UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

***In re* Application Pursuant to 28 U.S.C. § 1782 of** **The Republic of the Gambia,** **Petitioner,** **v.** **Facebook, Inc.,** **Respondent.**	**Civil Action No. 20-mc-36-JEB-ZMF**

ORDER

I come to praise Facebook, not to bury it. By Facebook's own admission it was "too slow to respond to the concerns raised" about its role in the genocide of the Rohingya, an ethnic and religious minority in Myanmar. Steve Stecklow, *Why Facebook is losing the war on hate speech in Myanmar*, Reuters (Aug. 15, 2018), https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/. In 2018, roughly six years into the genocide, Facebook began deleting accounts and other content from its platform used by Myanmar government agents that sparked the genocide. *See Removing Myanmar Military Officials From Facebook*, Facebook (Aug. 28, 2018), https://about.fb.com/news/2018/08/removing-myanmar-officials/ (last updated Dec. 18, 2018) ("De-platforming Post").

Pursuant to 28 U.S.C. § 1782, The Republic of The Gambia ("The Gambia") seeks the content Facebook deleted for use in The Gambia's litigation against the Republic of the Union of Myanmar ("Myanmar") at the International Court of Justice ("ICJ"). The Gambia seeks these records for "evidence of genocidal intent necessary to support a finding of responsibility for

genocide" of the Rohingya. *See* ECF No. 1, Ex. 1 (Pet'r's Mot.) at 8. Facebook argues that The Gambia's request: (1) violates the Stored Communications Act ("SCA"), and (2) is unduly burdensome. *See* ECF No. 8 (Resp't's Opp'n). After several rounds of briefing, The Gambia's motion is now ripe for resolution.[1] The Court GRANTS The Gambia's application in part and DENIES it in part.

I. BACKGROUND

A. Rohingya Genocide

In November 2019, The Gambia instituted proceedings against Myanmar at the ICJ. *See* Pet'r's Mot. at 1. The Gambia seeks to hold Myanmar accountable for the crime of genocide against the Rohingya.[2] *See id.* The ICJ has jurisdiction to adjudicate disputes over the responsibility of a State for genocide under the 1948 Convention on the Prevention and Punishment of the Crime of Genocide. *See id.* at 6.

According to the Independent International Fact-Finding Mission on Myanmar of the United Nations Human Rights Council ("U.N. Mission"), the Rohingya were "in a situation of severe, systemic and institutionalised oppression from birth to death" due to "State policies and

[1] On June 8, 2020, The Gambia filed its discovery request. *See* ECF. No. 1 (Order). On June 9, 2020, Judge James E. Boasberg referred this case to a magistrate judge for full case management. *See* Minute Order (June 9, 2020). "Since the Court's decision on a Section 1782 application is non-dispositive, it may be decided by a magistrate judge by opinion and order, rather than a report and recommendation to the district court." *Food Delivery Holding 12 S.a.r.l. v. DeWitty & Assocs. CHTD*, No. 21-mc-5, 2021 WL 1854343, at *1 n.2 (D.D.C. May 10, 2021) (quoting *In re Application of Shervin Pishevar Pursuant to 28 U.S.C. § 1782*, 439 F. Supp. 3d 290, 301 (S.D.N.Y. 2020); *see also see also In re Pons*, —— F. Supp. 3d ——, 2020 WL 1860908, at *3 (S.D. Fla. 2020) ("The great majority of courts to address the issue" have determined that a magistrate judge may dispose of "Section 1782 discovery motions" by order; collecting cases); *In re Hulley Enters. Ltd.*, 400 F. Supp. 3d 62, 71 (S.D.N.Y. 2019) (same).

[2] That proceeding is styled as *The Gambia v. Myanmar (Application of the Convention on the Prevention and Punishment of the Crime of Genocide).*

practices implemented over decades." *Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar*, A/HRC/39/CRP.2 at ¶ 458, United Nations Human Rights Council (Sept. 17, 2018) ("U.N. Report"). "The Myanmar military and other security forces committed human rights violations on a colossal scale, in violation of all basic tenets of international law. The operations had a devastating impact on the Rohingya civilian population, which was targeted, brutalised and terrorised." *Id.* at ¶ 883. Indeed, the "level of oppression faced by the Rohingya is hard to fathom." *Id.* at ¶ 622. "[T]his oppressive climate, and the fear and desperation resulting from it," are the context for the "episodes of violence in 2012, 2016 and 2017." *Id.* at ¶ 622.

In 2012, violence erupted in the Rakhine State, where the Rohingya Muslims lived. *Id.* at ¶ 624. "The violence saw the burning and looting of houses, murders, summary executions and large-scale displacement affecting both ethnic Rakhine and Muslims." *Id.* at ¶ 643. The U.N. Mission "conclude[d] that the 2012 and 2013 violence in Rakhine State was pre-planned and instigated and that the Myanmar security forces were actively involved and complicit." *Id.* at ¶ 747.

Beginning in October 2016, the Myanmar military carried out so-called "clearance operations" constituting systematic mass executions, disappearances, detention, and torture of Rohingya civilians, and the destruction of homes, mosques, and Qurans. *See id.* at ¶¶ 1069–95. "In addition to . . . mass targeted killings, members of the security forces shot individual persons, including at point blank range, and executed people, including those injured, by slitting their throats using long knives." *Id.* at ¶ 893. "Infants and children were frequently killed by gunfire, stabbed or burned to death." *Id.* at ¶ 942. "Another feature of the 'clearance operations' was the widespread destruction of Rohingya homes and villages, causing further death and injury through

burning. . . . Death by burning in this manner disproportionately affected vulnerable persons less able to run and escape from the 'clearance operations,' including the elderly, disabled, young children and pregnant women." *Id.* at ¶ 905. Myanmar military forces "perpetrated on a massive scale" "[r]ape and other sexual and gender-based violence . . . includ[ing] mass gang rapes, sexually humiliating acts, sexual slavery and sexual mutilations." *Id.* at ¶ 920. "Many of the women and girls had infants and children with them, who were killed or severely injured, while their mothers were raped." *Id.* at ¶ 924. "Many victims were killed after being raped. Most had their throats slit, or were burned to death." *Id.* at ¶ 927.

The U.N. Mission concluded Myanmar intended to eradicate the Rohingya. *Id.* at ¶¶ 1439–41. Multiple other international human rights organizations likewise concluded that Myanmar's actions constituted genocide. *See* Pet'r's Mot. at 4–6.

B. Facebook's Role In The Genocide

The U.N. Mission found that Facebook has been "by far the most common social media platform in use in Myanmar" since 2012. U.N. Report at ¶ 1344. "Facebook [was] the main, if not only, platform for online news." *Id.* at ¶ 1345. The Myanmar officials "rel[ied] on Facebook to release news and information" and media outlets "use[d] Facebook as a main way of disseminating articles." *Id.*

In October 2018, Facebook commissioned a human rights impact assessment (HRIA)[3] of its presence in Myanmar. It too revealed that, in Myanmar, "Facebook is the internet." HRIA at

[3] Facebook commissioned BSR to author the HRIA using a methodology based on recognized international principles. The assessment identified actual and potential human rights impacts, reached conclusions about those impacts, and made recommendations for mitigation and management. Although Facebook funded the HRIA, BSR retained editorial control over its contents. *See* BSR, *Human Rights Impact Assessment: Facebook in Myanmar*, 1 (2018), https://about.fb.com/wp-content/uploads/2018/11/bsr-facebook-myanmar-hria_final.pdf ("HRIA").

