

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION**

X CORP.,

Plaintiff,

v.

**MEDIA MATTERS FOR AMERICA,
ET AL.,**

Defendants.

§
§
§
§
§
§
§
§
§
§

Civil Action No. 4:23-CV-01175-O

OPINION & ORDER

Before the Court are Defendants’ Motion to Compel Discovery, Brief in Support, and Appendix in Support (ECF Nos. 240, 267); Plaintiff’s Response and Appendix (ECF Nos. 246–47); and Defendants’ Reply and Appendix in Support (ECF No. 250); Plaintiff’s Supplemental Brief in Opposition to Defendants’ Motion to Compel (ECF No. 293); Defendants’ Response (ECF No. 300-1); and Plaintiff’s Reply (ECF No. 303), which were filed at the Court’s request (*see* ECF No. 288) in response to the Court deferring ruling on Request for Production 79 in Defendants’ Motion to Compel (ECF No. 267). Also before the Court are Defendants’ Motion to Compel (ECF No. 269) and Appendix in Support (ECF No. 261-2); Plaintiff’s Response and Appendix in Support (ECF Nos. 277–78) and Notice of Errata Correcting Response (ECF No. 284); and Defendants’ Reply and Appendix in Support (ECF Nos. 290–91). After reviewing the Parties’ briefing and the applicable law, the Court **GRANTS in part** and **DENIES in part** Defendants’ Motion to Compel Request for Production 79 (ECF No. 267) and **GRANTS in part** and **DENIES in part** Defendants’ Motion to Compel (ECF No. 269).

I. BACKGROUND¹

Plaintiff X Corp. (“Plaintiff” or “X”) brought this action on November 20, 2023, against Media Matters, Eric Hananoki, and Angelo Carusone (collectively, “Defendants”) alleging interference with contract, business disparagement, and interference with prospective economic advantage. Plaintiff contends that Defendants knowingly and maliciously fabricated side-by-side images of various advertisers’ posts on Plaintiff’s social media platform, X, next to neo-Nazi or other extremist content and then portrayed these designed images as if they were what the average user experiences on X. Plaintiff asserts that Defendants intended to harm it by proceeding with this course of action in an effort to deceptively portray X as a social media platform dominated by neo-Nazism and antisemitism and thereby alienate major advertisers, publishers, and users from X.

On April 23, 2026, the Court issued an opinion addressing two of the Parties’ many motions to compel.² In its Order, the Court deferred ruling on Defendants’ Motion to Compel as to Request for Production 79 (“RFP 79”) and ordered additional briefing regarding Plaintiff’s invocation of the Stored Communications Act (“SCA”), 18 U.S.C. § 2702(a).³ Plaintiff filed its supplemental brief on May 4, 2026, Defendants responded on May 11, 2026, and Plaintiff filed a reply on May 18, 2026.

¹ Unless otherwise indicated, the Court’s recitation of the facts is taken from Plaintiff’s Amended Complaint. *See* Pl.’s Am. Compl., ECF No. 37.

² *See* Order, April 23, 2026, ECF No. 288.

³ *Id.* at 8.

On March 2, 2026, Defendants filed a separate Motion to Compel seeking the removal of redactions on produced documents made by Plaintiff pursuant to the SCA.⁴ Plaintiff filed a timely response,⁵ and Defendants similarly replied.⁶ Both Motions are ripe for the Court's review.

II. LEGAL STANDARDS

Federal Rule of Civil Procedure 26(b) governs the scope of discovery. The Rule provides that “parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case.” FED. R. CIV. P. 26(b)(1).

Federal Rule of Civil Procedure 37 controls motions to compel discovery or disclosure. “A party seeking discovery may move for an order compelling an answer, designation, production, or inspection.” FED. R. CIV. P. 37. After a party has attempted in good faith to obtain discovery without court action, Rule 37 allows a motion to compel when a party fails to answer or respond to a request for production under Rule 34, provided such discovery requests are within the scope of Rule 26(b). FED. R. CIV. P. 37(a)(3). “[A]n evasive or incomplete disclosure, answer, or response must be treated as a failure to disclose, answer, or respond.” FED. R. CIV. P. 37(a)(4).

The party resisting discovery must show specifically how each discovery request is not relevant or otherwise objectionable. *McLeod, Alexander, Powel & Apffel, P.C. v. Quarles*, 894 F.2d 1482, 1485 (5th Cir. 1990). A response to a Rule 34 request “must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons” for each item or category. FED. R. CIV. P. 34(b)(2)(B). The 2015 revision of the Federal Rules precludes the use of boilerplate objections. *See* FED. R. CIV. P. 26(b) advisory committee’s notes to 2015 amendment.

⁴ Defs.’ Mot. Compel, ECF No. 269.

⁵ Pl.’s Resp., ECF No. 277.

