

**UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
JACKSONVILLE DIVISION**

WILLIAM LEE LAWSHE,

Plaintiff,

v.

Case No. 3:24-cv-137-MMH-LLL

VERIZON COMMUNICATIONS,  
INC., and SYNCHRONOSS  
TECHNOLOGIES, INC.,

Defendants.

---

**ORDER**

**THIS CAUSE** is before the Court on Defendant Synchronoss Technologies, Inc.'s Motion to Dismiss Amended Complaint (Doc. 26; Synchronoss's Motion), filed on April 12, 2024, and Defendant Verizon Communications Inc.'s Rule 12(b)(6) Motion to Dismiss (Doc. 27; Verizon's Motion), filed on April 12, 2024 (collectively Motions). In the Motions, invoking Rule 12(b)(6) of the Federal Rules of Civil Procedure (Rule(s)), Defendants seek dismissal of the claims in Plaintiff, William Lee Lawshe's, Amended Complaint (Doc. 39; Second Amended Complaint).<sup>1</sup> Lawshe timely responded

---

<sup>1</sup> Defendants filed the Motions when an earlier pleading was the operative complaint. See Amended Complaint (Doc. 22; First Amended Complaint), filed on March 11, 2024. The Magistrate Judge directed Lawshe to file a second amended complaint because the First Amended Complaint was not signed by an attorney and thus violated Rule 11(a). See Endorsed Order (Doc. 38), entered on May 29, 2024. Lawshe corrected this error by filing the

in opposition to the Motions. See Plaintiff's Response to Verizon's Rule 12(b)(6) Motion to Dismiss (Doc. 28; Response to Verizon's Motion), filed on May 3, 2024; Plaintiff's Response to Synchronoss's Rule 12(b)(6) Motion to Dismiss (Doc. 30; Response to Synchronoss's Motion), filed on May 3, 2024.<sup>2</sup> With leave of Court, Defendants filed a joint reply in support of the Motions. See Endorsed Order (Doc. 34), entered on May 20, 2024; Defendants Verizon Communications Inc. and Synchronoss Technologies, Inc.'s, Joint Reply in Support of Rule 12(b)(6) Motions to Dismiss (Doc. 40; Reply), filed on June 3, 2024. Accordingly, this matter is ripe for review.

---

Second Amended Complaint, which is otherwise identical to the First Amended Complaint. After Lawshe filed the Second Amended Complaint, the Court gave the parties the opportunity to file any objections to the Court considering the Motions as directed at the Second Amended Complaint. See Order (Doc. 41), entered on June 5, 2024. No party objected. As such, the Court considers the Motions to be directed at the Second Amended Complaint.

<sup>2</sup> In the Response to Synchronoss's Motion, Lawshe purports to incorporate by reference the arguments he raises in his Response to Verizon's Motion. Response to Synchronoss's Motion at 1. In doing so, Lawshe violates Rule 3.01(f), Local Rules of the United States District Court for the Middle District of Florida (Local Rule(s)). Local Rule 3.01(f) provides: "A motion, other legal memorandum, or brief may not incorporate by reference all or part of any other motion, legal memorandum, or brief." The Court reminds all counsel of their obligation to review and comply with the Local Rules of this Court. In this instance, in the interests of judicial economy, the Court will accept the Response to Synchronoss's Motion and consider the arguments Lawshe raises in the Response to Verizon's Motion to be directed also to Synchronoss's Motion. Future violations of the Court's Local Rules, however, will not be permitted.

## I. Background<sup>3</sup>

As a Verizon customer, Lawshe stores legal pornographic pictures depicting consenting adult models on Verizon’s cloud. Second Amended Complaint ¶¶ 7, 9, 10, 40, 44, 51, 54, 62(c), 83. Synchronoss is the data-storage subcontractor for Verizon’s cloud services. Id. ¶¶ 6, 9. Verizon and Synchronoss use technology called “hashing” to determine whether any of the data they host is child sexual abuse material (CSAM). Id. ¶ 21. Hashing involves using algorithms to compare an image’s “hash value” or “hash” to a list of hashes previously identified as actual or possible CSAM. Id. ¶¶ 21–24. A hash is a digital fingerprint for an image, and if two images share the same hash, they are almost certain to be identical images. Id. ¶¶ 22, 28. Like many others in the industry, Verizon and Synchronoss maintain lists of hashes that have been flagged as possible or alleged CSAM. Id. ¶¶ 23, 24, 31. By comparing the hashes of their customers’ files to the flagged hashes in their lists, Verizon and Synchronoss can determine with a high degree of confidence whether a customer is storing an image that has been previously flagged as

---

<sup>3</sup> In considering the Motions, the Court must accept all factual allegations in the Second Amended Complaint as true, consider the allegations in the light most favorable to Lawshe, and accept all reasonable inferences that can be drawn from such allegations. See Hill v. White, 321 F.3d 1334, 1335 (11th Cir. 2003); Jackson v. Okaloosa Cnty., 21 F.3d 1531, 1534 (11th Cir. 1994). As such, the facts recited here are drawn from the Second Amended Complaint and may well differ from those that ultimately can be proved.

actual or possible CSAM. Id. ¶¶ 24, 28, 31. However, the process of flagging images is “largely unregulated,” and an image can be flagged after “customer complaints” or reports from law enforcement. Id. ¶¶ 26, 27. When an image is flagged, the flag can include a “tag” for a particular category of image. Id. ¶¶ 31, 48, 81. The lists maintained by Verizon and Synchronoss rely entirely on tags provided by third parties including The National Center for Missing and Endangered Children (NCMEC) and law enforcement agencies. Id. ¶ 70. NCMEC, an organization tasked by statute with collecting and reporting information on online CSAM, uses tags including “unconfirmed” and “apparent” CSAM. Id. ¶¶ 31, 48, 81; see generally 34 U.S.C. § 11293(b)(1)(K). When Synchronoss or Verizon find a hash match, they send reports of the match (CyberTips) to NCMEC “instantly,” without human review or collecting any information about the subject images other than what the hash match itself provides. Second Amended Complaint ¶¶ 62(a), 63, 66.