12. Undoubtedly Facebook had "a powerful democratizing effect in Myanmar by exposing millions of people to concepts like democracy and human rights." *Id.* However, "[d]igital literacy [was] generally low across the country, and many people [found] it difficult to verify or differentiate content (for example, real news from misinformation)." *Id.* Myanmar officials were therefore able to credibly "spread rumors about people and events" via Facebook. *Id.* at 13.

Facebook content "contributed to shaping public opinion on the Rohingya and Muslims more generally," U.N. Report at ¶ 696, and was used "to spread anti-Muslim, anti-Rohingya, and anti-activist sentiment," HRIA at 24. Specifically, "organized groups [made] use of multiple fake accounts and news pages to spread hate speech, fake news, and misinformation for political gain." *Id.* at 13. The viral spread of disinformation on Facebook led to instances of "communal violence and mob justice." *Id.*

The U.N. Mission concluded that Myanmar officials weaponized Facebook for "a carefully crafted hate campaign [to] develop[] a negative perception of Muslims among the broad population in Myanmar." U.N. Report at ¶ 696. This hate campaign portrayed "the Rohingya and other Muslims as an existential threat to Myanmar and to Buddhism. In the case of the Rohingya, it [went] a step further. It [was] accompanied by dehumanising language and the branding of the entire community as 'illegal . . . immigrants.'" *Id.* For example, on June 1, 2012, Zaw Htay, the spokesperson for the President of Myanmar, posted a statement advocating for the destruction of the Rohingya to his personal Facebook account:

> Rohingya terrorists as members of the [Rohingya Solidarity Organization] are crossing the border into Myanmar with weapons. . . . Our troops have received the news in advance so they will completely destroy them [the Rohingya]. It can be assumed that the troops are already destroying them [the Rohingya]. We don't want to hear any humanitarian or human rights excuses. We don't want to hear your moral superiority, or so-called peace and loving kindness. (Go and look at Buthidaung, Maungdaw areas in Rakhine State. Our ethnic people are in constant fear in their own land. I feel very bitter about this. This is our country. This is our

> land.) (I'm talking to you, national parties, MPs, civil societies, who are always opposing the President and the Government.)

Id. at ¶ 705. The U.N. Mission determined that "[a]lthough this post was later deleted, the impact of a high[-ranking] official equating the Rohingya population with terrorism may have been significant ahead of the 2012 violence, which erupted a week later." *Id.* at ¶ 706. Ultimately, "[t]his discourse created a conducive environment for the 2012 and 2013 anti-Muslim violence . . . and subsequent waves of State-led violence in 2016 and 2017." *Id.* at ¶ 696.

In August 2018, Facebook acknowledged that the "ethnic violence in Myanmar [was] horrific" and that Facebook was "too slow to prevent misinformation and hate." Sara Su, *Update on Myanmar*, Facebook (Aug. 15, 2018), https://about.fb.com/news/2018/08/update-on-myanmar/. In August 2018, Facebook deleted and banned the accounts of key individuals and organizations in Myanmar—including the commander-in-chief of Myanmar's armed forces and the military's television network. *See* De-platforming Post. Facebook also deleted "seemingly independent news and opinion Pages [that] covertly push[ed] the messages of the Myanmar military." *Id.* Facebook determined that Myanmar officials surreptitiously controlled these facially unassociated accounts, which qualified as "coordinated inauthentic behavior" in violation of Facebook's terms of service. *Id.*

In October and December 2018, Facebook deleted an additional 438 pages, 17 groups, and 160 Facebook and Instagram accounts, *see id.*, for engaging in "coordinated inauthentic behavior" designed to perpetuate misinformation and hate speech targeting the Rohingya, *see* U.N. Report ¶ 1353. Facebook estimated that nearly 12 million people followed these accounts, groups, and pages prior to deletion. *See* De-platforming Post. In taking these actions, Facebook sought to "act against those [who] use[d] Facebook in ways that spread violence and enable[d] genocide." HRIA at 27. Facebook preserved the content it deleted. *See id.*

The Gambia makes three discovery requests: (1) public and private communications associated with the deleted content; (2) documents associated with Facebook's internal investigation on how Facebook identified the content it deleted; and (3) a Rule 30(b)(6) deposition regarding all of the above. *See* Pet'r's Mot. at 14–17.

II. LEGAL STANDARD

A. 28 U.S.C. § 1782

"The district court of the district in which a person resides or is found may order him 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." 28 U.S.C. § 1782. Consideration of a § 1782 application requires a two-step inquiry. "A court must first consider whether it has the authority to grant the request and, second, whether it should exercise its discretion to do so." *In re Barnwell Enters. Ltd*, 265 F. Supp. 3d 1, 8 (D.D.C. 2017) (cleaned up). The statutory elements are that (1) the person resides or is found in the district, (2) the discovery requested will be used in a proceeding before a foreign or international tribunal, and (3) the request is made by an interested person. *See id.* at 8–9. "As long as these three mandatory factors are met, courts have broad discretion in deciding whether to grant or deny these applications." *Attorney Gen. of British Virgin Islands v. Hyman*, No. 19-mc-164, 2020 WL 2615519, at *4 (D.D.C. May 23, 2020).

A court must evaluate whether it should exercise its discretion according to four prudential guidelines: (1) whether the respondent is a participant in the international proceedings, (2) whether the tribunal is resistant to using this kind of discovery, (3) whether the application circumvents the tribunal's proof-gathering restrictions, and (4) whether the requested discovery is unduly intrusive or burdensome. *See Intel Corp. v. Adv. Micro Devices, Inc.*, 542 U.S. 241, 255 (2004). "The discretionary guidelines in *Intel* do not command that each factor be weighed equally, nor do they

dictate whether any particular factor should take precedent." *In Matter of Application of Leret*, 51 F. Supp. 3d 66, 71 (D.D.C. 2014). They merely "suggest guides for the exercise of district-court discretion." *Intel*, 542 U.S. at 263 n.15. "A court's discretion to grant or deny a § 1782 application is 'considerable,' and may appropriately take into account the 'specific facts of [the] application' to determine which factor or factors 'to weigh most heavily.'" *In re Ord. of Hulley Enters. Pursuant to 28 U.S.C. §1782*, No. 17-mc-1466, 2017 WL 3708028, at *4 (D.D.C. Aug. 18, 2017) (quoting *Lazaridis*, 473 F. App'x at 4). "'[D]istrict courts must exercise their discretion under § 1782 in light of the twin aims of the statute,' which have been described as 'providing efficient means of assistance to participants in international litigation in our federal courts and encouraging foreign countries by example to provide similar means of assistance to our courts.'" *Norex Petroleum Ltd. v. Chubb Ins. Co. of Canada*, 384 F. Supp. 2d 45, 49 (D.D.C. 2005) (quoting *Schmitz v. Bernstein Liebhard & Lifshitz, LLP*, 376 F.3d 79, 84 (2d Cir. 2004)).