⁶ Defs.’ Reply, ECF No. 290.

III. ANALYSIS

Both of Defendants' motions pending before the Court implicate the SCA. The first asks the Court to compel production of certain X posts based on RFP 79. The second asks the Court to compel Plaintiff to remove redactions it made to internal communications produced through discovery to Defendants.

A. Defendants' Motion to Compel RFP 79

In RFP 79, Defendants request production of "[a]ll content posted to [certain] accounts from November 15, 2022 through the present, including any content that was removed, suspended, or otherwise disciplined for any reason."⁷ Defendants clarify that this request "does not seek private messages or communications between non-parties to this lawsuit."⁸ Plaintiff objects on the grounds that the user content responsive to Defendants' request is protected by the SCA and is irrelevant and unduly burdensome to produce.⁹ Defendants argue that the SCA does not prevent production of posts from the disputed accounts because the content was originally publicly available, and that after Defendants' reporting, Plaintiff or the users deleted the formerly public posts from these accounts and Plaintiff then suspended many of the accounts.¹⁰ Plaintiff does not dispute that currently public posts are not protected by the SCA.¹¹ As such, the Court's evaluation of these arguments is limited to posts not currently publicly available on the X platform.

The posts at issue could fall into three buckets: (1) private posts available only to a user's followers, (2) formerly public user-deleted posts, and (3) formerly public platform-deleted posts. Defendants assert that "only posts that were configured as public by users are at issue."¹² Plaintiff

⁷ Defs.' App. Supp. Mot. Compel, App. 011, ECF No. 240-2.

⁸ Defs.' Br. Supp. Mot. Compel 5, ECF No. 240-1.

⁹ Pl.'s Resp. 2–8, ECF No. 246.

¹⁰ Defs.' Br. Supp. Mot. Compel 4, ECF No. 240-1.

¹¹ Pl.'s Resp. Mot. Compel 3, ECF No. 277.

¹² Defs.' Suppl. Resp. 1, ECF No. 300-1.

does not appear to dispute this assertion.¹³ Thus, only formerly public posts that were either (1) deleted by a user or (2) removed by X are at issue. The Parties have not provided, and the Court has not found, a case squarely addressing whether such posts are subject to protection by the SCA.

1. Whether the SCA applies to X and the Posts at Issue

The SCA was enacted in 1986—long before the advent of social media platforms like X—to protect against potential intrusions on individual privacy that current federal statutes and the Fourth Amendment did not address. *Hately v. Watts*, 917 F.3d 770, 782 (4th Cir. 2019); *see also Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 791 (5th Cir. 2012). The statute “reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility.” *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072–73 (9th Cir. 2004). The SCA applies to two types of communication providers: an electronic communication service (“ECS”) and a remote computing service (“RCS”). *See* 18 U.S.C. § 2702(a).

Per the statute, “a person or entity providing an electronic communication service 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(a)(1) (emphasis added). An “electronic communication service” is 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). “Electronic communications” are defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12). And “‘electronic storage’ means-- (A) any temporary, intermediate storage of a wire

¹³ Pl.’s Suppl. Br. 9, ECF No. 293.

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).

The SCA further provides that

a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) 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 of any such communications for purposes of providing any services other than storage or computer processing.

18 U.S.C. § 2702(a)(2) (emphasis added). “The term ‘remote computing service’ 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). An “electronic communications system” is defined as “any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(14).

Defendants argue that the SCA only “protects private communications and user storage, not public content a platform may use for its own business purposes.”¹⁴ They urge the Court to follow *Snap, Inc. v. Superior Court*, which held that because social media companies access user content for business purposes, the SCA’s privacy protections do not apply.¹⁵ 323 Cal. Rptr. 3d

¹⁴ Defs.’ Suppl. Resp. 8, ECF No. 300-1.

¹⁵ *Id.*

576, 601–02 (2024). Plaintiff argues that *Snap*'s business theory is an atextual reading of the SCA and imposes limitations not found in the text of the statute.¹⁶ The Court agrees with Plaintiff.

The *Snap* decision is a novel reading of the SCA from a California appeals court, and it is the first decision to implement such a business theory.¹⁷ Nowhere in the text of the SCA does the statute contemplate whether communications are held for any business purpose. Moreover, *Snap* departs from the Ninth Circuit's decision in *Theofel*¹⁸ and the Fourth Circuit's decision in *Hately*¹⁹ where both Circuits determined that for purposes of ECS protections communications stored for a user's benefit were stored as backup protection. Because the Court disagrees with *Snap*'s holding as applied to the SCA, it declines to follow that decision.