Sometimes, Defendants’ hashing process flags images that are not CSAM. Id. ¶¶ 40, 41, 49, 62(c), 78, 79, 83, 88. Yet Defendants either have “no plan or process to determine” whether hash-matched images are CSAM, or they do not use such a plan. Id. ¶¶ 45, 46. On October 29, 2022, Synchronoss reported to NCMEC (the First CyberTip) that Lawshe possessed a file flagged as “apparent” CSAM (the First Image). Id. ¶ 81. The First Image was not

CSAM. Id. ¶ 83. On January 25, 2023, Defendants’ hashing process determined that one of Lawshe’s photos was a hash match with an image NCMEC categorized as “unconfirmed” CSAM (the Second Image). Id. ¶¶ 47, 48. Synchronoss reported the Second Image to NCMEC the same day (the Second CyberTip). Id. ¶ 58. In the Second CyberTip, Synchronoss stated that it “had viewed the entire contents” of the Second Image, that the Second Image “was not available publicly,” and that the Second Image “contained the lascivious exhibition of a ‘pre-pubescent’ minor.” Id. ¶ 61. None of these statements were true. Id. ¶¶ 49, 62. Indeed, the individuals depicted in both the First and Second Images “were easily identifiable as adults by the barest of review ... .” Id. ¶ 44; see also id. ¶ 54.<sup>4</sup>

---

<sup>4</sup> Verizon asks the Court to take judicial notice of alleged facts contained in documents filed in a different lawsuit Lawshe brought against different defendants. See Verizon’s Motion at 3 n.1, 5–6, 14–15; see also Response to Verizon’s Motion at 6. Courts may take judicial notice of documents from a prior proceeding because they are matters of public record and “capable of accurate and ready determination by resort to sources whose accuracy could not reasonably be questioned.” Horne v. Potter, 392 F. App’x 800, 802 (11th Cir. 2010) (internal quotation marks and quoted authority omitted). However, a “court may take judicial notice of a document filed in another court not for the truth of the matters asserted in the other litigation, but rather to establish the fact of such litigation and related filings.” United States v. Jones, 29 F.3d 1549, 1553 (11th Cir. 1994) (internal quotation marks and quoted authority omitted). Therefore, although the Court will take judicial notice of the docket and documents filed to determine that such documents were filed and that the parties and the court took certain actions, it will not take notice of the facts contained or alleged within those documents. See id.; see also Kruse, Inc. v. Aqua Sun Invs., Inc., No. 6:07-cv-1367-Orl-19UAM, 2008 WL 276030, at \*3 n.2 (M.D. Fla. Jan. 31, 2008) (“Pursuant to Federal Rule of Evidence 201, the Court is taking judicial notice of the state case and its docket entries[,] ... but not of the facts contained in those documents.”).

In citing to Horne, the Court notes that the Court does not rely on unpublished opinions as binding precedent; however, they may be cited in this Order when the Court finds them persuasive on a particular point. See McNamara v. GEICO, 30 F.4th 1055, 1060–

NCMEC relayed both CyberTips to law enforcement. Id. ¶¶ 72, 84, 100. After receiving the Second CyberTip, “law enforcement obtained a subpoena to search virtually all of [Lawshe’s] personal digital information and content.” Id. ¶ 72. The Second CyberTip led to Lawshe’s arrest. Id. ¶¶ 61(c), 72, 97, 101. Lawshe now brings claims against Verizon and Synchronoss for defamation and for violations of the Stored Communications Act, as amended, 18 U.S.C. § 2701 et seq., which prohibits companies like Verizon and Synchronoss from disclosing customer data unless an exception applies. See id. at 12–21; see also 18 U.S.C. §§ 2702, 2707.<sup>5</sup> Defendants contend Lawshe’s claims must be dismissed because the claims fail as a matter of law under the relevant statutory provisions, including provisions of the Protect Our Children

---

61 (11th Cir. 2022); see generally Fed. R. App. P. 32.1; 11th Cir. R. 36–2 (“Unpublished opinions are not considered binding precedent, but they may be cited as persuasive authority.”).

<sup>5</sup> Lawshe brings claims in eight counts, one for each combination of the cause of action, Defendant, and individual disclosure. See Second Amended Complaint at 12–21. In Count I, Lawshe brings a defamation claim against Verizon for the disclosure of Image Two. Id. ¶¶ 102–111. In Count II, Lawshe brings a defamation claim against Verizon for the disclosure of Image One. Id. ¶¶ 112–121. In Count III, Lawshe brings a defamation claim against Synchronoss for the disclosure of Image Two. Id. ¶¶ 122–126. In Count IV, Lawshe brings a defamation claim against Synchronoss for the disclosure of Image One. Id. ¶¶ 127–131. In Count V, Lawshe brings a claim under 18 U.S.C. § 2702 against Verizon for the disclosure of Image Two. Id. ¶¶ 132–140. In Count VI, Lawshe brings a claim under 18 U.S.C. § 2702 against Verizon for the disclosure of Image One. Id. ¶¶ 141–149. In Count VII, Lawshe brings a claim under 18 U.S.C. § 2702 against Synchronoss for the disclosure of Image Two. Id. ¶¶ 150–154. And in Count VIII, Lawshe brings a claim under 18 U.S.C. § 2702 against Synchronoss for the disclosure of Image One. Id. ¶¶ 155–159.