B. Stored Communications Act

"[I]t is well-established that civil subpoenas, including those issued pursuant to 28 U.S.C. § 1782, are subject to the prohibitions of the [SCA]." *Optiver Australia Pty. Ltd. & Anor. v. Tibra Trading Pty. Ltd. & Ors.*, No. C12-80242, 2013 WL 256771, at *1 (N.D. Cal. Jan. 23, 2013). The SCA mandates that "a person or entity providing an electronic communication service [("ECS")] to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702. Classification of an ECS is "context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract." 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, 1215 (2004).

III. ANALYSIS

A. SCA Applicability

1. *SCA Background*

Congress passed the SCA in 1986, prior to the existence of modern-day social media. *See* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1204–05 (2010). "To apply the [SCA] to modern computing, courts need to begin by" looking to the legislative history for the "problems that prompted the need for the legislation." *Id.* Congress was concerned that the absence of a clear statutory framework regarding new communication technologies (1) "unnecessarily discouraged potential customers from using innovative communications systems," (2) "encouraged unauthorized users to obtain access to communications to which they are not a party," and (3) "promote[d] the gradual erosion of the precious right to privacy." S. Rep. No. 99-541, at 5 (1986); *see also Hately v. Watts*, 917 F.3d 770, 783 (4th Cir. 2019) (detailing legislative history).

Yet, "there are many problems of Internet privacy that the SCA [did] not address. The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer networks." *Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 839 (8th Cir. 2015) (quoting 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, 1214 (2004)).

2. *Protected User*

The Gambia argues that Myanmar officials are not protected "users"[4] under the SCA. *See* ECF No. 10 (Pet'r's Reply) at 5–8. This is an issue of first impression that requires the Court to unpack the stacking doll of definitions in the SCA. An ECS is "any service which provides to *users* thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (emphasis added). A "user" is "any person or entity who—(A) uses an [ECS]; and (B) is duly authorized by the provider of such service to engage in such use." *Id.* § 2510(13). Person "means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 2510(6). The SCA does not define "entity."

The SCA defines "user" with the broadest possible language: "any person." *See* § 2510(13). "Any person means any person, including foreign citizens." *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 729 (9th Cir. 2011). The foreign government officials implicated here are undoubtedly "foreign citizens." Moreover, the SCA's definition of "person" is expansive: U.S. government agents *and* individuals. *See* § 2510(6). According to The Gambia, that U.S. government agents are listed separately from individuals means that agents are not considered individuals. *See* Pet'r's Reply at 6. The Gambia further hypothesizes Congress, by explicitly listing U.S. government agents, intended to forego SCA protection for foreign government agents. *See id.* The natural reading of the statute dictates otherwise. The definition of "person" merely

[4] The definition of "user" only operates to limit the designation of a provider as an ECS. According to 18 U.S.C. § 2702(a)(1), an ECS "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." The definition of "user" does not affect the disclosure prohibitions in § 2702, which are absolute. The Gambia tries to give the definition of "user" much more power than it has. Congress could have limited the application of the SCA to the communications of particular users, but it did not.

highlights government agents' inclusion in SCA protection, not their exclusion from the "any individual" category. Moreover, The Gambia's attempt to partition these categories does not comport with the SCA's legislative history. Congress was concerned with "civil litigants issuing discovery requests" and thus sought to protect all individuals from unauthorized access. *Suzlon*, 671 F.3d at 730. Myanmar officials are individuals.

The inclusion of "entity" in the definition of "user" provides an independent basis for SCA coverage. The ordinary definition of "entity" includes "a governmental unit[] that has a legal identity apart from its members or owners." *See* Pet'r's Reply at 6 (quoting *Black's Law Dictionary* (11th ed. 2019)). That definition covers the state-sanctioned, coordinated inauthentic content at issue here.[5] *See* De-platforming Post.

Therefore, Facebook is an ECS as to the content in question.[6]

---

[5] The Gambia makes a novel argument that the Myanmar government agents were not "authorized" users (and thus outside the scope of the SCA) because Facebook later banned them for terms of service violations. *See* Pet'r's Reply at 9–11. As explained below, application of the SCA is not tied to terms of service violations. Thus, ruling on whether the users were duly "authorized" is unnecessary; particularly given that analyzing such question would require facts not before this court, such as when did each account violate the terms of service.

[6] The SCA also covers providers of remote computing services ("RCS"). *See* 18 U.S.C. § 2702(a). An RCS is subject to the same prohibitions on content disclosure as an ECS. *See id.* RCS is defined as "the provision to the *public* of computer storage or processing services by means of an electronic communications system." *Id.* (emphasis added).

Waiting until its surreply, Facebook asserted in a footnote that it is also an RCS and that it "reserves" the right to argue this as a basis against disclosure. Resp't's Surreply at 2, n.1. "[A]rguments raised in footnotes are not preserved." *SmithKline Beecham Corp. v. Apotex Corp.*, 439 F.3d 1312, 1320 (Fed. Cir. 2006). Waiver is particularly appropriate where the parties declined the opportunity for further briefing, *cf. Sugar Cane Growers Co-op. of Fla. v. Veneman*, 289 F.3d 89, 93 n.3 (D.C. Cir. 2002), which Facebook did here, *see* Conf. Tr. at 159. In any case, the RCS argument is without merit.

"Whether an entity is acting as an RCS or an ECS (or neither) is context dependent, and depends, in part, on the information disclosed." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1023 (N.D.

3. *Electronic Storage*

An ECS provider is prohibited from divulging communications "while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). "[The 'electronic storage'] requirement is commonly misunderstood because the statutory definition of 'electronic storage' is much narrower than its name suggests." *Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 839 (8th Cir. 2015) (quoting Robison, *supra* at 1206).

The SCA defines two types of "electronic storage." 18 U.S.C. § 2702(17). The first is temporary storage, which includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." *Id.* § 2510(17)(a). It is undisputed that the content in question was "delivered," *Hately*, 917 F.3d at 785, or "post[ed]," *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010). Because the content had reached its destination, it was not in temporary storage. *See Hately*, 917 F.3d at 784–85; *Crispin*, 717 F. Supp. 2d at 989.