Plaintiff contends that under the SCA the posts at issue are subject to both ECS and RCS requirements.²⁰ Defendants argue that neither protection applies because the posts (1) are not in electronic storage for purposes of the ECS requirements and (2) are not maintained by Plaintiff solely for storage or computer processing without Plaintiff having access for another purpose, as required by an RCS under the SCA.²¹

2. X as an ECS

The Parties do not appear to dispute that X is an ECS.²² Plaintiff asserts that the X platform's "central function is for users to send and receive communications electronically—whether broadcast publicly, restricted to followers of a protected account, or sent as direct

¹⁶ Pl.'s Resp. Mot. Compel 6–7, ECF No. 277.

¹⁷ Pl.'s App. Supp. Resp. Mot. Compel App. 023, 045, ECF No. 278.

¹⁸ 359 F.3d at 1076.

¹⁹ 917 F.3d at 797.

²⁰ Pl.'s Suppl. Br. 4–6, ECF No. 293.

²¹ Defs.' Suppl. Resp. 4–5, ECF No. 300-1.

²² Pl.'s Suppl. Br. 1, ECF No. 293; Defs.' Mot. Compel 3, ECF No. 269; Defs.' Suppl. Resp. 5, ECF No. 300-1.

messages.”²³ The Court agrees that X, as a “service which provides to users thereof the ability to send or receive wire or electronic communications,” is an ECS. 18 U.S.C. § 2702(a)(1). And because this finding triggers the requirements of the SCA, the Court need not evaluate whether Plaintiff is an RCS.

3. Whether the Posts are Stored for Purposes of Backup Protection

While neither party disputes that the posts are electronic communications, Defendants do dispute whether the posts at issue are in electronic storage—that is, “temporary, intermediate storage” or stored for “purposes of backup protection.”²⁴ 18 U.S.C. § 2510(17). Plaintiff does not contend that the posts are in temporary, intermediate storage.²⁵ As such, the Court does not reach this question.

“As with any question of statutory interpretation, [the] analysis begins with the plain language of the statute.” *Jimenez v. Quarterman*, 555 U.S. 113, 118 (2009). Relevant here is the meaning of “backup protection.” 18 U.S.C. § 2510(17). Because the statute does not define backup protection, the Court looks first to the words’ ordinary meaning. *Schindler Elevator Corp. v. U.S. ex rel. Kirk*, 563 U.S. 401, 407 (2011). When the statutory language is clear, it must be enforced according to its plain meaning. *Jimenez*, 555 U.S. at 118.

When referring to computers, “backup” means “[a] copy of a program or file that is stored separately from the original,” *Backup*, AMERICAN HERITAGE DICTIONARY <https://ahdictionary.com/word/search.html?q=backup> (last visited July 21, 2026), or “a copy of computer data (such as a file or the contents of a hard drive),” *Backup*, MERRIAN WEBSTER <https://www.merriam-webster.com/dictionary/backup#dictionary-entry-1> (last visited July 21,

²³ Pl.’s Suppl. Br. 4, ECF No. 293.

²⁴ Defs.’ Suppl. Resp. 5–7, ECF No. 300-1.

²⁵ See generally Pl.’s Suppl. Br., ECF No. 293.

2026), or “to make a duplicate copy of (a file, program, etc.), esp. to safeguard against loss or corruption of the original.” *Backup*, VI.22.d., OXFORD ENGLISH DICTIONARY https://www.oed.com/dictionary/back_v?tab=meaning_and_use#30509152 (last visited July 21, 2026). Protection means “[t]he act of protecting,” which, in turn, means “[t]o keep from being damaged, attacked, stolen, or injured.” *Protecting*, AMERICAN HERITAGE DICTIONARY <https://ahdictionary.com/word/search.html?q=protecting> (last visited July 21, 2026). Protection is also defined as “the act of protecting : the state of being protected,” which stems from “protect,” meaning “to cover or shield from exposure, injury, damage, or destruction,” *Protect*, MERRIAM WEBSTER <https://www.merriam-webster.com/dictionary/protect> (last visited July 21, 2026), or “[t]he action of protecting someone or something,” which, in turn, means “[t]o defend or guard from danger or injury.” *Protect*, OXFORD ENGLISH DICTIONARY https://www.oed.com/dictionary/protect_v?tab=meaning_and_use#27936173 (last visited July 21, 2026). Thus, under the plain language of the SCA, an electronic communication is stored for backup purposes when a “copy” of the communication is stored to prevent it from being “damaged” or “injured.”

Defendants’ backup protection challenge rests on two grounds: (1) that X’s terms of service do not specify “that it retains deleted or removed public posts for ‘backup protection,’ and ‘backup protection’ is not a label X can simply attach to any retained archive”; and (2) that none of the posts at issue merit protection because they were not stored solely as backup for the user.²⁶ Plaintiff argues “there is no doubt X maintains deleted posts for backup protection”²⁷ based on its terms of

²⁶ Defs.’ Suppl. Resp. 6, ECF No. 300-1.

