrity purposes. These records are retrievable and the Committee intends that subscribers and customers be afforded some protection as to these records. Therefore, a provider of electronic communications to the public such as an electronic mail service may not disclose the contents of stored communications unless one of the statutory exceptions in 2702(b) apply.

H.R. Rep. No. 99-647, at 72. Although this passage does not clarify whether the House intended these communications to find protection under the ECS or RCS provision of the SCA, the language used — “backup copy” held by a “provider of electronic communications” — suggests that it anticipated that these communications would fall within the “backup protection” category

of “electronic storage” held by an ECS. Like the stored communications at issue here, those referenced above are copies stored by the service provider for its own purposes, rather than for the benefit of, or at the choice of, the user. Cf. Hately, 917 F.3d at 796–97 (communications may be stored for purposes of backup protection whether stored for benefit of user or service provider) (citing Theofel, 359 F.3d at 1075). If Congress wished to protect these provider-stored communications even after the user chose to delete them, it would make little sense for that protection to lapse when the provider made the decision to remove them, as occurred here. That would grant providers power inconsistent with the SCA’s goal to restrict their ability to disclose user communications.

The Gambia rejoins that Facebook’s policy concerns are overblown and encourages this Court to follow cases that have interpreted “backup” in the context of undeleted content. See Pet. Resp. at 18–23. Even under those decisions, however, much of the content at issue here — namely, Facebook and Instagram posts — would appear to be stored “for purposes of backup protection” if the posts were undeleted. See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010) (holding that Facebook posts are stored “for purposes of backup protection” under SCA by analogizing to electronic bulletin boards specifically discussed in SCA’s legislative history). The private Facebook messages and Instagram direct messages, conversely, pose a more difficult question, as courts are split on whether opened, undeleted messages fall within the definition of “electronic storage.” See Cheng v. Romo, 2013 WL 6814691, at \*3 (D. Mass. Dec. 20, 2013) (collecting cases and noting disagreement); see also Crispin, 717 F. Supp. 2d at 987 (applying email-message precedent to Facebook messages). Although some courts hold that such messages are not stored “for purposes of backup protection,” see Sartori v. Schrodtt, 424 F. Supp. 3d 1121, 1132–33 (N.D. Fl. 2019) (collecting

cases), the Fourth and Ninth Circuits have disagreed. See Hately, 917 F.3d at 797 (concluding that opened emails stored by web-based email service were stored for purposes of backup protection); Theofel, 359 F.3d at 1077 (same as to non-web-based email service). And at least one court has suggested that even if the copies of these opened messages available to the users are not in backup storage, “copies of webmail or private messaging communications on [providers’] servers separate from the storage available to [the user] . . . would plainly be [stored] for backup purposes.” Crispin, 717 F. Supp. 2d at 987 n.46. It remains unsettled, therefore, whether the private messages would be stored for backup protection if they were undeleted.

As the reader can readily discern, no clear thread ties these decisions together, nor is there any D.C. Circuit precedent to follow. More important, no case bears directly on the issue at hand, as all involve undeleted content, in contrast to the provider-deleted content here. That distinction matters. As evidenced by the House Report excerpted above, Congress may well have anticipated that copies of deleted content would be treated differently under the SCA from copies of content still available to — and within the control of — the user. That is especially so when the content has been removed by the provider. See supra, at 11–12. The Court therefore finds that the Gambia’s case citations provide no basis to reach a different outcome here.

It consequently holds that private Facebook and Instagram pages and their associated communications that have been deleted by Facebook and are maintained on its servers to prevent their destruction are stored “for purposes of backup protection” under the plain meaning of those words. Those communications are therefore in “electronic storage” by an “electronic communication service,” and § 2702(a)(1) of the Stored Communications Act prohibits their disclosure to The Gambia.

#### B. Remaining Issues

Having so concluded, the Court need not address Facebook's remaining objections to the Magistrate Judge's Order. It also declines to consider The Gambia's alternative grounds for sustaining the Order, as they are not presented as objections to any specific portion of the Order. See Klayman v. Judicial Watch, Inc., 628 F. Supp. 2d 98, 102 (D.D.C. 2009) (court may reject arguments that fail to comply with Local Rule 72.2(b)'s requirement that party specifically object to parts of magistrate judge order). Finally, the Court does not reach the parties' arguments regarding the scope of the subpoena or the request for a Rule 30(b)(6) deposition, as both sides have agreed that those are best put on hold pending their discussions about the disclosure of the public information and non-content metadata.

#### IV. **Conclusion**

For the foregoing reasons, Facebook's objections to the Magistrate Judge Order's determination that the private communications are not in "electronic storage" will be sustained, and the Order will be vacated to the extent it is inconsistent with this Opinion. A separate Order so stating will issue this day.

*/s/ James E. Boasberg*  
JAMES E. BOASBERG  
United States District Judge

Date: December 3, 2021