The second is backup storage, which includes "any storage of such communication by an electronic communication service for purposes of *backup protection* of such communication." 18 U.S.C. § 2510(17)(b) (emphasis added). The parties agree that the question is whether the records sought are backup storage. *See* Pet'r's Reply at 12–13; ECF No. 15 (Resp't's Surreply) at 3–4.

a. The Problem Of Content Moderation

Cal. 2012) (citing Kerr, 72 Geo. Wash. L. Rev. at 1215). Out of the gate, Facebook is incorrect to assert that it is *always* an RCS. The question here is whether Facebook was acting as an RCS for the deleted content it preserved. *See id.* at 1023. Indeed, "a storage service necessarily requires a retrieval mechanism to be useful. To retrieve communications in storage, the RCS provider must display those communications in some way." *Crispin*, 717 F. Supp. 2d at 990. The "distinction between public and nonpublic" availability is dispositive. *Kerr*, 72 Geo. Wash. L. Rev. at 1226. As to the *public*, no such retrieval mechanism is available here for the deleted content, nor is it publicly visible. Thus, Facebook is not an RCS here.

At the time of enactment, Congress viewed ECS and RCS providers as mail/package delivery services. *See* Cong. Rsch. Serv., R46662, *Social Media: Misinformation and Content Moderation Issues for Congress* (2021), https://crsreports.congress.gov/product/pdf/R/R46662. This view failed to consider content moderation; mail/package delivery services have neither the ability nor the responsibility to search the contents of every package. Yet after disinformation on social media has fed a series of catastrophic harms, major providers have responded by taking on the *de facto* responsibility of content moderation. *See id.* "The question of how social media platforms can respect the freedom of expression rights of users while also protecting [users] from harm is one of the most pressing challenges of our time." HRIA at 3.

This Court is the first to consider the question of what happens after a provider acts on its content moderation responsibility. Is content deleted from the platform but retained by the provider in "backup storage?"[7] It is not.

b. Deleted Content

[7] "Deleted" means permanently unavailable to the user. The instant question concerns provider-deleted content, not user-deleted content. When a user permanently deletes content, it is generally no longer accessible or recoverable. *See Can I see deleted messages in Messenger?*, Facebook, https://www.facebook.com/help/messenger-app/540897679352879/?helpref=search ("No, you can't see deleted messages or conversations. Deleting a message permanently removes it from your Chat list.") (last visited Sept. 14, 2021); *Delete or recover deleted Gmail messages*, Google, https://support.google.com/mail/answer/7401 ("When you delete a message, it stays in your Trash for 30 days. After that time, it will be permanently deleted from your account and can't be recovered.") (last visited Sept. 14, 2021). Permanently deleted content is also unavailable to law enforcement, unless they obtained a formal preservation order prior to deletion. *See Information for Law Enforcement Authorities*, Facebook, https://www.facebook.com/safety/groups/law/guidelines/ (last visited Sept. 14, 2021). Given that permanently deleted content by the user appears not to be retained by providers, the question of whether user-deleted content is protected is likely a non-issue.

"The ordinary meaning of the word 'backup' is 'one that serves as a substitute or support.'" *Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012) (quoting Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/backup). Congress's conception of "'backup' necessarily presupposes the existence of another copy to which this [backup record] would serve as a substitute or support." *Id.* Without an original, there is nothing to back up. Indeed "the lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired . . . , any copy is no longer performing any backup function. An [ECS] that kept permanent copies of [deleted] messages could not fairly be described as 'backing up' those messages." *Gonzales v. Uber Techs., Inc.*, No. 17-cv-02264, 2018 WL 4616266, at *4 (N.D. Cal. Sept. 26, 2018) (quoting *Theofel v. Farey-Jones* 359 F.3d 1066, 1076 (9th Cir. 2004).

Approximately three years ago, Facebook deleted the content in question as coordinated inauthentic behavior. *See* De-platforming Post; ECF No. 19 (Conf. Tr.) at 102–16. And coordinated inauthentic behavior violates Facebook's terms of service. *See Coordinated Inauthentic Behavior*, Facebook (Dec. 6, 2018) https://about.fb.com/news/tag/coordinated-inauthentic-behavior/. Facebook heavily publicized this action and its finality. *See* Conf. Tr. at 110; De-platforming Post.[8] Indeed, Facebook has kept the content offline since then and "nobody [on Facebook] can view it." *Id.* at 76. Because the original content is permanently off the platform, no backup copy can exist of it. *See Gonzales*, 2018 WL 4616266, at *4.

[8] This decision touches a narrow category: content *permanently* deleted by the provider. *See ante*, at n.7. Undoubtedly, the instant content falls into that category given the passage of time since Facebook deleted the content, that it banned related users, and Facebook's own words publicizing this as a final decision. *See* De-platforming Post. Not before this Court is what happens when content is in purgatory—i.e., de-platformed, but not yet subject to a decision about permanent deletion. *See* Conf. Tr. at 151. Ultimately, courts have a fact-intensive task of determining whether a provider has reached a final decision on de-platforming.

It is true that Facebook alone retains offline access to the deleted content. However, any "archive of [deleted] messages that [Facebook] continues to maintain . . . constitutes the *only* available record of these communications, and cannot possibly serve as a 'backup' copy of communications stored elsewhere." *Flagg v. City of Detroit*, 252 F.R.D. 346, 363 (E.D. Mich. 2008).

c. Analogy To Undeleted Content

Nearly all "backup storage" litigation relates to delivered, undeleted content. That case law informs and supports the Court's decision here. "Although there is no binding circuit precedent, it appears that a clear majority of courts have held that emails opened by the intended recipient (but kept on a web-based server like Gmail) do not meet the [backup protection] definition of 'electronic storage.'" *Sartori v. Schrodt*, 424 F. Supp. 3d 1121, 1132 (N.D. Fla. 2019) (collecting cases). The Department of Justice adopted this view, finding that backup protection "does not include post-transmission storage of communications." U.S. Dep't of Just., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 123 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. The Gambia argues for following the majority view's limited definition of backup storage. *See Sartori*, 424 F. Supp. 3d at 1132; ECF No. 16 (Pet'r's Resp. to Surreply) at 5–6. If undeleted content retained by the user is not in backup storage, it would defy logic for deleted content to which the user has no access to be in backup storage.

Facebook argues for the opposite reading of backup storage, relying on a Ninth and Fourth Circuit case that delivered, undeleted content is in backup storage. *See Theofel*, 359 F.3d at1070 (9th Cir. 2004); *Hately*, 917 F.3d at 785. However, as discussed below, the language of *Theofel*

and *Hately* explicitly supports a finding that deleted content is not backup storage. Thus, the Court need not determine the appropriate standard for delivered, undeleted messages.

> The emphasis in *Theofel* is on the purpose of the storage:
>
> > [T]he mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose. We see many instances where an [ECS] could hold messages not in electronic storage—for example, e-mail sent to or from the [provider]'s staff, or messages a user has flagged for deletion from the server. In both cases, the messages are not . . . kept for any backup purpose."

Theofel, 359 F.3d at 1070. Even under *Theofel*, the purpose of backup storage must be to backup the original. *See Gonzales*, 2018 WL 4616266, at *4 (applying *Theofel*, location data retained only by provider but not by the user was not backup storage). The *Crispin* court applied *Theofel*'s holding to a hypothetical context in which "Facebook . . . retain[ed] copies of webmail or private messaging communications on [its] servers separate from the storage available to [a user]." *See Crispin*, 717 F. Supp. 2d at 987 n.46. The court assumed that such off-platform data would be protected as backup storage *unless* it fell into one of *Theofel*'s exceptions, including "messages a user has flagged for deletion." *Id.* (quoting *Theofel*, 359 F.3d at 1076). Even the broadest interpretation of backup storage carved out content deleted from the platform. This is devastating to Facebook's argument.