²⁷ Defendants argue that Plaintiff has waived any storage conditions arguments made in its reply as new and in support cite the Court’s order waiving Defendants’ argument made in a prior reply. But the present situation is not analogous to Defendants’ previous discovery dispute. The Court previously held that Defendants waived their argument because Defendants argued in their motion to compel that exceptions to the SCA applied and then for the first time in reply argued that the SCA did not apply at all. Here, Plaintiff

service.²⁸ Plaintiff also contends that despite Defendants’ argument to the contrary, nothing in the SCA requires that the posts be stored exclusively for backup purposes.²⁹ The Court agrees with Plaintiff.

To start, Plaintiff’s privacy policy in effect during the relevant time period explains that X “may keep certain information . . . in order to comply with legal requirements and for safety and security reasons.”³⁰ Such a policy is sufficient to indicate that posts are kept for backup protection. Additionally, nothing in the SCA requires Plaintiff to keep a post solely for “backup protection.” The only requirement is that Plaintiff store a copy or duplicate of a post to prevent it from being damaged or destroyed, which Plaintiff asserts that it does. Citing several cases, Defendants argue that backup protection requires a “preservation or retrieval function for the user . . . [and] *deleted* messages d[o] not serve any backup purpose.”³¹ Defendants contend “[t]hese cases correctly read ‘backup protection’ to mean a secondary preservation copy connected to the user’s communication or retrieval interest, not every retained provider archive.”³²

But no such requirement is found in the SCA backup protection requirements, as other courts who have confronted this issue agree. For example, in *Republic of Gambia v. Facebook, Inc.*, the court applied the SCA to deleted private Facebook and Instagram pages and associated communications and determined that “copies stored by the service provider for its own purposes, rather than for the benefit of, or at the choice of, the user” are in electronic storage. 575 F. Supp.

has maintained throughout its briefing that the posts at issue cannot be disclosed because of the SCA, and its backup argument in its reply is made in response to Defendants’ argument that the posts are not stored for backup purposes. *See Cousin v. Trans Union Corp.*, 246 F.3d 359, 373 n.22 (5th Cir. 2001) (“[W]e see no real new issue in the reply brief, but rather responsive arguments to the appellee’s own contentions, and, therefore, little or no prejudice.”)

²⁸ Pl.’s Supp. Reply 3, ECF No. 303.

²⁹ *Id.*

³⁰ *See* X Privacy Policy Effective Sept. 29, 2023, § 4, https://x.com/en/privacy/previous/version_20.

³¹ Defs.’ Suppl. Resp. 6, ECF No. 300-1.

³² *Id.* at 7.

3d 8, 15 (D.D.C. 2021). The Fourth Circuit has also said that “messages stored by a web-based email service are stored for purposes of the web-based email service’s own backup protection as well as the user’s backup protection.” *Hately*, 917 F.3d at 796–97.

Logic further supports Plaintiff’s position. If a user deletes a post, the user is attempting to destroy that post. Likewise, if a social media company removes a post, they are damaging or destroying a user’s intended post. Therefore, if a post deleted by a user or removed by a social media company is still accessible by the company, then a copy of the post must be stored in some fashion as protection against destruction—*i.e.* backup protection. If not, a social media company could circumvent the protections of the SCA by removing posts at will or storing copies of user-deleted posts and claiming that the retained copies were not for backup protection. Such a system would allow a social media company to freely distribute to the government or other private parties content that would otherwise be protected by the SCA.

Because the Court finds that formerly public X posts removed by X or deleted by the user but still retained by X are stored for purposes of backup protection, the posts at issue are protected from disclosure by the SCA, absent an exception.

4. Whether an SCA Exception Applies

The SCA does not provide an exception to its general prohibition on disclosure for civil subpoenas. *See PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.*, 273 F. Supp. 3d 558, 560 (W.D. Pa. 2017). To permit disclosure of communications protected by the SCA, one of the exceptions enumerated in the SCA must apply. *See* 18 U.S.C. § 2702(b). Defendants contend that two exceptions, 18 U.S.C. §2702(b)(3) and (b)(5), allow Plaintiff to produce the content at issue.³³

³³ Defs.’ Br. Supp. Mot. Compel 5, ECF No. 240-1.

a. Section 2702(b)(5)

The Court begins with § 2702(b)(5), which provides that “[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.” 18 U.S.C. §2702(b)(5). Little caselaw exists applying § 2702(b)(5), as Plaintiff notes.³⁴ It does not appear that any federal court has evaluated whether a social media platform who is itself a party to a lawsuit can disclose formerly public, but now nonpublic, content pursuant to a civil subpoena. In evaluating this question, the Court again turns to the plain language of the statute.