Act of 2008, as amended (PROTECT Act), 18 U.S.C. § 2258A et seq. See generally Verizon’s Motion; Synchronoss’s Motion.<sup>6</sup>

## II. Legal Standard

In ruling on a motion to dismiss under Rule 12(b)(6), the Court must accept the factual allegations set forth in the complaint as true. See Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009); Swierkiewicz v. Sorema N.A., 534 U.S. 506, 508, 508 n.1 (2002); see also Lotierzo v. Woman’s World Med. Ctr., Inc., 278 F.3d 1180, 1182 (11th Cir. 2002). In addition, all reasonable inferences should be drawn in favor of the plaintiff. See Randall v. Scott, 610 F.3d 701, 705 (11th Cir. 2010). Nonetheless, the plaintiff must still meet some minimal pleading requirements. Jackson v. BellSouth Telecomm., 372 F.3d 1250, 1262–63 (11th Cir. 2004). Indeed, while “[s]pecific facts are not necessary,” the complaint should “give the defendant fair notice of what the ... claim is and the grounds upon which it rests.” Erickson v. Pardus, 551 U.S. 89, 93 (2007) (per curiam) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007)). Further, the plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” Twombly, 550 U.S. at 570. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable

---

<sup>6</sup> Defendants do not contend that Lawshe fails to state claims for defamation. For purposes of resolving the Motions, the Court assumes but does not decide that Lawshe’s allegations in the Second Amended Complaint plausibly state claims for defamation.

inference that the defendant is liable for the misconduct alleged.” Iqbal, 556 U.S. at 678 (citing Twombly, 550 U.S. at 556). “But where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct,” the plaintiff has failed to meet their pleading burden under Rule 8. Id. at 679.

The “plaintiff’s obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Twombly, 550 U.S. at 555 (citations omitted); see also Jackson, 372 F.3d at 1262 (explaining that “conclusory allegations, unwarranted deductions of facts or legal conclusions masquerading as facts will not prevent dismissal” (quotation marks and quoted authority omitted)). Indeed, “the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions,” which simply “are not entitled to [an] assumption of truth.” See Iqbal, 556 U.S. at 679. Thus, in ruling on a motion to dismiss, the Court must determine whether the complaint contains “sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” Id. at 678 (quoting Twombly, 550 U.S. at 570).<sup>7</sup>

---

<sup>7</sup> The Court notes that, in his Response to Verizon’s Motion, Lawshe cites Hishon v. King & Spaulding, 467 U.S. 69 (1984), for the proposition that “a court may dismiss a complaint only if it is clear that no relief could be granted under any set of facts that could



### III. Discussion

#### A. The Protect Our Children Act of 2008

##### i. Interpreting the Relevant Statutory Provisions

Under 18 U.S.C. § 2258A, “providers” like Verizon and Synchronoss must issue CyberTips to the “CyberTipline of NCMEC” when they find CSAM on their platforms. 18 U.S.C. § 2258A(a)(1)(B).<sup>8</sup> Providers must satisfy this obligation “as soon as reasonably possible after obtaining actual knowledge of any facts or circumstances ... from which there is an apparent violation” of CSAM laws. 18 U.S.C. § 2258A(a). A CyberTip must describe “such facts or circumstances,” and at the provider’s discretion, may include additional

---

be proven consistent with the allegations.” See Response to Verizon’s Motion at 4. This is the standard the Supreme Court articulated in Conley v. Gibson, 355 U.S. 41 (1957). See Hishon, 467 U.S. at 73 (citing Conley, 355 U.S. at 45–46). Such an argument is shocking given that in 2007 the Supreme Court issued the Twombly decision in which it explicitly retired Conley’s “no set of facts” test, stating that the phrase is “best forgotten as an incomplete, negative gloss on an accepted pleading standard ... .” See Twombly, 550 U.S. at 563. The Supreme Court further clarified the pleading standard and emphasized Conley’s demise in its 2009 Iqbal decision. See Iqbal, 556 U.S. at 670. Nevertheless, despite the passage of over seventeen years since the Twombly decision, and over fifteen years since Iqbal, as well as the abundance of Eleventh Circuit precedent citing those decisions, Lawshe has included Conley in his Response to Verizon’s Motion with apparently no effort to cite currently applicable legal authority. See Response to Verizon’s Motion at 4 (citing no case more recent than 2005 in the “Standard on a Motion to Dismiss” section). Counsel is cautioned that his duty of candor to the Court includes the obligation to assure the continuing viability of any authority cited to the Court.

<sup>8</sup> A “provider” is “an electronic communication service provider or remote computing service.” 18 U.S.C. § 2258E. No party disputes that Verizon and Synchronoss are providers.

information, including identifying information for the apparent violator, historical information, geolocation information, and the subject images. 18 U.S.C. § 2258A(a)(1)(B)(ii), 2258A(b). Upon receipt of a CyberTip, NCMEC reviews the report and must then forward it to an appropriate law enforcement agency. 18 U.S.C. § 2258A(c). A provider that “knowingly and willfully fails to make a report” as required under subsection (a) faces a fine up to hundreds of thousands of dollars. 18 U.S.C. § 2258A(e).