Facebook argues that because the provider-deleted content remains on Facebook servers in proximity to where active content on the platform is stored, both sets of content should be protected as backup storage. *See* Conf. Tr. at 76. However, the question is not *where* the records are stored but *why* they are stored. *See Theofel*, 359 F.3d at 1070. Facebook claims it kept the instant records as part of an autopsy of its role in the Rohingya genocide. *See* Conf. Tr. at 80–81. While admirable, that is storage for self-reflection, not for backup. Moreover, Facebook's interpretation of backup—anything on its servers—reads the term out of the statute. Congress limited the SCA

to protection of backup storage rather than all electronic storage. *See* 18 U.S.C. § 2510(17). This Court "construe[s] [the SCA] so that effect is given to all its provisions." *Delaware Dep't of Nat. Res. & Env't Control v. EPA*, 895 F.3d 90, 99 (D.C. Cir. 2018) (internal quotation omitted).

Facebook's reliance on *Hately* is similarly misplaced. *See* Resp't's Surreply at 3–4. The *Hately* court reasoned that "a wire or electronic communication is stored for 'purposes of backup protection' if it is a 'copy' or 'duplicate' of the communication stored to prevent, among other things, its 'destruction.'" *Hately*, 917 F.3d at 791. Here, Facebook itself "destroyed" the content in question by removing it from its platform and banning the associated accounts. While Facebook retained offline access to the deleted content, that access was not was not meant to prevent its destruction on the platform—indeed far from it, as Facebook deemed that content illicit and unwelcome on its platform.[9] The SCA was created to allow platforms to flourish for users, not to protect records for a provider. *See e.g.*, *Suzlon*, 671 F.3d at 729–30.

The *Hately* court's reliance on the three legislative history prongs is inapposite here.[10] First, the risk of a chilling effect deterring potential users from "using innovative communications systems," S. Rep. No. 99-541, at 5 (1986), is nonexistent as Facebook usage is already ubiquitous,

[9] Backup protection need not be solely for the benefit of the user. *See Hately*, 917 F.3d at 795. The provider may create backup copies for self-serving reasons, such as "decreasing email downtime, protecting against loss of data in the event a particular server fails, and for their own commercial purposes, such as to more effectively target advertisements." *Id.* (citation omitted). Facebook has not alleged that the instant offline retention served any such commercial purposes recognized by courts. Moreover, the backup protection determination is not based on who, if anyone, is benefitted, but rather if the purpose was for backup storage.

[10] The *Hately* court held that the messages a user "chooses *not* to delete . . . [we]re likely precisely the types of messages Congress sought to protect." *Hately*, 917 F.3d at 798 (emphasis added). Nothing suggests that messages a *provider* chooses to delete for violating terms of service and fanning the flames of genocide are the kind of messages Congress sought to protect. Moreover, "the Supreme Court [has] reiterated . . . [this] resort to legislative history is not appropriate in construing plain statutory language." *U.S. ex rel. Totten v. Bombardier Corp.*, 380 F.3d 488, 494 (D.C. Cir. 2004) (collecting cases).

see HRIA 12–14. Moreover, by banning coordinated inauthentic behavior from Facebook nearly three years ago, Facebook has already deterred users with such content from entering its platform. *See Coordinated Inauthentic Behavior*, Facebook (Dec. 6, 2018), https://about.fb.com/news/tag/coordinated-inauthentic-behavior/. Second, the harm of "unauthorized users [] obtain[ing] access to communications to which they are not a party," S. Rep. No. 99-541, at 5 (1986), is mitigated where the content is limited to unauthorized inauthentic accounts, as opposed to genuine communications from real users. Additionally, the Court and Facebook still serve as gatekeepers on releasing records to unauthorized users. Third, concerns about disclosure damaging the right to privacy, *see id.*, is a boogeyman that does not haunt here. Coordinated inauthentic behavior—i.e., fake accounts that violated the terms of service—had no privacy rights from Facebook. And the right to privacy in this case must be balanced against the need to uncover the cause of the Rohingya genocide.

d. Privacy Concerns

Finally, Facebook advances a policy argument, opining that this Court's holding will "have sweeping privacy implications—every time a service provider deactivates a user's account for any reason, the contents of the user's communications would become available for disclosure to anyone, including the U.S. government."[11] Resp't's Surreply at 7. Facebook taking up the mantle of privacy rights is rich with irony. News sites have entire sections dedicated to Facebook's sordid history of privacy scandals. *See, e.g.*, *Facebook Privacy Scandal*, AP News,

[11] Facebook's argument that this holding is a boon to law enforcement misses the mark. Law enforcement already accesses content regularly via search warrants. The Fourth Amendment requirement for a search warrant is untouched by this Court's reading of the SCA. The Fourth Amendment's privacy protections stand apart from the SCA. *See United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Indeed, the Fourth Amendment broadly protects digital media irrespective of SCA coverage. *See, e.g.*, *Riley v. California*, 573 U.S. 373 (2014).

https://apnews.com/hub/facebook-privacy-scandal-. In 2019, Facebook was fined $5 billion by the government after "deceiving users about their ability to control the privacy of their personal information" in violation of a prior FTC order. Federal Trade Commission Press Release, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. These facts undercut the moral suasion of this argument.

Regardless, this is the way Congress authored the SCA. When a user signs up for a Facebook account, they agree to abide by Facebook's terms of service. *See Terms of Service*, Facebook, https://www.facebook.com/terms. Failure to abide by these terms may result in Facebook unilaterally deleting the account. *See Why is my personal Facebook account disabled?*, Facebook, https://www.facebook.com/help/103873106370583/. And once content is deleted from the platform, it is no longer protected by the SCA. *See infra*. Thus, Congress empowered ECSs to denature parts of the SCA. But de-platformed content is just one of the many SCA exceptions. Other provisions similarly permit providers to make unilateral determinations about "disclos[ing] records, information, and contents of accounts." *United States v. Sykes*, No. 3:18-cr-178, 2020 WL 8484917, at *9 (E.D. Tenn. Oct. 5, 2020). So, in a twist of irony, Facebook already held the keys to many of the SCA's privacy protections.[12]

[12] Facebook is right that foreign governmental and foreign/domestic non-governmental entities may more easily obtain de-platformed content (via a subpoena) than U.S. law enforcement (via a search warrant). *See* Resp't's Opp'n at 12. This merely reflects that the Constitution places the greatest burden on U.S. authorities when conducting searches. Civil litigants, domestic and foreign, can frequently obtain records more easily than the U.S. government can. This is not a reason to upend Congress' explicitly laid out statutory scheme. Moreover, Congress' primary concern was limited to U.S. government action according to the statute's text. *See Suzlon*, 671 F.3d at 730.