The Court agrees with Defendants that the “disjunctive ‘**or**’ creates two independent prongs: disclosure incident to rendering the service, and disclosure to protect the provider’s rights or property.”³⁵ *See Encino Motorcars, LLC v. Navarro*, 584 U.S. 79, 87 (2018) (“‘or’ is almost always disjunctive”) (internal quotations omitted). As to the first prong, the Parties do not appear to argue that disclosure is necessarily incidental to rendering X’s service. Accordingly, the Court does not reach this issue.

Defendants argue that, under prong two, the plain language of § 2702(b)(5) permits disclosure of the posts at issue because Plaintiff brought suit to enforce to enforce its rights.³⁶ Plaintiff contends that § 2702(b)(5) is inapplicable here because it only permits disclosure of information “necessarily incident” to protecting its rights and is meant to be used at the providers discretion for self-protection.³⁷ Plaintiff asserts that this exception has typically been used to

³⁴ Pl.’s Suppl. Br. 14, ECF No. 293.

³⁵ Defs.’ Suppl. Resp. 19, ECF No. 300-1 (emphasis in original).

³⁶ Defs.’ Reply 6, ECF No. 250-1.

³⁷ Pl.’s Resp. 8, ECF No. 246; Pl.’s Suppl. Br. 14–17, ECF No. 293.

protect service providers who voluntarily disclose child pornography or evidence of child sexual exploitation.³⁸

To start, nothing in the plain language of § 2702(b)(5) limits it only to disclosure of child sexual abuse, even if that is how the statute is generally applied. As Defendants point out, § 2702(b)(6) expressly allows reporting of child pornography to the National Center for Missing and Exploited Children, and § 2702(b)(8) allows reporting to a governmental entity if the provider believes there is risk of death or serious injury to any person.³⁹ *See* § 2702(b)(6), (8).

The meaning of prong two comes down to what “as may be necessarily incident . . . to the protection of the rights or property of the provider of that service” means. § 2702(b)(5). Several phrases in this sentence are key to understanding its meaning. First, “necessarily incident.” *Necessarily* means “of necessity” or “unavoidably.” *Necessarily*, MERRIAM WEBSTER <https://www.merriam-webster.com/dictionary/necessarily> (last visited July 21, 2026). *Necessity*, in turn, means “the quality or state of being necessary,” or in other words, “absolutely needed.” *Necessity*, MERRIAM WEBSTER <https://www.merriam-webster.com/dictionary/necessity> (last visited July 21, 2026). *Unavoidably* means “not avoidable” or “inevitable,” *Unavoidably*, MERRIAM WEBSTER <https://www.merriam-webster.com/dictionary/unavoidably> (last visited July 21, 2026), or said another way, “incapable of being avoided or evaded.” *Inevitable*, MERRIAM WEBSTER <https://www.merriam-webster.com/dictionary/inevitable> (last visited July 21, 2026). *Incident* is defined as “occurring or likely to occur especially as a minor consequence or accompaniment.” *Incident*, MERRIAM WEBSTER <https://www.merriam-webster.com/dictionary/incident> (last visited July 21, 2026). Accordingly, for a disclosure to be

³⁸ Pl.’s Resp. 8, ECF No. 246; Pl.’s Suppl. Br. 14–17, ECF No. 293.

³⁹ Defs.’ Reply 3, ECF No. 250-1.

necessarily incident, the disclosure must be an absolutely needed or inevitable occurrence for the “protection of the rights or property of the provider.” § 2702(b)(5).

Requiring discovery in a case involving civil money damages does not seem to be a situation in which production is absolutely needed or an inevitable occurrence for the protection of the rights or property of X. If that were the case, then any time X, or another social media company, filed a lawsuit, or was sued, a discovery subpoena could be used to eviscerate the protections of the SCA by seeking any nonpublic information that might have relevance to the case. This cannot be what Congress intended. Indeed, “Congress expressed its ‘judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility.’” *Hately*, 917 F.3d at 783 (quoting *Theofel*, 359 F.3d at 1072). Defendants urge that the “legislative history confirms that ‘rights’ and ‘property’ include ‘intellectual property rights’ and ‘the right to be free from the theft of services’” thereby presupposing legal enforcement as an exception.⁴⁰ Such exceptions may indeed be what the House of Representatives intended but the Court is hesitant to give weighty consideration to this record because such a report often applies to a limited portion of legislators, is incomplete, or is unreliable. *See, e.g., United States v. Hinds Cnty. Bd. of Supervisors*, 128 F.4th 616, 640 n.1 (5th Cir. 2025) (“This court often holds that legislative history, of which a Senate Report is a component, is unreliable.”). Even so, citing to this legislative history does not change the conclusion that production would need to be absolutely necessary or an inevitable occurrence. The Court is not satisfied that allowing a user’s interest in confidentiality to be breached by a third party through civil discovery is “necessarily incident . . . to the protection of the rights or property of” Plaintiff.