Providers are not, however, required to put in any effort whatsoever to identify CSAM on their platforms. In a subsection captioned “Protection of Privacy,” Congress has directed that:

Nothing in [§ 2258A] shall be construed to require a provider to—  
(1) monitor any user, subscriber, or customer of that provider;  
(2) monitor the content of any communication of any person described in paragraph (1); or  
(3) affirmatively search, screen, or scan for facts or circumstances described in [sub]sections (a) and (b).

18 U.S.C. § 2258A(f). Still, § 2258C authorizes providers and NCMEC to coordinate efforts to combat CSAM. Section 2258C permits NCMEC to share hash values associated with CyberTips with providers, and providers may use these hash values “for the sole and exclusive purpose of permitting that provider to stop the online sexual exploitation of children.” 18 U.S.C. § 2258C(a). Consistent with § 2258A(f), § 2258C(c) reiterates that nothing in the section “requires providers receiving [hashes] relating to any CyberTip[]

from NCMEC to use the [hashes] to stop the online sexual exploitation of children.” 18 U.S.C. § 2258C(c).

Turning to the heart of the parties’ dispute, in § 2258B, the PROTECT Act gives providers limited immunity. Unless an exception applies, “a civil claim ... against a provider ... arising from the performance of the reporting or preservation responsibilities of such provider ... under [§ 2258B], [§] 2258A, or [§] 2258C may not be brought in any Federal or State court.” 18 U.S.C. § 2258B(a). That immunity, however, does not apply when the provider “engaged in intentional misconduct” or acted or failed to act “with actual malice[,] with reckless disregard to a substantial risk of causing physical injury without legal justification[,] or for a purpose unrelated to the performance of any responsibility or function under [ §§] 2258A, 2258C, 2702, or 2703.” 18 U.S.C. § 2258B(b) (subsection identifiers omitted). Verizon and Synchronoss contend that they benefit from § 2258B immunity for their disclosures to NCMEC of the hash matches for the subject images and, as such, that Lawshe’s claims must be dismissed. See generally Motions. Lawshe disagrees, contending that the disclosures do not satisfy the requirements of § 2258B immunity, and that even if they do, an exception to immunity applies. See generally Responses.

To determine if Defendants are entitled to immunity under § 2258B, the Court must determine whether the reports about which Lawshe complains constitute conduct “arising from the performance” of Defendants’ “reporting responsibilities.” See 18 U.S.C. § 2258B(a). As a preliminary matter, the Court concludes that, as relevant to immunity based on § 2258A(a) disclosures, immunity extends only to those disclosures which a provider is required to make—optional reports do not “aris[e] from the performance” of “reporting responsibilities.” See id. As discussed above, the § 2258A(a) reporting responsibilities of a provider such as Verizon or Synchronoss require the submission of CyberTips to NCMEC when the provider has “actual knowledge of any facts or circumstances ... from which there is an apparent violation” of federal CSAM laws. See 18 U.S.C. § 2258A(a). Unhelpfully, the PROTECT Act does not define what constitutes an “apparent violation” of federal CSAM laws. See 18 U.S.C. § 2258A et seq.

Lawshe contends that the word “apparent” in § 2258A has a technical meaning (“certain”) because in the CSAM-detection industry, “apparent CSAM” means content that is “certain, clear, or overtly clear” CSAM. See Response to Verizon’s Motion at 5, 7. As a general matter, courts “normally interpret[] a statute in accord with the ordinary public meaning of its terms at the time of its enactment.” Bostock v. Clayton Cnty., 590 U.S. 644, 654 (2020).

However, sometimes Congress employs “terms of art,” and courts are tasked with determining from context whether Congress intended a term to carry its ordinary meaning or a technical, legal meaning. See United States v. Hansen, 599 U.S. 762, 770–78 (2023) (holding that the context of the words “encourages or induces” indicated “that Congress used them as terms of art” with specialized meaning in criminal statutes). The phrases “apparent CSAM” and “apparent child pornography” are not found in the PROTECT Act or in the criminal statutes addressing CSAM crimes. Other than the fact that the word “apparent” is used in both phrases, there is no context to indicate that Congress had the term “apparent CSAM” in mind when referring to an “apparent violation” in § 2258A(a). Neither “apparent violation” nor “apparent CSAM” are defined in the edition of Black’s Law Dictionary contemporary with the PROTECT Act’s passage, and the pertinent edition of Black’s Law Dictionary provides two definitions of “apparent” which are both consistent with ordinary meaning. See Apparent, Black’s Law Dictionary (8th ed. 2004) (“1. Visible; manifest; obvious. 2. Ostensible; seeming”). As such, the Court will look to the ordinary meanings of the phrase “apparent violation.”

In ordinary use, the word “apparent” can have either a narrow meaning or a broad one. Apparent can narrowly mean openly or manifestly so, or more broadly mean seeming to be so yet perhaps not actually so. Compare Apparent

(1), (2), Merriam-Webster, <https://www.merriam-webster.com/dictionary/apparent>, accessed on February 28, 2025, (“open to view” or “clear or manifest to the understanding”), with id. (3), (4) (“appearing as actual to the eye or mind” or “manifest to the senses or mind as real or true on the basis of evidence that may or may not be factually valid”). The parties have provided no authority, and the Court has located none other than dicta, that defines the term “apparent violation” as it is used in § 2258A(a). Compare United States v. Lowers, 715 F. Supp. 3d 741, 754 n.4 (E.D.N.C. 2024) (stating in dicta, without elaboration, that “[i]t would defy logic for Congress to require [a provider] to report to NCMEC media that is seemingly [CSAM], but not necessarily so” (internal quotation marks and quoted authority omitted)), with Meta Platforms, Inc. v. District of Columbia, 301 A.3d 740, 750 (D.C. 2023) (stating in what is likely dicta that “providers must disclose to [NCMEC] any communications that they become aware of which indicate a violation of various laws against [CSAM]”).<sup>9</sup> The Court need not and does not decide how to resolve the ambiguity in the phrase “apparent violation” in § 2258A(a)