The privacy implications here are minimal given the narrow category of requested content. Content urging the murder of the Rohingya still permeates social media. *See* Stecklow, *supra* (documenting "more than 1,000 examples . . . of posts, comments, images and videos attacking the Rohingya or other Myanmar Muslims that were on Facebook" even after Facebook apologized for its services being "used to amplify hate or exacerbate harm against the Rohingya"). Such content, however vile, is protected by the SCA while it remains on the platform. The parade of horribles is limited to a single float: the loss of privacy protections for de-platformed content. And even that could be mitigated by users joining sites that do not de-platform content.

The deleted content at issue here does not fall within electronic storage protected by the SCA.

4. *Exceptions To SCA Protection*

Irrespective of the above analysis, the SCA includes enumerated exceptions permitting disclosure of otherwise protected content. Most relevant here is the consent exception: "A provider . . . may divulge the contents of a communication . . . with the lawful consent of the originator . . . ." § 2702(b)(3). The Gambia also raises the provider protection exception: "A provider . . . may divulge the contents of a communication . . . as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." *Id.* § 2702(b)(5). Several district courts have held that disclosure under any SCA exception is purely voluntary on the part of the provider, relying on the term "may." *See, e.g.*, *United States v. Wenk*, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017); *PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.*, 273 F. Supp. 3d 558, 561 (W.D. Pa. 2017); *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012). This Court is not convinced. The California Supreme Court engaged in a more searching analysis:

> Congress's use of the word "may" to frame an exception to the Act's general prohibition on disclosure is not such a "clear expression of . . . intent" as will justify a reading of the Act that categorically immunizes service providers against compulsory civil process where the disclosure sought is excepted on other grounds from the protections afforded by the Act . . . . Insofar as the Act permits a given disclosure, it permits a court to compel that disclosure . . . .

Facebook, Inc. v. Super. Ct., 417 P.3d 725, 751 (2018) (quoting *Negro v. Superior Court*, 179 Cal. Rptr. 3d 215, 233–34. (2014)). Without clear statutory intent to show otherwise, this Court cannot logically conclude that Congress gave Facebook greater power over discovery than the judiciary. Thus, this Court concurs with the California Supreme Court that courts may compel production of communications excepted from SCA protections. *See id.*

a. Consent Exception

The consent exception is largely applicable here because much of the content The Gambia seeks was posted publicly before Facebook removed it. "[O]ne who posts a communication with a reasonable basis for knowing that it will be available to the public should be considered to have implicitly consented to such disclosure under section 2702(b)(3)." *Id.* at 742 (citing *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008)). This is because the SCA "was intended to cover and protect only private and not public posts." *Id.* at 739. Facebook agrees that it has the discretion to disclose public content under the consent exception. *See* Conf. Tr. at 65–66.

Because social media is public by nature, "the critical inquiry is whether Facebook users took steps to limit access to the information in their posts." *Facebook*, 417 P.3d at 741 (quoting *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013)). Not all "public" Facebook posts are created equally—users set some to be public to anyone at any time, while others are shared only to members of a group or followers of a page. *See When I post*

something on Facebook, how do I choose who can see it?, Facebook, https://www.facebook.com/help/120939471321735/ (last visited Sept. 19, 2021). Although "private" groups and pages requires an administrator to grant access to the content, such forums can still reach thousands to millions of followers. *See, e.g.*, *A group where we all pretend to be ants in an ant colony*, Facebook, https://www.facebook.com/groups/1416375691836223/ (1.8 million members as of Sept. 19, 2021). Administrators can automatically grant access to every requestor, such that a private group effectively becomes public. *See How do I automatically approve members to join my Facebook group?*, Facebook, https://www.facebook.com/help/540954519763978 (last visited Sept. 19, 2021).

There is no magic number of accessible viewers for content to trigger the consent exception. The consent analysis instead turns on the fact-intensive inquiry as to "whether the posts had been configured by the user as being 'sufficiently restricted that they are not readily available to the general public.'" *Facebook*, 417 P.3d at 743 (quoting *Crispin*, 717 F. Supp. 2d at 991). At bottom, the Court is looking to discern the user's "intent" as to the public versus private nature of the post. *Id.* at 747.

The relevant facts are undisputed here. The parties agree that the content in question was inauthentic accounts and pages Myanmar authorities created with the intent of "spread[ing] hate speech, fake news, and misinformation for political gain." HRIA at 13. Although some of the pages were nominally private, the Myanmar officials intended their reach to be public, and in fact they reached an audience of nearly 12 million followers. *See* De-platforming Post. Making their accounts and pages private would have defeated their goal of inflaming hate in the widest possible audience. *See Facebook*, 417 P.3d at 747. It is the rare case here that the authors nakedly displayed their *intent* to reach the public and such intent was independently confirmed. *See* U.N. Report at

¶¶ 1439–41. Thus, outside of private messages,[13] the content requested by The Gambia (as scoped to only include hate-speech and violent content) falls within the consent exception.[14] Ordering discovery is particularly appropriate here because much of the requested content would have been publicly available to The Gambia had Facebook not deleted it.[15]

b. Provider Protection Exception

The provider protection exception is inapplicable here. The purpose of this exception is to protect the rights and property of the provider. *See* H.R. Rep. No. 99-647, at 67 (1986). This exception is properly within the provider's discretion, and no court has determined otherwise. The Court does not purport to know better than Facebook what is to Facebook's own benefit.

B. Burden And Scope Under *Intel*

[13] Private messages refer to "secret conversation[s] in [Facebook's] Messenger [that are] end-to-end encrypted and intended just for you and the person you're talking to." *How do I start a secret conversation in Messenger?*, Facebook, www.facebook.com/help/messenger-app/811527538946901/ (last visited Sept. 19, 2021).

[14] As with any discovery dispute, the Court is drawing general parameters here. The Gambia agrees that the consent exception does not apply to private messages. *See* Conf. Tr. at 33, 37. Facebook agrees that the consent exception covers some exclusively public content. *See id.* at 66–67. Yet The Gambia has no visibility into the data itself. *See id.* at 34. The parties will have to meet and confer to resolve any questions about content in between, with the backdrop of the Court's ruling that all pages and groups intended to be public should be disclosed. Future litigation may revolve around specific inquiries at to the nature of such content.

[15] This Court does not wish to discourage the complicated work Facebook undertook to find and delete the content in question. *See* HRIA 25–28. Facebook's dual responsibilities of upholding free speech and preventing misinformation from causing catastrophic real-world consequences is arguably the issue of this generation. But Facebook's self-regulation is not the only tool for combating abuse. The Gambia is pursuing another recognized tool: international litigation before an authorized tribunal. And Congress has empowered this Court to facilitate such litigation.