⁴⁰ Defs.’ Suppl. Resp. 19, ECF No. 300-1 (quoting H.R. Rep. No. 99-647, at 67 (1986)).

b. Section 2702(b)(3)

Section 2702(b)(3) provides that “[a] provider . . . may divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or the intended recipient of such communication, or the subscriber in the case of remote computing service.” 18 U.S.C. § 2702(b)(3). As the Court previously explained, the posts sought by Defendants, and contested by Plaintiff, can be divided into two buckets: (1) user-deleted posts and (2) platform-deleted posts. Defendants argue that under this exception a user who publicly posts on the X platform consents to disclosure of their content regardless of whether the post is later deleted by the user or the platform.⁴¹ Plaintiff argues that consent is revokable and, regardless of whether a user or X deletes a post, the post should be protected by the SCA.⁴²

i. User-Deleted Posts

Plaintiff argues that posts voluntarily deleted by a user indicate that the user has withdrawn their initial consent to public disclosure.⁴³ Defendants argue that because the posts were previously publicly posted, any expectation of privacy was waived through X’s terms of service, and as such, the posts cannot now be withheld.⁴⁴ The Court agrees with Plaintiff.

Here, it is not readily apparent who the “addressee or the intended recipient of such communication” would be, which leaves only the originator to give or revoke consent. 18 U.S.C. § 2702(b)(3). When a user intentionally deletes content, the user’s intent is clearly to render that content inaccessible to the public. Requiring Plaintiff to produce deleted content in response to a discovery demand would directly undermine the user’s deliberate choice to remove the content from public view. By voluntarily and intentionally removing a post from public view, the user

⁴¹ *Id.* at 10–16.

⁴² Pl.’s Resp. 4–5, ECF No. 246); Pl.’s Suppl. Br. 12, ECF No. 293.

⁴³ Pl.’s Suppl. Br. 12, ECF No. 293.

⁴⁴ Defs.’ Br. Supp. Mot. Compel 5, ECF No. 240-1; Defs.’ Reply, 3–4, ECF No. 250-1.

demonstrates his intent to shield the deleted post from general access. Similar to Fourth Amendment searches, while a user might initially consent to public display of a post, the user can withdraw that consent and regain their right to privacy.⁴⁵ See, e.g., *United States v. Ho*, 94 F.3d 932, 934 (5th Cir. 1996) (holding that a warrantless search is improper after consent is withdrawn); see also *Facebook, Inc. v. Superior Court*, 4 Cal. 5th 1245, 1287, 417 P.3d 725, 753 (2018) (observing that whether “reconfiguration or deletion should be understood as a revocation of lawful consent for purposes of section 2702(b)(3)” is an issue of first impression and declining to express an opinion on the issue).

Defendants’ argument that by agreeing to X’s terms of service a user consents to use of their content for “any purpose” is also unavailing.⁴⁶ First, X’s terms of service provide that “[y]ou retain your rights to any Content you submit, post or display on or through the Services. What’s yours is yours — you own your Content (and your incorporated audio, photos and videos are considered part of the Content).”⁴⁷ The logical outflow of this is that a user could delete and therefore withdraw consent for their content to be shared. Plaintiff agrees with this interpretation.⁴⁸ Further, embracing Defendants’ position would mean that a post made publicly only momentarily—whether by accident or upon reflection that the post was in bad taste—and then deleted would forfeit all SCA protections. Such a harsh result seems counter to the SCA’s goal of protecting a user’s expectation of privacy. Because producing posts deleted by a user contravenes the user’s recapture of their privacy, the Court finds that in this instance user-deleted posts are protected from disclosure under the SCA.

⁴⁵ “Congress passed the SCA in 1986 as part of the Electronic Communications Privacy Act. The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.” *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1179 (9th Cir. 2013).

⁴⁶ Defs.’ Suppl. Resp. 10–11, ECF No. 300-1.

⁴⁷ Defs.’ App. Supp. Reply App. 008, ECF No. 250-2.

⁴⁸ Pl.’s Supp. Reply 6, ECF No. 303.

ii. Platform-Deleted Posts

Posts deleted or removed by X present a straightforward question: does a user's consent for disclosure continue even after a post is deleted or removed by a social media platform? Plaintiff argues that deleting a user's post removes the user's ability to withdraw consent and therefore posts deleted or removed by X should be protected from disclosure under the SCA because courts cannot infer that users whose posts were removed months or years ago would continue to maintain their posts publicly.⁴⁹ Defendants counter that a user provides consent for disclosure under § 2702(b)(3) by publicly posting to X's platform, and X's removal or deletion of a post does nothing to alter that.⁵⁰ Based on the plain language of § 2702(b)(3), the Court agrees with Defendants.