---

<sup>9</sup> In citing to Lowers, the Court notes that although decisions of other district courts are not binding, they may be cited as persuasive authority. See Stone v. First Union Corp., 371 F.3d 1305, 1310 (11th Cir. 2004) (noting that, “[a]lthough a district court would not be bound to follow any other district court’s determination, the decision would have significant persuasive effects”).

because, for the reasons explained below, the resolution of the Motions does not depend on which meaning is applied.

ii. Applying § 2258A(a) to the First and Second CyberTips

Defendants contend that a hash match always constitutes “facts or circumstances from which there is an apparent violation” of federal CSAM laws. See Synchronoss’s Motion at 6; Verizon’s Motion at 12–14. The Court finds that a more precise approach is appropriate, considering that the hash matches for Image One and Image Two contained different tags, thereby giving Defendants knowledge of different information.<sup>10</sup> In particular, Lawshe alleges that NCMEC’s tag on Image One identified the image as “apparent CSAM,” while NCMEC’s tag on Image Two identified the image as “unconfirmed.” Second Amended Complaint ¶¶ 48, 81. The parties agree that “apparent CSAM” is a term of art in the industry that is applied to content when it is “certain, clear, or overtly clear” that a child is depicted in the image. See Response to Verizon’s Motion at 5, 7; Reply at 2. Lawshe contends, and Defendants do not dispute, that the tag “unconfirmed,” on the other hand, refers to an image depicting individuals whose ages cannot be readily

---

<sup>10</sup> Lawshe’s allegations in the Second Amended Complaint do not make it clear whether Defendants’ hash databases include the NCMEC tags assigned to the hash. See generally Second Amended Complaint. Drawing all reasonable inferences in Lawshe’s favor, the Court will assume that Defendants’ database does tell Defendants what tag NCMEC assigned to the hash before Defendants submit the CyberTip.

determined. See Response to Verizon’s Motion at 5, 9; see generally Motions; Reply.

As to Image One, Lawshe acknowledges that Synchronoss and Verizon, through hashing, obtained knowledge that NCMEC categorized one of Lawshe’s images as “certain, clear, or overtly clear” CSAM. See Response to Verizon’s Motion at 5, 7; Second Amended Complaint ¶ 81. Even applying the narrow definition of “apparent” as “manifest,” see Apparent (2), Merriam-Webster, this would be a “circumstance” in which there is an “apparent violation” of CSAM laws. To conclude otherwise would frustrate Congress’s purposes in enacting § 2258A by practically requiring providers that wish to detect CSAM on their platforms to commit the acts constituting the subject offense that Congress seeks to prevent. See 18 U.S.C. § 2252A(a)(5) (imposing criminal penalties on anyone who “knowingly accesses with intent to view ... any ... material that contains an image of [CSAM]” that has been transported or produced with a computer). While caselaw is sparse in this area, in the Fourth Amendment context, courts have found that when a hash match to “known” or apparent CSAM is reported to law enforcement, no Fourth Amendment search takes place if a law enforcement officer opens the subject file because, in opening the file, law enforcement obtains no more information than was already provided by the hash match. See, e.g., United



States v. Reddick, 900 F.3d 636, 638–40 (5th Cir. 2018); Lowers, 715 F. Supp. 3d at 756–58.

The Court recognizes, as Lawshe’s allegations in the Second Amended Complaint demonstrate, a hash match to “apparent CSAM” does not establish with absolute certainty that an image is in fact CSAM. But even the narrow definition of “apparent” as “manifest” allows for the possibility of a false positive. If Congress had intended to mandate reporting only for actual CSAM, it could have specified as much. See N.L.R.B. v. SW Gen., Inc., 580 U.S. 288, 301 (2017) (explaining that Congress’s choice not to adopt a “readily available” alternative wording “strongly support[ed]” the conclusion that the alternative meaning does not apply). Accordingly, Defendants were required to send a CyberTip to NCMEC regarding Image One, and § 2258B immunity shields them from legal claims arising from the performance of their “reporting responsibilities.” The claims based on the First CyberTip (Counts II, IV, VI, and VIII) are due to be dismissed.<sup>11</sup>

---

<sup>11</sup> Lawshe attempts to raise two additional arguments to save these claims from dismissal, but neither succeeds. First, Lawshe argues that the exceptions to immunity in § 2258B(b) save his claims as to the First CyberTip. Response to Verizon’s Motion at 14–17. But Lawshe’s allegations are not enough to permit the reasonable inference that, in submitting the (ultimately false) First CyberTip, Verizon or Synchronoss engaged in “intentional misconduct” or acted “with actual malice.” Indeed, the Second Amended Complaint is devoid of any factual allegations which shed light on Verizon and Synchronoss’s motives in submitting the First CyberTip or their subjective beliefs regarding the veracity of the statements made in the First CyberTip. Lawshe’s analogy to a person who, knowing that one in ten packages contains a bomb, mails all ten packages anyway, is

As to Image Two and the Second CyberTip, however, the Court concludes that the hash match did not necessarily trigger Defendants' reporting responsibilities under § 2258A(a). Drawing all reasonable inferences in Lawshe's favor, the tag of "unconfirmed" CSAM in this case revealed only that, at some unidentified point in the past, an unidentified person at NCMEC, using unknown methods, flagged Image Two as an image that could not be determined to be CSAM (presumably because the person reviewing the image could not tell if the individual depicted was a minor). See Second Amended Complaint ¶ 48. While this could have alerted Defendants to a possible violation of CSAM laws, without more, this is not enough information for Defendants to conclude that a violation of CSAM laws "appear[ed] likely."