"Assuming a district court has the authority to grant a discovery request under § 1782, the court then considers whether to exercise its discretion to do so." *Norex Petroleum*, 384 F. Supp. 2d at 49. It is uncontested that the statutory factors of § 1782 are met here.[16]

"The fourth [*Intel*] factor is the salient one here." *Hulley Enters.*, 2017 WL 3708028, at *4. It considers "the scope of the requested discovery, asking whether it is 'unduly intrusive or burdensome.'" *In re DiGiulian*, 314 F. Supp. 3d 1, 9 (D.D.C. 2018) (quoting *Intel*, 542 U.S. at 265). "[C]ourts have interpreted this inquiry to encompass 'the relevance of the requested discovery to the foreign proceeding.'" *Id.* (quoting *Hulley Enters.*, 2017 WL 3708028, at *4). This is the traditional proportionality analysis. *See MetaLab Design Ltd. v. Zozi Int'l, Inc.*, 2018 WL 368766, at *4 (N.D. Cal. Jan. 11, 2018) (quoting Fed. R. Civ. P. 26(b)(1)).

1. *Burden Of Production*

The Gambia seeks a discrete and known universe of records—the content that Facebook previously found and deleted from its platform. Yet Facebook argues that the discovery requests offer no meaningful metric for identifying accounts and are overbroad. *See* Resp't's Opp'n at 10–13. Rather than requesting communications from "a litany of individuals or entities, none of whom are specifically identified," *id.* at 10, The Gambia specifically identified the communications of seventeen individuals, four entities, and nine Facebook pages, *see* Pet'r's Mot. at 14–17. Any pages or accounts of which The Gambia does not know the specific identity, Facebook does. *See id.* Indeed, The Gambia's discovery requests are cribbed from Facebook's press release on de-platforming and are limited to the information Facebook de-platformed. *See* Conf. Tr. at 10, 139

[16] Facebook has offices in the District of Columbia. *See* Pet'r's Mot. at 19. The pending ICJ case constitutes a proceeding before an international tribunal and The Gambia is an interested party in that proceeding as a litigant. *See Intel*, 542 U.S. at 256 (finding that a litigant before the foreign tribunal is the quintessential interested person).

(referencing Facebook's de-platforming post). The Gambia is not asking, nor is the Court ordering, Facebook to conduct further searches for coordinated inauthentic behavior related to the Rohingya genocide. Thus, the traditional discovery burden of searching for content does not manifest here. In fact, Facebook has already produced some records. *See id.* at 38–42.

The Gambia scoped its request to only seek content "relevant to the ICJ case," that is documents related to "hate speech and [the] incitement to violence on Facebook." *Id.* at 11, 46. In so doing, The Gambia focused its request on only the most relevant documents. Facebook argues that it is unduly burdensome to review its documents for a specific content. *See id.* at 101. Facebook's de-platforming process did not include a forensic review of all account and page data. *See id.* at 106–07. And Facebook says it would be challenging to search for specific content now, particularly due to translation issues. *See id.* at 103–04. However, such review should present minimal difficulties as Facebook has publicly touted the strength of its Myanmar language team and its content-review capabilities. *See e.g.*, Rafael Frankel, *An Update on the Situation in Myanmar*, Facebook (Feb. 11, 2021), https://about.fb.com/news/2021/02/an-update-on-myanmar/. Moreover, Facebook would seemingly know a thing-or-two about searching its data, as that is in part how it generates revenue. *See Data Policy*, Facebook, https://www.facebook.com/about/privacy.

The Gambia limited its request to de-platformed content dating back to 2012. *See* Pet'r's Mot. at 14–17. Facebook challenges this as overly broad and counters with a 2016 date range, Conf. Tr. 46–47; however, this fails for three reasons. First, the 2012 data is highly probative of the instigation of the genocide. The U.N. Mission found that Myanmar officials posted disinformation on Facebook in 2012 that led to violence then and beyond. *See* U.N. Report at ¶ 696. And concluded that the extreme levels of violence perpetrated against the Rohingya in 2016

and 2017 could only be understood by examining Myanmar officials' activities dating back to 2012. *See id.* at ¶¶ 745–48. Second, Facebook has not demonstrated how the additional four years of content unduly expands the document production. Facebook could have analyzed the metadata of its records to substantiate its claim, but it did not. Third, there is nothing to suggest The Gambia's request for content dating back to 2012 was "made in bad faith, for the purpose of harassment, or [was] part of a fishing expedition." *Intel*, 542 U.S. at 265.

Ultimately, this case raises at most the normal burdens of discovery—including for § 1782 requests. Facebook can mitigate the primary burden it identified by using "technology assisted review [which] is cheaper, more efficient and superior to keyword searching." *In re Mercedes-Benz Emissions Litig.*, No. 216-cv-881, 2020 WL 747195, at *6 (D.N.J. Feb. 14, 2020); *see also* Conf. Tr. at 141–42. The parties are otherwise left to negotiate how to efficiently comply with this Court's order. For example, The Gambia has already offered to take the full de-platformed data set, minus any content searches, to alleviate the burden on Facebook. *See* Conf. Tr. at 144–45.

2. *Relevance*

"[W]hether the [ICJ] will ultimately find [the requested discovery] 'useful' . . . comes into play only in the context of the discretionary *Intel* factors." *In re Veiga*, 746 F. Supp. 2d 8, 19 (D.D.C. 2010). The ICJ is considering whether Myanmar violated the Genocide Convention. The Gambia seeks evidence to prove genocidal intent. As the U.N. Mission concluded:

> The role of social media [in Myanmar] is significant. Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the Internet. Although improved in recent months, the response of Facebook has been slow and ineffective. The extent to which Facebook posts and messages have led to real-world discrimination and violence must be independently and thoroughly examined."

Report of the Independent International Fact-Finding Mission on Myanmar, A/HRC/39/64 at ¶ 74, U.N. Human Rights Council (Sept. 12, 2018). Facebook has admitted that Myanmar authorities used Facebook as part of a coordinated campaign of hate against the Rohingya. *See* De-platforming Post. Yet the scope and underlying proof of this conclusion is unknown to The Gambia. *See* Conf. Tr. at 51. The records sought by The Gambia answer these questions, which are the gravamen of the ICJ inquiry. Moreover, the U.N. Mission's report and Facebook's HRIA each independently corroborate the relevancy of the request. That the records are highly relevant to the foreign proceeding balances out any incremental burden on Facebook.

3. *Alternative Avenues Of Discovery*

Facebook opines that The Gambia should have made its request via a mutual legal assistance treaty (MLAT), the CLOUD Act, or a different international body. This is a nonstarter. The only issue is whether The Gambia has met the requirements of § 1782. A court need not consider whether other paths exist to collecting records. *Cf. HT S.R.L. v. Velasco*, No. 15-mc-664, 2015 WL 13759884, at *3 (D.D.C. Nov. 13, 2015) ("nothing in the text of 28 U.S.C. § 1782 . . . supports a quasi-exhaustion requirement" in part because doing so would impose an additional burden on parties seeking assistance from federal courts for matters relating to international litigation). And the alternatives Facebook suggests largely involve voluntary compliance, whereas an order under § 1782 mandates compulsory production.