According to the statute, once a provider has the "lawful consent of the originator," it "may divulge the contents of a communication." 28 U.S.C. § 2702(b)(3). By posting content publicly for anyone to see, the originator of the post has unequivocally consented to disclosure. Further, before publicly posting, users agree to X's terms of service, which grant X a license to "use, copy, reproduce, process, adapt, modify, publish, transmit, display, upload, download, and distribute" public content "in any and all media . . . for any purpose" and informs users that the license allows X "to make your Content available to the rest of the world and to let others do the same."⁵¹ As the Parties agree, the purpose of the SCA is to keep private communications a user intends to keep private.⁵² By publicly posting content, a user has indicated that they do not intend to keep the communication private. And once X removes or deletes an already public post, there is no indication that the poster has withdrawn consent or would withdraw consent if given the

⁴⁹ Pl.'s Resp. 6, ECF No. 246; Pl.'s Suppl. Br. 12, ECF No. 293.

⁵⁰ Defs.' Suppl. Resp. 12–14, ECF No. 300-1.

⁵¹ Defs.' App. Supp. Reply App. 008, ECF No. 250-2.

⁵² Pl.'s Suppl. Br. 2, ECF No. 293; Defs.' Suppl. Resp. 3, ECF No. 300-1.

opportunity. Nor does the statute require inquiring whether a user still consents to disclosure. Rather, all that is required is lawful consent, which unless revoked, is given by a user when making a public post. As such, under the text of § 2702(b)(3), publicly made posts that are later deleted or removed by X are allowed to be disclosed by a provider, absent an indication that the user revoked consent. To be clear, communications that a user intends to keep private or posts shared only with a user’s followers would not fall under this same analysis.

5. Remaining Objections

Plaintiff objects that the posts Defendants seek are not relevant because “[t]his litigation concerns a handful of post adjacencies occurring in November 2023 and involving specific users named in RFP 79. It does not involve the substance of thousands of posts made by these users in the years before or after.”⁵³ Defendants respond that Plaintiff knew or should have known that these accounts were producing distasteful content before Defendants’ articles.⁵⁴ Because “relevancy is broadly construed, and a request for discovery should be considered relevant if there is ‘any possibility’ that the information sought may be relevant to the claim or defense of any party,” the Court **OVERRULES** Plaintiff’s objections. *S.E.C. v. Brady*, 238 F.R.D. 429, 437 (N.D. Tex. 2006) (Ramirez. M. J.) (quoting *Merrill v. Waffle House, Inc.*, 227 F.R.D. 467, 470 (N.D. Tex. 2005)).

* * *

Because the SCA does not prohibit disclosure of publicly made posts that a user has consented to, and the Court has overruled Plaintiff’s remaining objections, the Court **ORDERS** Plaintiff to produce publicly made posts that were deleted or removed by X—and to which a user

⁵³ Pl.’s Resp. 7, ECF No. 246.

⁵⁴ Defs.’ Reply 3, ECF No. 250-1.

has not otherwise withdrawn consent—that are responsive to RFP 79 no later than August 31, 2026.

The Court is mindful of Plaintiff’s declaration from its Director of Safety that “Plaintiff can estimate, but cannot determine with absolute certainty, whether a specific post was deleted voluntarily by the user, deleted involuntarily by the user after a platform enforcement action, or removed involuntarily through platform enforcement actions.”⁵⁵ Accordingly, the Court **ORDERS** Plaintiff to take reasonable and good faith measures to locate and produce responsive posts. For any posts that X determines should not be produced, whether because a user deleted it or for some other reason, X is **ORDERED** to create a privilege log of the undisclosed posts and provide the log to Defendants. If Defendants believe a post has not been produced that should have been produced, the Court **ORDERS** Defendants to notify Plaintiff and provide all identifying information Defendants have in their possession which would allow Plaintiff to locate the disputed post and make a determination as to whether the post was publicly made and deleted or removed by X.

B. Defendants’ Motion to Compel Removal of Improper Redactions

Defendants move the Court to compel Plaintiff to remove redactions made pursuant to the SCA to internal email communications about content on the X platform produced in discovery.⁵⁶ Defendants raise four arguments to support their position that the redactions are improper and should be removed: (1) the business theory rule articulated in *Snap*, 323 Cal. Rptr. 3d at 601–02; (2) the provider-protection exception, § 2702(b)(5); (3) the user-consent exception for public posts, § 2702(b)(3); and (4) that Plaintiff’s internal memoranda, notes, and communications about user posts are not protected by the SCA because they are Plaintiff’s corporate records created for

⁵⁵ Pl.’s App. Supp. Resp., App. 006, 013, ECF No. 247-3.

⁵⁶ Defs.’ Mot. Compel 11–15, ECF No. 269.

its own business purposes.⁵⁷ Plaintiff argues that most of its SCA redactions are proper for the same reasons as discussed above.⁵⁸ It also acknowledges that a few redactions are improper because they relate to public content and has offered to remove these and any other improper public content redactions.⁵⁹ The Court takes each of Defendants' four arguments in turn.