---

inapplicable to the facts alleged in the Second Amended Complaint. See Response to Verizon's Motion at 14–15. While Lawshe alleges that Synchronoss submits tens of thousands of CyberTips per year, he includes no facts from which any inference can be drawn as to the rate of false positives. His vague allegations that "some" or "a substantial percentage" of hash matches are false positives lack the specificity required to raise an inference of intentional misconduct or malice. See Second Amended Complaint ¶¶ 40, 41, 78, 79. Notably, he identifies only one other specific instance of a CyberTip with a false positive. Id. ¶ 88.

Second, Lawshe contends that an algorithmic hash match cannot constitute "actual knowledge" of anything because a hash match does not involve "a sentient human being." See Response to Verizon's Motion at 7–8. To support this contention, Lawshe cites to United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) (Gorsuch, J.) and United States v. Montijo, No. 2:21-cr-75-SPC-NPM, 2022 WL 93535 (M.D. Fla. Jan. 10, 2022). Yet neither of these cases even mentions what is required for a corporation to obtain "actual knowledge." As such, the Court concludes that Lawshe has not sufficiently raised this argument and considers the argument no further.

Indeed, even under Defendants’ proposed broad definition of “apparent” as “something that seems to be, or something that appears likely,” see Synchronoss’s Motion at 7; Verizon’s Motion at 11–12, knowledge that Lawshe possessed an image that is “unconfirmed” CSAM alone would not be knowledge of an “apparent violation” of CSAM laws. As such, at this early stage in the proceedings, the Court cannot say that knowledge of an “unconfirmed” CSAM tag match is “knowledge of the facts or circumstances from which there is an apparent violation” of CSAM laws.<sup>12</sup> Taking Lawshe’s allegations as true, he plausibly alleges that the Second CyberTip was a voluntary disclosure made as a result of Defendants’ voluntary efforts to net CSAM. Accordingly, relying on the allegations in the Second Amended Complaint, Defendants’ report of the hash match for Image Two did not “arise from the performance” of their “reporting responsibilities” under § 2258A, and

---

<sup>12</sup> The Court is unaware of any case in which a court has determined whether an “unconfirmed” tag gives rise to reporting responsibilities under § 2258A(a). Ostensibly importing the industry term “apparent CSAM” into the statutory phrase “apparent violation,” some courts suggest that only hash matches tagged as “apparent” CSAM trigger the reporting requirement. See, e.g., United States v. Sykes, No. 3:18-cr-178-TAV-HBG, 2020 WL 8484917, at \*10 (E.D. Tenn. Oct. 5, 2020), report and recommendation adopted, No. 3:18-cr-178-TAV-HBG, 2021 WL 165122 (E.D. Tenn. Jan. 19, 2021), aff’d, 65 F.4th 867 (6th Cir. 2023) (stating in what is likely dicta that “the mandatory reporting requirements apply only to apparent images of child pornography”).

§ 2258B does not shield them from potential liability for the claims in Counts I, III, V, and VII, which stem from the Second CyberTip.<sup>13</sup>

---

<sup>13</sup> One of the more in-depth discussions of NCMEC’s process for adding tags is found in United States v. Williamson, No. 8:21-cr-355-WFJ-CPT, 2023 WL 4056324, at \*1–3 (M.D. Fla. Feb. 10, 2023), report and recommendation adopted, No. 8:21-cr-355-WFJ-CPT, Doc. 144 (M.D. Fla. Mar. 21, 2023). In Williamson, the Magistrate Judge held an evidentiary hearing on a criminal defendant’s motion to suppress evidence law enforcement obtained from an NCMEC report. Id. at \*1. At the hearing, “the Executive Director of NCMEC’s Exploited Children Division, ... a Yahoo legal services manager, ... a former Yahoo employee, ... and [a law enforcement officer] all testified.” Id. Relying on this testimony, in a Report and Recommendation to the assigned District Judge, the Magistrate Judge recommended the finding that:

NCMEC applies the label of apparent child pornography to an image when it believes the activity depicted in the photograph “meets the federal definition of child pornography” and it is “overtly clear” a child is involved in that activity. By contrast, NCMEC employs the label of child pornography unconfirmed when it believes “the activity depicted ... appears to meet the federal definition of child pornography” but “there may be [a] question of the age of the individual seen in that particular image.” NCMEC only places an image on its CSAM hash list if the file was reviewed by at least two of its analysts and the analysts reached the same conclusion.

NCMEC, however, does not view its designations to be definitive, nor does it consider itself “the determiner[] of what is illegal or legal content.” As explained by Ms. Newman, who has worked at NCMEC for twenty-one years, including as a CyberTipline analyst, NCMEC’s classification of an image amounts to “an educated and informed impression of what is being depicted,” and NCMEC relies on law enforcement to do its own independent “investigation and assessment” of a file.

Id. at \*3 (alteration in original) (footnote and citations to the hearing transcript omitted). The District Judge adopted the Report and Recommendation as the opinion of the Court. See Amended Order (M.D. Fla. No. 8:21-cr-355-WFJ-CPT Doc. 144), entered on March 21, 2023. If true, these facts could support Defendants’ contention that the hash match for Image Two constitutes “facts or circumstances” of an “apparent violation” of CSAM laws. But the Court is limited to the facts Lawshe alleges in the Second Amended Complaint and to the reasonable inferences that can be drawn from those allegations and cannot take judicial notice of facts found by a court in a different proceeding.