Specifically, Facebook directs The Gambia to obtain discovery through the U.N. Independent Investigative Mechanism for Myanmar ("IIMM"), which "Facebook is actively working to support." Resp't's Surreply at 1. However, Facebook's "voluntar[y] produc[tion]" of records to the IIMM only began in August 2020, *id.*, and reportedly has been stilted, *see* Poppy McPherson, *U.N. investigator says Facebook has not shared 'evidence' of Myanmar crime*,

Reuters (Aug. 11, 2020), https://www.reuters.com/article/us-myanmar-facebook/u-n-investigator-saysfacebook-has-not-shared-evidence-of-myanmar-crime-idUSKCN2570K9; Conf. Tr. at 38–40. Relying on Facebook's own interpretation of the consent exception, Facebook has provided only limited public postings to the IIMM. *See* Conf. Tr. at 65–66.

Facebook opines that, compared to the ICJ, the IIMM is a "uniquely positioned body . . . tasked with collecting, preserving, and analyzing information for use in criminal proceedings under international law and in other contexts on a case-by-case basis, and with expediting and facilitating fair criminal proceedings." Resp't's Surreply at 1. The ICJ is not the McDowell's to the IIMM's McDonald's. *See* Panama Jackson, Coming to America *Questions That Need Answers: Was McDowell's Better than McDonald's? An Examination* (Mar. 3, 2021), https://www.theroot.com/coming-to-america-questions-that-need-answers-was-mcdo-1846387969. The ICJ is "the central expositor of international law," *Doe v. Nestle, S.A.*, 748 F. Supp. 2d 1057, 1083 (C.D. Cal. 2010), whose "judgments and opinions . . . are accorded great weight," Restatement (Third) of Foreign Relations, § 103 cmt. (b). In fact, the ICJ may be a superior venue given that it regularly adjudicates Genocide Convention issues. *See*, *e.g.*, *Sarei v. Rio Tinto, PLC*, 671 F.3d 736, 759 (9th Cir. 2011) (overturned on other grounds). The Court agrees that "the IIMM is not participating in the proceedings before the [ICJ]—and [The Gambia has] no reason to believe that any materials that Facebook would provide to the IIMM would be sufficient to satisfy its obligations under 28 U.S.C. § 1782." Pet'r's Resp. to Surreply at 1–2.

C. Facebook's Internal Investigation

The Gambia separately requests records related to Facebook's internal investigation of its role in the Rohingya genocide. *See* Resp't's Opp'n at 8. To the extent these records are protected

by a legal privilege, the normal prohibitions on discovery apply. However, Facebook must produce any non-privileged documentation that relates to the internal investigation.

The Gambia reasonably expects Facebook's internal investigation will reveal information that goes beyond the content of the deleted posts. *See* Conf. Tr. at 52–53. The investigation records will illuminate how Facebook connected the seemingly unrelated inauthentic accounts to Myanmar government officials. *See id.* Specifically, these records may show which accounts or pages were operated by the same officials or from the same government locations.[17] Therefore, Facebook's internal investigation data—to the extent it exists—may be even more significant to The Gambia's ability to prove genocidal intent. Given that Facebook has already conducted its investigation, the additional burden of production is minimal. Moreover, the requested discovery could not have greater import in the ICJ litigation.

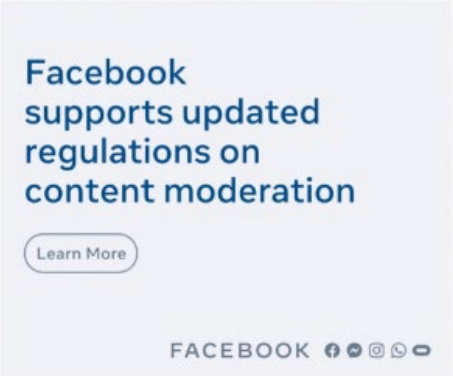
D. Deposition

While it may be helpful to The Gambia, a Rule 30(b)(6) deposition is too much to demand of Facebook. The Gambia seeks this deposition to make sense of the documents it has asked Facebook to produce—an analysis which The Gambia could conduct thorough its own examination of the documents. This request is unduly burdensome and adds little in the way of concrete evidence given the Court's order for document production.

[17] Much of The Gambia's request for internal investigation data involves Facebook's analysis of non-content metadata of the deleted content. *See* Conf. Tr. at 25, 42–43, 50. "[F]ederal courts have held that service providers may divulge non-content information to non-governmental entities in response to civil subpoenas," because such data falls outside of the SCA. *Williams v. AT&T Corp.*, No. 15-3543, 2016 WL 915361, at *3 (E.D. La. Mar. 9, 2016) (collecting cases). Non-content information includes the identifying information for the account holder and "the date, time, originating and receiving telephone number, and duration for incoming and outgoing calls." *Doe v. City of San Diego*, No. 12-CV-0689-MMA DHB, 2013 WL 2338713, at *4 (S.D. Cal. May 28, 2013). Ultimately, the content/non-content distinction is unimportant here, given the Court's determination above that the SCA does not preclude disclosure.

IV. CONCLUSION

After seventeen years of existence, Facebook has grown self-aware. It has realized that "[t]he need for extensive content moderation is inherent in any platform that is built upon user-generated content, and with over 2 billion users, this is a task of immense complexity and intensity for Facebook." HRIA at 25. Indeed, the internet is littered with ads by Facebook touting their support for updated content moderation and internet regulations to handle "today's toughest challenges":



A MESSAGE FROM FACEBOOK

It's time to update internet regulations

The internet has changed a lot in the 25 years since lawmakers last passed comprehensive internet regulations. It's time for an update.

See how we're making progress on key issues and why we support updated regulations to set clear rules for addressing today's toughest challenges.

Although an update to the SCA is sorely needed as it "was written prior to the advent of the Internet and the World Wide Web," *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002), none is needed here. Facebook's concern was that the SCA prevented the requested disclosure. However, the SCA has a well-established path for disclosure of deleted content.

Facebook can act now. It took the first step by deleting the content that fueled a genocide. Yet it has stumbled at the next step, sharing that content. Failing to do so here would compound the tragedy that has befallen the Rohingya. A surgeon that excises a tumor does not merely throw it in the trash. She seeks a pathology report to *identify* the disease. Locking away the requested

content would be throwing away the opportunity to understand how disinformation begat genocide of the Rohingya and would foreclose a reckoning at the ICJ.

Facebook describes its remediation efforts for its role in what happened in Myanmar as "some of the most important work being done at Facebook. . . . The weight of this work, and its impact on the people of Myanmar, is felt across the company." Su, *supra*. The Court's decision compels Facebook to live up to its words.

For the foregoing reasons, The Gambia's request for de-platformed content and related internal investigation documents is GRANTED and its request for a deposition with Facebook is DENIED.[18]

2021.09.22
18:05:15 -04'00'

ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE

[18] Pursuant to LCvR 72.2, any party may file written objections to this ruling under within 14 days after being served. The objections shall specifically designate the order or part thereof to which objection is made, and the basis for the objection. The filing of oppositions and replies shall be governed by LCvR 7(b) and (d).