1. Snap and SCA Exceptions

As the Court addressed above, it declines to follow *Snap* because nothing in the plain language of the SCA appears to disclaim protection for communications used for business purposes while in electronic storage. Likewise, the Court determined above that § 2702(b)(5) does not apply here because allowing a user's interest in confidentiality to be breached by a third party through civil discovery is not "necessarily incident . . . to the protection of the rights or property of" Plaintiff. 18 U.S.C. § 2702(b)(5). For these reasons, the Court finds that Defendants' first two arguments fail.

As for § 2702(b)(3), the Court explained above that two types of posts are implicated under this exception: (1) user-deleted posts and (2) platform-deleted posts. When a user deletes a post, even if it was once public, the user has withdrawn consent for a stored copy of the post to be disclosed. But when a platform deletes a public post, the user has consented to disclosure by making the post public, and even though the platform deletes or removes the post, that is no indication that the user has or would withdraw consent for disclosure. As such, under § 2702(b)(3), Plaintiff is allowed to disclose public posts that it deleted or removed from its platform, absent other indications that a user withdrew consent.

⁵⁷ *Id.* at 14.

⁵⁸ *See generally* Pl.'s Resp. Mot. Compel, ECF No. 277.

⁵⁹ *Id.* at 18.

2. Business Records

Defendants contend that Plaintiff's internal emails produced through discovery are business records and not subject to SCA protections.⁶⁰ Plaintiff argues that emails containing or discussing the contents of communications are protected by the SCA, while "noncontent information" is not protected from disclosure to non-governmental entities.⁶¹

Under the SCA, an ECS like X is prohibited from disclosing the "contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). "Contents" is broadly defined, to "include[] any information concerning the substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510(8). The Parties seemingly agree that "noncontent information" is defined as "information about the communication." *See* 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, 1227–28 (2004). Applying these definitions, the SCA protects any information concerning "the substance, purport, or meaning" of a user's communication, § 2510(8), but it does not protect "record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014).

Plaintiff avers that it "does not intend to redact 'noncontent information.'"⁶² As such, only content redactions are in dispute. Under the text of the SCA, when Plaintiff communicates internally and quotes, paraphrases, describes, or summarizes what a user said, such a communication is protected by the SCA because it discusses the "substance, purport, or meaning" of a user's communication. As the Court discussed above, to disclose a protected communication under the SCA, an exception must apply. Building on the Court's prior determinations, the only

⁶⁰ *Id.*

⁶¹ Pl.'s Resp. Mot. Compel 21, ECF No. 277.

⁶² *Id.*

exception that might permit disclosure is the user consent exception under § 2702(b)(3). Consistent with the Court's prior findings, if an internal communication discusses a public post that was deleted or removed by X, then, absent some indication that a user has withdrawn consent, there is user consent. But if an internal document references a private post or a post deleted by a user, then a user has not consented to disclosure, and the contents of the communication must be protected.

* * *

Because contents of communications that were public and subsequently deleted or removed by Plaintiff are not protected by the SCA, the Court **GRANTS in part** Defendants' Redaction Motion and **ORDERS** Plaintiff to remove redactions to all documents produced to Defendants containing communications about posts that are currently public or were public and subsequently deleted or removed by Plaintiff when there is not otherwise a revocation of consent.

The Court has considered Plaintiff's proportionality objection and the reported difficulties in determining whether a post was public and then deleted or removed by Plaintiff.⁶³ At this time, the Court **OVERRULES** this objection because Defendants assert that only about 200 documents need to be reviewed and have redactions removed, which is not overly burdensome.⁶⁴ In removing redactions to already produced documents and in making redactions going forward, Plaintiff shall make a good faith attempt to determine whether a post referenced in a communication was public and subsequently deleted or removed by the user. If a determination cannot be made, Plaintiff is permitted to make an appropriate SCA redaction unless Defendants can produce evidence that the contested post was public and then deleted or removed by Plaintiff. If Defendants make such a showing, Plaintiff shall remove the redaction.

⁶³ Pl.'s Resp. Mot. Compel 23–25, ECF No. 277.

⁶⁴ Defs.' Mot. Compel 15, ECF No. 269.

IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS in part** and **DENIES in part** Defendants' Motion to Compel (ECF No. 267) with respect to RFP 79. Plaintiff is **ORDERED** to produce all posts that were publicly available and subsequently deleted by Plaintiff by no later than August 31, 2026. For the reasons stated above, the Court additionally **GRANTS in part** and **DENIES in part** Defendants' Motion to Compel (ECF No. 269). Plaintiff is **ORDERED** to produce unredacted documents in accordance with this Order to Defendants by no later than August 31, 2026.

SO ORDERED on this **23rd day of July, 2026**.



Reed O'Connor
CHIEF UNITED STATES DISTRICT JUDGE