To the extent Defendants argue that requiring additional investigation into images tagged as “unconfirmed” CSAM would chill providers’ content moderation and undermine Congressional intent, a review of § 2258A caselaw reveals that image-by-image human review is not uncommon. See, e.g., Sykes, 2020 WL 8484917, at \*3, \*12 (Facebook reviews the entire file before sending a CyberTip); United States v. Miller, No. CR 16-47-ART-CJS, 2017 WL 9325815, at \*1 (E.D. Ky. May 19, 2017), report and recommendation adopted, No. CV 16-47-DLB-CJS, 2017 WL 2705963 (E.D. Ky. June 23, 2017), aff’d, 982 F.3d 412 (6th Cir. 2020) (Google employees view images before adding apparent CSAM tags); United States v. Hart, 3:cr-20-197, 2021 WL 2412950, at \*10 (M.D. Pa. June 14, 2021) (Kik employees view images before sending CyberTips); Ackerman, 831 F.3d at 1294 (AOL employees view images before adding CSAM tags); United States v. Brillhart, No. 2:22-cr-53-SPC-NPM, 2023 WL 3304278, at \*2 (M.D. Fla. May 7, 2023) (Yahoo employees view images before sending CyberTips); Williamson, 2023 WL 4056324, at \*2 (same); United States v. DiTomasso, 81 F. Supp. 3d 304, 306 (S.D.N.Y. 2015), aff’d, 932 F.3d 58 (2d Cir. 2019) (human reviewers view images before Omegle sends CyberTips); but see Reddick, 900 F.3d at 637–38 (Microsoft uses an automated process to send CyberTips based on hash matches to “known” CSAM); United States v. Crawford, No. 3:18 CR 435, 2019 WL 3207854, at \*2

(N.D. Ohio July 16, 2019) (Synchronoss uses a fully automated process to send CyberTips and sends CyberTips based on hash matches to “suspected” CSAM). Certainly, the Court recognizes that minimizing the number of people who view CSAM is a paramount concern—but when all a provider knows about a customer’s image is that it depicts an individual of indeterminate age, some level of further investigation is appropriate before a provider is shielded from liability for reporting its customer’s private information to the government.

Last, while Defendants contend that permitting Lawshe’s claims regarding Image Two to proceed would destroy the immunity provided by Congress, which, they say, is “clearly” designed to “immuniz[e] civil claims for mistaken and incorrect reports,” see Synchronoss’s Motion at 5; Verizon’s Motion at 9 (quoting United States v. Richardson, 607 F.3d 357, 367 (4th Cir. 2010)), Defendants conflate an intent to immunize mistaken reports with an intent to immunize unfounded reports. As to Image Two, the issue is not whether Defendants were mistaken as to its contents, but whether given the information they had, Defendants possessed actual knowledge of facts or circumstances constituting an apparent violation of CSAM laws. Here, Lawshe plausibly alleges that a hash match to “unconfirmed” CSAM without anything more constitutes an unfounded report because Defendants did not

have actual knowledge triggering their reporting responsibilities under § 2258A(a).

Yet even if Defendants were arguably obligated to disclose Lawshe's possession of Image Two based on the hash match to "unconfirmed" CSAM, Lawshe has adequately alleged facts to support application of the "actual malice" exception to § 2258B immunity. See 18 U.S.C. § 2258B(b). In the context of defamation, "actual malice" means "with knowledge that [the statement] was false or with reckless disregard of whether it was false or not." New York Times Co. v. Sullivan, 376 U.S. 254, 280 (1964). The circumstances Lawshe alleges about the Second CyberTip support a reasonable inference that Defendants acted with reckless disregard as to the truthfulness of the statements they made in the Second CyberTip. Indeed, Lawshe alleges that Defendants made several unequivocally false statements in the Second CyberTip. In the Second CyberTip, Defendants stated that they "viewed the entire contents" of Image Two, that the image "was not available publicly," and that "the image contained the lascivious exhibition of a 'pre-pubescent' minor." Second Amended Complaint ¶ 61. Yet Lawshe alleges that Image Two was watermarked by a public website, id. ¶ 54(a), and that the individual depicted in Image Two was "easily identifiable as [an] adult[] by the barest of review," id. ¶ 44. These allegations suggest that Defendants did not in fact

view Image Two before submitting the Second CyberTip. Drawing all reasonable inferences in Lawshe's favor, as the Court must, Defendants' willingness to make false statements that they viewed Image Two, that it was not publicly available, and that it contained the lascivious exhibition of a prepubescent minor would plausibly support a finding that Defendants willfully disregarded the risk that the contents of the Second CyberTip were defamatory. Accordingly, even if Defendants were obligated to disclose Lawshe's possession of Image Two based on its "unconfirmed" hash match, Lawshe has adequately alleged that Defendants acted with actual malice as to the defamatory nature of the statements made in the Second CyberTip. For all of the foregoing reasons, to the extent Defendants seek dismissal of Counts I, III, V, and VII based on § 2258B immunity, the Motions are due to be denied.

B. The Stored Communications Act

Verizon and Synchronoss contend that Lawshe's remaining claims arising from the Second CyberTip under the Stored Communications Act (Counts V and VII) are due to be dismissed because § 2702 explicitly permits providers to make the disclosures about which Lawshe complains. Verizon's Motion at 18–19; Synchronoss's Motion at 11–12. Section 2702 provides that, unless an exception applies, a provider may not disclose to any third party the contents of one of its customer's communications or stored data (records). 18



U.S.C. § 2702(a). One of the statutory exceptions is that a provider may disclose such communications and records “to [NCMEC], in connection with a report submitted thereto under [§] 2258A.” 18 U.S.C. § 2702(b)(7), 2702(c)(5). Notably, § 2707 provides a civil action to individuals whose records or communications have been wrongfully disclosed under § 2702. See 18 U.S.C. § 2707.

Verizon and Synchronoss suggest that the § 2702 statutory exception applies to all disclosures made to NCMEC. See Verizon’s Motion at 18–19; Synchronoss’s Motion at 11–12. But Defendants’ singular focus on the recipient of the disclosure without considering the content and basis of the disclosure is at odds with the text of § 2702. It is true that for the exception to apply, NCMEC must be the recipient; but the disclosure also must be made “in connection with a report submitted thereto under [§] 2258A.” 18 U.S.C. § 2702(b)(6). And as the Court already discussed, § 2258A addresses mandatory reporting—nothing in § 2258A authorizes a provider to make disclosures to NCMEC outside of its mandatory reporting responsibilities. See 18 U.S.C. § 2258A. To read § 2702 as Defendants suggest would permit a provider to disclose the entirety of its customers’ stored data and communications to NCMEC. Nothing in the language of the statute supports such a conclusion. As such, the Court determines that the exceptions for

reports to NCMEC in § 2702 are coextensive with providers' reporting responsibilities under § 2258A. Accordingly, the Court concludes that, with regard to the Second CyberTip, Lawshe has sufficiently stated claims under §§ 2702 and 2707 in Counts V and VII.

C. The Good-Faith Defense Under 18 U.S.C. § 2707(e)

Last, Defendants contend Lawshe's claims must be dismissed because Defendants have a defense under § 2707(e). See Verizon's Motion at 17–18; Synchronoss's Motion at 10. Section 2707(e) states that “[a] good faith reliance on ... a statutory authorization ... is a complete defense to any civil or criminal action brought under this chapter or any other law.” 18 U.S.C. § 2707(e). Although Defendants call this defense an “immunity,” that characterization is belied by the plain language of § 2707(e), which calls it a “defense.” “[G]enerally, the existence of an affirmative defense will not support a rule 12(b)(6) motion to dismiss for failure to state a claim.” Fortner v. Thomas, 983 F.2d 1024, 1028 (11th Cir. 1993). But “[a] district court ... may dismiss a complaint on a rule 12(b)(6) motion ‘when [the plaintiff’s] own allegations indicate the existence of an affirmative defense, so long as the defense clearly appears on the face of the complaint.’” Id. (quoted authority omitted). Notably, the viability of a § 2707(e) defense depends on a fact: the defendant's subjective reliance on a statutory authorization. Here,

Defendants' subjective reliance on authorization under § 2702, § 2258A, or § 2258B does not clearly appear on the face of the Second Amended Complaint. Accordingly, the Court concludes that the Motions are due to be denied to the extent Defendants rely on the § 2707(e) defense with regard to the claims in Counts V and VII.

#### **IV. Conclusion**

The Motions are due to be granted as to Lawshe's claims that are based on the First CyberTip, Defendants' disclosure of Image One (Counts II, IV, VI, and VIII), because a hash match to "apparent" CSAM constitutes "facts or circumstances from which there is an apparent violation" of CSAM laws, and Lawshe failed to allege facts permitting the reasonable inference that Defendants engaged in intentional misconduct or acted with actual malice in making the disclosure. The Motions are due to be denied as to Lawshe's claims that are based on the Second CyberTip, Defendants' disclosure of Image Two (Counts I, III, V, and VII), because a hash match to "unconfirmed" CSAM does not constitute such facts or circumstances, and in the alternative, Lawshe has plausibly alleged that Defendants acted with actual malice in making false statements in the Second CyberTip. Whether Defendants acted in a good-faith reliance on a statutory authorization is not apparent from the face of the Second Amended Complaint.

Accordingly, it is

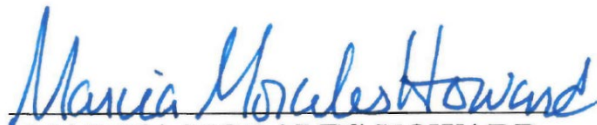
**ORDERED:**

1. Synchronoss's Motion to Dismiss (Doc. 26) is **GRANTED IN PART** and **DENIED IN PART**.
  - A. Synchronoss's Motion is **GRANTED** to the extent that Counts IV and VIII of the Second Amended Complaint (Doc. 39) are **DISMISSED**.
  - B. In all other respects, Synchronoss's Motion is **DENIED**.
2. Verizon's Motion to Dismiss (Doc. 27) is **GRANTED IN PART** and **DENIED IN PART**.
  - A. Verizon's Motion is **GRANTED** to the extent that Counts II and VI of the Second Amended Complaint are **DISMISSED**.
  - B. In all other respects, Verizon's Motion is **DENIED**.
3. Defendants must answer the remaining claims in the Second Amended Complaint in accordance with Rule 12.

*(remainder of page intentionally left blank)*

4. The parties shall conduct a case management conference and file an amended case management report on the form required by this Court no later than **March 21, 2025**.

**DONE AND ORDERED** in Jacksonville, Florida this 28th day of February, 2025.

  
**MARCIA MORALES HOWARD**  
United States District Judge

lc33

Copies to:  
Counsel of Record